Государственное бюджетное образовательное
учреждение высшего образования
Московской области

«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

РЕСУРСАМ ОБЛАСТИ - ЭФФЕКТИВНОЕ ИСПОЛЬЗОВАНИЕ

XVI Ежегодная научная конференция студентов
Технологического университета

Сборник материалов
Часть 1

г.о. Королёв
2016

УДК 330:316:004
ББК 65
Р43

Ресурсам области - эффективное использование [Текст] /
Р43 Сборник материалов XVI Ежегодной научной конференции студентов Технологического университета. Часть 1 – Королёв М.О.: «МГОТУ», 2016. – 644 с.
ISBN 978-5-9908699-7-4

Настоящий сборник содержит материалы XVI Ежегодной научной конференции студентов Технологического университета «Ресурсам области - эффективное использование».

Цель проведения Конференции - привлечение молодежи к решению актуальных задач современной науки, обмен информацией о результатах студенческих исследовательских работ, углубление и закрепление знаний, стимулирование творческого отношения к своей профессии, приобретение навыков научных дискуссий и публичных выступлений. Сборник дает представление о разнообразии научных интересов студентов Университета, новых направлениях исследований в различных областях знаний.

Конференция проходила в два тура: кафедральный и секционный. В первом туре приняли участие 11 кафедр, студентами которых были подготовлены 243 научно-практических и аналитических работ. В рамках второго тура была организована работа трех секций: «Финансово-экономическая», «Техническая», «Науки о человеке и обществе». Оценка представленных работ проводилась Организационным комитетом Конференции.

В качестве почетных гостей и членов жюри в конференции приняли участие представители Администрации наукограда Королёв и ряда крупных предприятий города. Гости оценили высокий уровень и практическую значимость представленных на конференции научных студенческих работ.

УДК 330:316:004
ББК 65

** Все материалы даны в авторской редакции*

ISBN 978-5-9908699-7-4

СОДЕРЖАНИЕ

ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКИЙ ФАКУЛЬТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И УПРАВЛЯЮЩИХ СИСТЕМ

КАФЕДРА МАТЕМАТИКИ И ЕСТЕСТВЕННОНАУЧНЫХ ДИСЦИПЛИН

КАФЕДРА УПРАВЛЕНИЯ КАЧЕСТВОМ И СТАНДАРТИЗАЦИИ

ФИНАНСОВО-ЭКОНОМИЧЕСКИЙ ФАКУЛЬТЕТ

КАФЕДРА ФИНАНСОВ И БУХГАЛТЕРСКОГО УЧЕТА

КАФЕДРА ЭКОНОМИКИ

ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКИЙ ФАКУЛЬТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

БИОИНСПЕРИРОВАННЫЙ ПОДХОД ПРИ ПОСТРОЕНИИ САМОРАЗВИВАЮЩИХСЯ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Афонин Алексей Андреевич, студент 4 курса кафедры Информационной безопасности
Научный руководитель: **Соляной Владимир Николаевич,** к.воен.н., доцент, заведующий кафедрой Информационной безопасности

В данной статье рассматривается проблема построения системы обеспечения информационной безопасности, которая могла бы прогнозировать потенциально возможные деструктивные воздействия на информационные объекты и самостоятельно искала способ по ее предотвращению. За основу при построении такой системы взяты биологические механизмы.

Информационная безопасность (ИБ) компьютерных систем и сетей, деструктивные воздействия на информационные объекты, биоинсперированный подход, антиципация.

BIOINSPIRED APPROACH TO BUILDING INFORMATION SECURITY SYSTEM

Afonin Aleksey, 4rd year student of the Department of information security
Scientific adviser: **Solyanoy Vladimir,** Candidate of Military Sciences, Assistant Professor, Head of the Department of information security

In this article we are going to take a view of the structure of the informational security. It could predict potentially possible destructive impacts on the objects of information. It also could independently search for the ways of preventing these impacts. This structure is based on biological mechanisms.

Informational security of computing systems and network, destructive impacts on objects of information, bioinspirated method, anticipation.

В настоящее время вопросам обеспечения информационной безопасности посвящается большое количество работ как у нас в стране, так и за рубежом. Анализ существующих подходов в области проектирования компьютерных систем и сетей говорит о том, что в рамках обеспечения информационной безопасности объектов

отсутствуют механизмы, позволяющие осуществить пресечение атак. Одним из вариантов построения системы обеспечения ИБ объекта могут быть биологические системы (человек, клетки, нейронные сети), которые представляют собой достаточно сбалансированные системы, они в достаточной степени надежны, хотя и намного более сложные, чем современные компьютерные системы. Биологические системы могут приспосабливаться к изменяющимся условиям окружающей среды. Кроме того, биологические системы используют децентрализованные механизмы управления, что позволяет им успешно сохранять работоспособность и бороться с возникающими вредоносными воздействиями [1-17].

Подход, основанный на заимствовании и присвоении системе механизмов и свойств живых существ, есть не что иное, как биоинсперированный подход.

Анализ литературных источников позволил выдвинуть предположение о том, что если для защиты компьютерных систем удастся использовать механизмы, которые применяют в процессе своего существования биологические организмы, то можно добиться их высокой устойчивости к атакам и возможности самовосстановления после повреждений.

Живая природа породила многообразие различных механизмов, позволяющих биоорганизмам и биосистемам эффективно защищаться в условиях постоянно влияющих негативных факторов [4], вырабатывая иммунитет для выживания последующих поколений. Работу защитных механизмов организма можно наблюдать в различных аспектах проявления, начиная от химических реакций на клеточном уровне, заканчивая сложнейшим функционалом нервной и иммунной систем [2, 4].

Однако многообразие различных механизмов, реализуемых биосистемами, вызывает определенные трудности для понимания, какие именно из них можно использовать на данном этапе развития компьютерных технологий. Результатами исследования были выявлены три основных этапа, которые необходимо пройти, чтобы иметь возможность использовать биологические механизмы в компьютерных системах [3]:

• нахождение аналогий, то есть структур и методов, похожих как в биологических, так и в компьютерных системах;

• понимание того, как работает биосистема, поскольку необходимо наиболее точно описать и построить модель поведения биологической системы;

• упрощение модели биологической системы (без потери необходимых свойств) до такого уровня, при котором ее реализация в компьютерных системах станет возможной.

Можно проследить некую аналогию между биологическими и компьютерными системами: и те и другие принимают, обрабатывают, хранят и передают информацию, а их защитные механизмы не могут быть эффективными, если находятся только на одном уровне.

Биоорганизмы обладают развитыми механизмами координации, реализуемыми, к примеру, нервной системой, благодаря чему они могут координировать свои действия и накапливать опыт.

Предлагается механизм, обеспечивающий информационную безопасность компьютерных систем и сетей, на начальном этапе проектирования представить в виде иерархической [2, 4, 5] многоагентной системы, организованной по региональному принципу, который предполагает наличие (рис. 1):

• программных/аппаратно-программных агентов-сенсоров (АСн) и Агентов-эффекторов (АЭф), непосредственно участвующих в решении прикладных задач (нижний уровень);

• региональных центров сенсоров (РЦСи) и региональных центров, эффекторов (РЦЭф), осуществляющих управление АСн и АЭф в регионе, а также региональных центров (РЦ), координирующих действия РЦСи и РЦЭф (средний уровень);

• главного центра (ГЦ), координирующего деятельность РЦ, систематизирующего и обрабатывающего данные, полученные от РЦ (верхний уровень).

Рассматриваемая система должна выполнять как минимум следующие три основные функции:

• планирование раннего предупреждения и пресечения информационно-технических воздействий на объекты сетевой инфраструктуры;

• составление рабочих заданий АСн и АЭф, а также региональным узлам управления ими и координация этих работ;

• управление технологическими процессами.

Автоматизация процессов раннего обнаружения деструктивных воздействий на объекты сетевой инфраструктуры и их пресечения

предполагает разработку и внедрение сеть интеллектуальных агентов сбора и обработки информации, также системы управления ими.

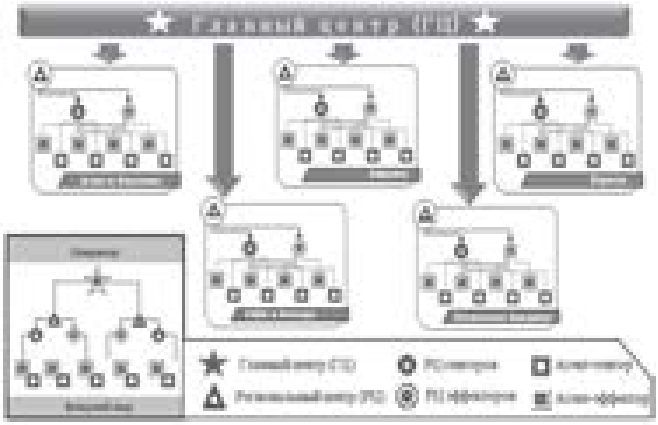


Рисунок 1 - Схема системы обеспечения информационной безопасности

Весь механизм должен функционировать как адаптивная система с автоматической переконфигурацией своей структуры и перепланированием действий, поддерживающих требуемый уровень безопасности информационно-технического ресурса. Это невозможно без предвидения развития ситуации. Данный метод носит название антиципация [6, 7].

Антиципация - способность представить себе возможный результат действия до его выполнения, а также представить способ решения проблемы прежде, чем она реально будет решена [2].

Антиципация характерна для многих видов животных. Особенно велика и многогранна роль антиципации в деятельности человека. Во всех без исключениях видах задач, решаемых человеком в процессе жизнедеятельности, антиципационные процессы являются базисом успешности и продуктивности их решения. Различают два смысловых аспекта понятия «антиципация»: во-первых, это способность прогноза и представления возможного результата действия до его выполнении, во-вторых, способность заблаговременно подготовиться к реакции на возможное событие до его реального наступлении.

Проблема исследования антиципации и вероятностного прогнозирования в последнее время активно обсуждается представителями разных наук [6]. Современные концепции,

существующие в этой области, обусловленные сложностью данных феноменов, многообразием их проявлений, отображают разнообразие теоретических и экспериментальных подходов.

Несмотря на то, что определенные подходы к дальнейшему развитию понятия антиципации уже сложилось, до настоящего времени недостаточно изученной оказалась область, затрагивающая функционирование антиципации в области обеспечения информационной безопасности [1-17].

Очевидно, что понятие антиципации может быть с пользой применимо не только к психической деятельности человека, но и к деятельности других сложных систем. Так, видится весьма заманчивым перенос свойства антиципации (или какого-то иного подобного) в системы, обеспечивающие информационную безопасность предприятий, занимающихся стратегически важными разработками в военной сфере, сфере медицины, новейших информационных технологий. Так же, применение данных систем необходимо на всех стратегических объектах страны.

Под антиципирующими системами обеспечения информационной безопасности предлагается понимать такие системы, которые способны принимать решения и действовать с определенным опережением в отношении ожидаемых событий, направленных на нарушение политики безопасности организации [1-17].

Для того чтобы система обеспечения информационной безопасности могла обладать свойствами антиципации, она должна (рис.2):

1. Получать информацию из «внешнего мира» через систему сенсоров;
2. Потреблять информацию из памяти системы о прошлом опыте;
3. Сопоставлять полученную информацию от сенсоров с имеющейся информацией;
4. Выдвигать гипотезы о возможных отдаленных событиях;
5. Порождать стратегии целенаправленного поведения системы;
6. Поддерживать требуемый уровень информационной защищенности компьютерной системы и сетей.

На современном этапе развития средств обеспечения информационной безопасности назрела объективная необходимость создания новых распределенных, многоагентных, адаптируемых,

самоконфигурируемых систем, способных осуществлять предупреждение и заблаговременное пресечение возможных информационно-технических воздействий на защищаемые ресурсы [7].

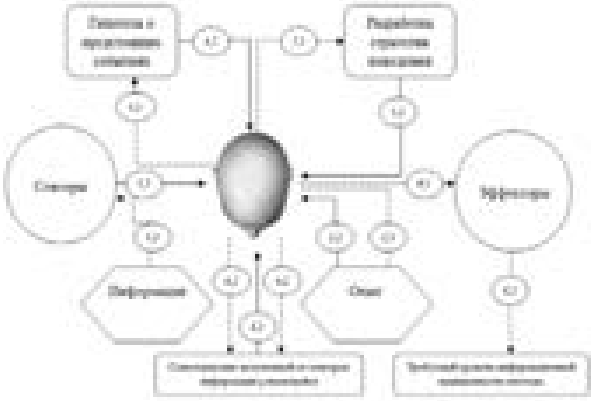


Рисунок 2 - Общая схема антиципирующей системы

Таким образом, в работе предлагается:

- рассмотреть механизм обеспечения защищенности компьютерных систем и сетей как информационную систему, способную к самообучению.
- при проектировании подобных систем обратить внимание на возможности биологических организмов, а именно на их способность действовать и принимать те или иные решения с определенным временно-пространственным упреждением в отношении ожидаемых, будущих событий.
- приступить к разработке методики создания саморазвивающихся систем информационной безопасности, основанных на работе биологических систем, что является следующим этапом рассмотрения данной проблемы.

Литература

1. Распоряжение Правительства РФ от 03.11.2011 № 1944-р «О перечне направлений подготовки (специальностей) в образовательных учреждениях высшего профессионального образования, специальностей научных работников, соответствующих приоритетным направлениям модернизации и технологического развития российской экономики» Официальная публикация в СМИ:

"Российская газета", № 254, 11.11.2011 "Собрание законодательства РФ", 14.11.2011, № 46, ст. 6584.
2. Доктрина информационной безопасности Российской Федерации. - М. 2000.
3. Климов С.М., «Методы и интеллектуальные средства предупреждения и обнаружения компьютерных атак на критически важные сегменты информационно-телекоммуникационных систем» - Таганрог: ТРТУ. 205.
4. Карпенко Л.А., Петровский А.В., Ярошевский М. Г., «Краткий психологический словарь» — Ростов-на-Дону: «ФЕНИКС». 1998.
5. Котенко И.В., Шоров А.В., Нестерук Ф.Г., «Анализ биоинспирированных подходов для защиты компьютерных систем и сетей» - Труды СПИИРАН. 2011
6. Котенко И.В., Шоров А.В., «Использование биологической метафоры для защиты компьютерных систем и сетей: предварительный анализ базовых подходов». - Инсайд. 2011.
7. Мессарович М., Мако Д., Тахара И., «Теория иерархических многоуровневых систем»: Пер.с англ – М.: Мир, 1973.
8. Соляной В.Н., Сухотерин А.И.. Взаимодействие человека, техники и природы: проблема информационной безопасности. Научный журнал (КИУЭС) Вопросы региональной экономики. УДК 007.51 №5 (05) г. Королёв. ФТА. 2010г.
9. Соляной В.Н., Сухотерин А.И., Федоров М.А. Выбор и внедрение новых образовательных технологий в (учебный процесс) подготовку бакалавров (специалистов) и магистров по информационной безопасности. «Современные образовательные технологии, используемые в очном, заочном и дополнительном образовании» [Текст] сборник – Королёв МО: Изд-во «Канцлер», ФТА, 2014.
10. Соляной В.Н., Сухотерин А.И. Модульно-ориентированный подход формирования базовых дисциплин ФГОС ВО 3+ как основа реализации профессиональной подготовки бакалавров в области информационной безопасности Научно-практический журнал №25, том 2 2015г. Информационное противодействие угрозам терроризма Материалы XIX Пленума учебно-методического объединения по образованию в области информационной безопасности «учебно-методическое обеспечение образовательных программ в области информационной безопасности» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН.ФЕД.УНИВ, 2015.-332 с. ISSN 2219-8792

11. Соляной В.Н., Сухотерин А.И. Становление направления «Радиоэлектронная безопасность информационных объектов» в системе дополнительного профессионального по информационной безопасности. Научно-практический журнал №25, том 2 2015г. Информационное противодействие угрозам терроризма материалы XIX пленума учебно-методического объединения по образованию в области информационной безопасности «учебно-методическое обеспечение образовательных программ в области информационной безопасности» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН.ФЕД.УНИВ, 2015.-332 с. ISSN 2219-8792
12. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Некоторые перспективы применения систем контроля и управления доступом в региональных ВУЗАХ. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» При поддержке Посольства Туркменистана в Российской Федерации. Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
13. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Развитие сотрудничества российских и зарубежных ВУЗОВ по защите информационного ресурса. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества Российских и зарубежных ВУЗов» При поддержке Посольства Туркменистана в Российской Федерации. Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
14. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
15. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных

учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
16. Соляной В.Н., Сухотерин А.И Выработка коммуникативной компетенции при подготовке профессионалов по информационной безопасности с использованием технологии модерации. «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7
17. Соляной В.Н., Сухотерин А.И, Антоненко В.И. Проблемно-ориентированная подготовка специалистов по информационной безопасности с использованием имитационного метода (мозговой штурм). «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. – М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7.

СОВЕРШЕНСТВОВАНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В БАНКАХ

Бакалов Даниил Игоревич, студент 1 курса кафедры Информационной безопасности
Научный руководитель: **Соляной Владимир Николаевич,** к.воен.н., доцент, заведующий кафедрой Информационной безопасности

Современная компьютерная система является информационной системой, представляющей собой многообразную совокупность средств и методов, обеспечивающих хранение, обработку, сбор, передачу и отображение информации в целях их достижения. Функциональной основой любой информационной системой являются информационные процессы, протекающие в ней. Характер этих процессов определяется соответствующей информационной технологией. Информационная технология – это совокупность средств и методов сбора, обработки, передачи данных (первичной информации) для получения информации нового качества (информационного продукта) о состоянии объекта, процесса или

явления. Иначе говоря, информационная технология представляет собой процесс, реализуемый в среде информационной системы.

Информационная система, процессы, информационная технология.

IMPROVING THE PROTECTION OF PERSONAL DATA IN BANKS

Bakalov Daniil, 1st year student of the Department of information security
Scientific adviser: **Solyanoy Vladimir,** Candidate of Military Sciences, Associate Professor, Head of the Department of information security

Modern computer system is an information system, which is a diverse set of tools and techniques that provide storage, processing, gathering, transmission, and display of information in order to achieve them. The functional basis of any information system is the information processes occurring in it. The nature of these processes is determined by the appropriate information technology. Information technology - a set of tools and methods for collecting, processing, transmitting data (primary data) for the new quality (product information) about the status of an object, process or phenomenon. In other words, information technology is a process implemented in the environment information system.

The information system, processes, information technology.

В ОАО «Альфа Банк» реализована политика безопасности, основанная на избирательном способе управления доступом. Такое управление в ОАО «Альфа Банк» характеризуется заданным администратором множеством разрешенных отношений доступа. Матрица доступа заполняется непосредственно системным администратором компании. Применение избирательной политики информационной безопасности соответствует требованиям руководства и требований по безопасности информации и разграничению доступа, подотчетности, а также имеет приемлемую стоимость ее организации. Реализацию политики информационной безопасности полностью возложено на системного администратора ОАО «Альфа Банк».

Функциональной основой любой ИС являются протекающие в ней информационные процессы. Характер этих процессов определяется соответствующей информационной технологией.

Информационная технология – это совокупность средств и методов сбора, обработки, передачи данных (первичной информации) для получения информации нового качества (информационного продукта) о состоянии объекта, процесса или явления. Иначе говоря, информационная технология представляет собой процесс, реализуемый в среде информационной системы.

Наряду с существующей политикой безопасности в компании ОАО «Альфа Банк», используется специализированные аппаратные и программные средства обеспечения безопасности.

В качестве аппаратного средства обеспечения безопасности используется средство зашиты – Cisco 1605. Маршрутизатор снабжен двумя интерфейсами Ethernet (один имеет интерфейсы TP и AUI, второй - только TP) для локальной сети и одним слотом расширения для установки одного из модулей для маршрутизаторов серии Cisco 1600. В дополнение к этому программное обеспечение Cisco IOS Firewall Feature Set делает из Cisco 1605-R идеальный гибкий маршрутизатор/систему безопасности для небольшого офиса. В зависимости от установленного модуля маршрутизатор может поддерживать соединение, как через ISDN, так и через коммутируемую линию или выделенную линию от 1200 бит/сек до 2Мбит/сек, FrameRelay, SMDS, x.25.

Для защиты информации владелец ЛВС должен обезопасить "периметр" сети, например, установив контроль в месте соединения внутренней сети с внешней сетью. Cisco IOS обеспечивает высокую гибкость и безопасность как стандартными средствами, такими как: Расширенные списки доступа (ACL), системами блокировки (динамические ACL) и авторизацией маршрутизации. Кроме того Cisco IOS Firewall Feature Set доступный для маршрутизаторов серии 1600 и 2500 обеспечивает исчерпывающие функции системы защиты включая:

- контекстное Управление Доступом (CBAC);
- блокировка Java;
- журнал учета;
- обнаружение и предотвращение атак;
- немедленное оповещение.

Кроме того, маршрутизатор поддерживает работу виртуальных наложенных сетей, туннелей, систему управления приоритетами, систему резервирования ресурсов и различные методы управления маршрутизацией.

В качестве программного средства защиты используется решение Kaspersky Open Space Security.

Kaspersky Open Space Security полностью отвечает современным требованиям, предъявляемым к системам защиты корпоративных сетей:

- решение для защиты всех типов узлов сети;
- защита от всех видов компьютерных угроз;
- эффективная техническая поддержка;
- «проактивные» технологии в сочетании с традиционной сигнатурной защитой;
- инновационные технологии и новое антивирусное ядро, повышающее производительность;
- готовая к использованию система защиты;
- централизованное управление;
- полноценная защита пользователей за пределами сети;
- совместимость с решениями сторонних производителей;
- эффективное использование сетевых ресурсов.

Основой задачей данной проектируемой системы является автоматизация защиты персональных данных. Оперативное управление процессами защиты информации составляет от одного до нескольких дней и реализует регистрацию событий, например оформление и мониторинг выполнения заявок, приход и удаление персональной информации и кодов защиты, и т.д. Эти задачи имеют итеративный, регулярный характер, выполняются непосредственными исполнителями бизнес-процессов (специалистами отдела кредитования, службы безопасности и т.д.) и связаны с оформлением и пересылкой документов в соответствии с четко определенными алгоритмами. Результаты выполнения операций регистрируются в соответствующих журналах. Автоматизация этих процессов позволит хранить информацию в одной базе.

Разрабатываемая система должна обеспечивать полный контроль, автоматизированный учёт и анализ защиты персональной информации, позволять уменьшить время обслуживания клиентов, получать информацию о кодах защиты информации и персональных данных.

Для формирования требования к разрабатываемой системе, необходимо сформировать требования к организации БД, информационной совместимости к разрабатываемой системе.

В данном случае, ИС содержит данные о сотрудниках фирмы. Одной из технологий, которая существенно иллюстрирует работу информационной системы, является разработка схемы документооборота для документов. В предлагаемой информационной системе основным документом является заявка на получение доступа к персональным данным, схема документооборота представлена на рис.1.

Функции разрабатываемой системы могут быть достигнуты, за счет использования вычислительной техники и программных средств. Учитывая, что поиск информации, сведений и документов учета в деятельности специалистов банка составляют порядка 30% рабочего времени, то внедрение автоматизированной системы учета позволит существенно высвободить квалифицированных специалистов, может привести к экономии фонда заработанной платы, уменьшения штата сотрудников, однако могут привести к и введению в штат сотрудников отдела штатной единицы оператора, в обязанности которого будет входить ввод сведений о протекающих бизнес-процессах: документов учета персональных данных и кодов доступа.

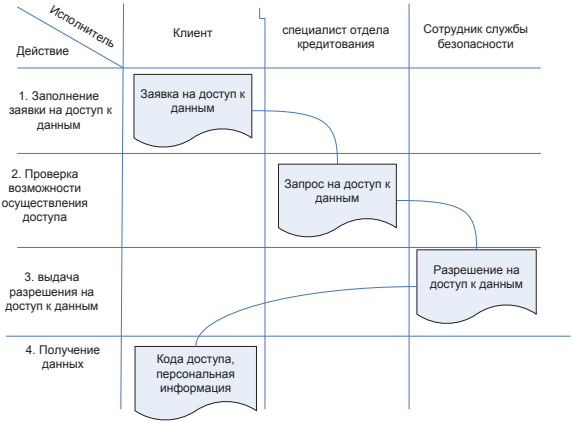


Рисунок 1 - Схема защищенного документооборота

Заявки на получение доступ к персональным данным

Необходимо отметить, что внедрение разрабатываемой системы, позволит снизить, а в идеале, полностью исключить ошибки учета персональной и информации и кодов защиты. Таким образом,

внедрение автоматизированного рабочего места менеджера приведет к значительному экономическому эффекту, сокращению штата сотрудников на 1/3, экономии фонда заработанной платы, повышению производительности труда. Необходимо отметить, что увеличение производительности приведет к возможности увеличения прибыли банка порядка 20%.

Автоматизация предприятия «по участкам» предусматривает внедрения небольших автоматизированных систем для прикрытия узких мест. Таким образом, через некоторое время предприятие будет представлять собой ряд разрозненных небольших автоматизированных систем, не согласованных друг с другом. Обычно такой вид автоматизации вызван непониманием руководства предприятия преимуществ комплексной автоматизации в долгосрочной перспективе, которое приведет к экономии средств на внедрение автоматизированных и информационных систем. В итоге приобретаются самые необходимые системы, которые опять же нагромождаются в набор несвязанных друг с другом элементов.

При полном (комплексном) подходе предприятие рассматривается как сложная система взаимосвязанных компонентов, все «узкие» места которой необходимо автоматизировать для повышения общей эффективности системы.

Программное обеспечение для работы с базами данных используется на персональных компьютерах уже довольно давно. К сожалению, эти программы либо были элементарными диспетчерами хранения данных и не имели средств разработки приложений, либо были настолько сложны и трудны, что даже хорошо разбирающиеся в компьютерах люди избегали работать с ними до тех пор, пока не получали полных, ориентированных на пользователя приложений.

Деятельность предприятия автоматизируется при помощи построения интегрированной автоматизированной системы общего делового процесса предприятия, который может состоять из множества взаимосвязанных сложным образом технологических, производственных и управленческих процессов.

Система должна обеспечивать полный контроль, автоматизированный учёт и анализ защиты персональной информации, позволять уменьшить время обслуживания клиентов, получать информацию о кодах защиты информации и персональных данных.

Для формирования требования к разрабатываемой системе, необходимо сформировать требования к организации БД, информационной совместимости к разрабатываемой системе.

При решении проблемы защиты информации в КС необходимо учитывать еще и противоречивость человеческого фактора. Обслуживающий персонал и пользователи могут быть как объектом, так и источником несанкционированного воздействия на информацию.

Таким образом, компьютерная система как объект защиты представляет собой совокупность следующих взаимосвязанных компонентов:

• информационных массивов, представленных на различных машинных носителях;

• технических средств обработки и передачи данных (компьютерных и телекоммуникационных средств);

• программных средств, реализующих соответствующие методы, алгоритмы и технологию обработки информации;

• обслуживающего персонала и пользователей системы, объединенных по организационному, предметно-тематическому, технологическому и другим принципам для выполнения автоматизированной обработки информации (данных) с целью удовлетворения информационных потребностей субъектов информационных отношений. В данном случае, ИС содержит данные о сотрудниках фирмы. Одной из технологий, которая существенно иллюстрирует работу информационной системы, является разработка схемы документооборота для документов. В предлагаемой информационной системе основным документом является заявка на получение доступа к персональным данным. Разрабатываемая система должна обеспечивать полный контроль, автоматизированный учёт и анализ защиты персональной информации, позволять уменьшить время обслуживания клиентов, получать информацию о кодах защиты информации и персональных данных.

При полном (комплексном) подходе предприятие рассматривается как сложная система взаимосвязанных компонентов, все «узкие» места которой необходимо автоматизировать для повышения общей эффективности системы.

Деятельность предприятия ОАО «Альфа банк» автоматизируется при помощи построения автоматизированной

системы позволяющей обеспечивать защиту персональных данных,в виде типовой вычислительной сети (рис. 2).

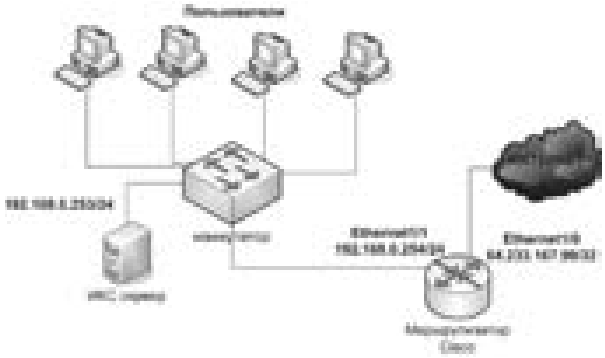


Рисунок 2 – Типовая защищенная локальная компьютерная сеть структурного подразделения банка

В связи с отсутствием достаточного количества средств для проведения комплексной защиты системы автоматизация типового банка целесообразно обеспечить безопасность персональных данных последовательно с учетом значимости различных подразделений банка, например:

- отдел кредитования;
- служба безопасности банка;
- бухгалтерия;
- отдел по работе с корпоративными клиентами и т.д.

Литература

1. Архангельский А.Я. 100 компонентов общего назначения библиотеки Delphi 5. — М.: Бином, 2011. — 266 с.
2. Конноли Томас, Бегг Каролин. Базы данных. Проектирование, реализация и сопровождение. Теория и практика. — М.: Вильямс, 2010. – 1111 с.
3. Базы данных: модели, разработка, реализация / Карпова Т.- СПб.: Питер, 2011. –304с.
4. Галатенко В. Информационная безопасность // Открытые системы- 2011. – N 1-4.
5. Волков В. Ф. Экономика предприятия. – М.: Вита-Пресс, 2009. – 380с.
6. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Некоторые перспективы применения систем контроля и управления доступом в

региональных ВУЗАХ. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
7. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Развитие сотрудничества российских и зарубежных ВУЗОВ по защите информационного ресурса. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
8. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
9. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
10. Соляной В.Н., Сухотерин А.И Выработка коммуникативной компетенции при подготовке профессионалов по информационной безопасности с использованием технологии модерации. «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7

11. Соляной В.Н., Сухотерин А.И, Антоненко В.И. Проблемно-ориентированная подготовка специалистов по информационной безопасности с использованием имитационного метода (мозговой штурм). «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. – М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7.

НАПРАВЛЕНИЯ РАЗВИТИЯ СОВРЕМЕННЫХ DLP – СИСТЕМ

Беляева Наталья Андреевна, студентка 4 курса кафедры Информационной безопасности
Научный руководитель: **Соляной Владимир Николаевич,** к.воен.н., доцент, заведующий кафедрой Информационной безопасности

Эффективность бизнеса во многих случаях зависит от сохранения конфиденциальности, целостности и доступности информации. В настоящее время одной из наиболее актуальных угроз в области информационной безопасности является утечка конфиденциальных данных от несанкционированных действий пользователей. При решении подобных задач нам на помощь приходят DLP – системы. Сегодня рынок DLP-систем является одним из самых быстрорастущих и быстроразвивающихся среди всех средств обеспечения информационной безопасности с десятками различных направлений развития.

Интернет, инсайдеры, утечка информации, DLP-системы, развитие.

DEVELOPMENT TRENDS OF DLP-SYSTEMS

Belyaeva Natalia, 4th year student of the Department of information security
Scientific adviser: **Solyanoi Vladimir,** Candidate of Military Sciences, Associate Professor, Head of the Department of information security

Business effectivy in many cases depends on confidentiality, integrity and availability of information. Currently, one of the most pressing threats to information security is a leak of confidential data from unauthorized user activity. In solving these problems, we come to the aid DLP - system. Today the market of DLP-systems is one of the fastest growing among all

means of information security with dozens of different areas of development.

Internet, insiders, leaking information, DLP- system, development.

В последнее время проблема защиты от внутренних угроз стала настоящим вызовом понятному и устоявшемуся миру корпоративной ИБ.

Прежде всего, стоит определить, что угроза конфиденциальности данных является внутренней, если ее источником является сотрудник предприятия или какое-либо другое лицо, имеющее легальный доступ к этим данным. Таким образом, когда мы говорим о внутренних угрозах, мы говорим о каких-либо возможных действиях легальных пользователей, умышленных или случайных, которые могут привести к утечке конфиденциальной информации за пределы корпоративной сети предприятия. Для полноты картины стоит добавить, что таких пользователей часто называют инсайдерами, хотя этот термин имеет и другие значения [1-10].

Аналитический центр компании InfoWatch представил глобальное исследование утечек конфиденциальной информации за 2014 год. По данным отчета (Рис. 1), по сравнению с прошлым годом число утечек информации в мире выросло на 22%, в России – на 73%

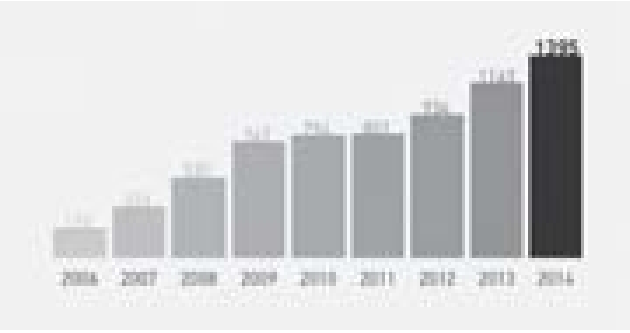


Рисунок 1 - Число утечек информации по годам

В большинстве случаев (73%) информация утекала по вине внутреннего нарушителя, как правило, рядового сотрудника, бывшего или нынешнего [7].

Большинство утечек в 2014 г. пришлось на три основных канала (Рисунок 2): Интернет (35%), бумажные документы (18%) и

кража/потеря оборудования (16%). При этом умышленные утечки чаще всего происходят через Интернет, а случайные – в результате потери или кражи оборудования [5].

Существует ряд программ, позволяющих проводить мониторинг действий пользователя в сети, таких как Spector 360, однако наиболее популярным и приемлимым решением на сегодняшний день, является использование DLP-систем.

Рисунок 2 - Каналы утечки информации

Термин защита от утечек (data loss prevention, DLP) появился в лексиконе специалистов по ИБ сравнительно недавно, и уже успел стать, без преувеличения, самой горячей темой последних лет. Как правило, аббревиатурой DLP обозначают системы, контролирующие возможные каналы утечки и блокирующие их в случае попытки пересылки по этим каналам какой-либо конфиденциальной информации. Кроме этого, в функции подобных систем часто входит возможность архивирования проходящей по ним информации для последующего аудита, расследования инцидентов и ретроспективного анализа потенциальных рисков [2].

Одной из основных проблем при реализации и внедрении DLP-систем является способ детектирования конфиденциальной информации, то есть, момент принятия решения о том, является ли передаваемая информация конфиденциальной и основания, которые учитываются при принятии такого решения. Как правило, для этого производится анализ содержимого передаваемых документов, называемый также контентным анализом. Рассмотрим основные подходы к детектированию конфиденциальной информации:

- Метки. В документы внедряются метки, описывающие степень конфиденциальности информации, что можно делать с этим документом, и кому посылать. По результатам анализа меток система

DLP принимает решение, можно ли данный документ отправить наружу или нельзя.

- Сигнатуры. Данный метод заключается в задании одной или нескольких последовательностей символов, наличие которых в тексте передаваемого файла должно говорить DLP-системе о том, что этот файл содержит конфиденциальную информацию.
- Метод Байеса. Данный метод, применяемый при борьбе со спамом, может успешно применяться и в системах DLP. Для применения этого метода создается список категорий, и указываются список слов с вероятностями того, что если слово встретилось в файле, то файл с заданной вероятностью принадлежит или не принадлежит к указанной категории.
- Морфологический анализ. Метод морфологического анализа аналогичен сигнатурному, отличие заключается в том, что анализируется не 100% совпадение с сигнатурой, а учитываются также однокоренные слова.
- Цифровые отпечатки. Суть данного метода заключается в том, что для всех конфиденциальных документов вычисляется некоторая хэш-функция таким образом, что если документ будет незначительно изменен, хэш-функция останется такой же, или тоже изменится незначительно.
- Регулярные выражения. Известные всем, кто имел дело с программированием, регулярные выражения позволяют легко находить в тексте шаблонные данные, например, телефоны, паспортные данные, номера банковских счетов, номера социального страхования и т.д.

Из приведенного списка легко заметить, что методы детектирования либо не гарантируют 100% определения конфиденциальной информации, поскольку уровень ошибок как первого, так и второго рода в них достаточно высок, либо требуют постоянного бдения службы безопасности для обновления и поддержания в актуальном виде списка сигнатур или присваивания меток конфиденциальным документам [1].

Состав современного комплексного DLP-решения, должен содержать следующие компоненты, которые представлены на рис. 3:

- *Защита на уровне сети* - предотвращение утечек информации по сети (SMTP, HTTP, HTTPS, IM и сетевая печать). Как правило, это мониторинг и/или блокирование исходящего трафика на

уровне интернет-шлюза, но есть и попытки переноса функций контроля трафика на уровень рабочих станций.

- *Защита конечных точек* - предотвращение утечек информации через подключаемые устройства (USB, HDD/CD/DVD, WiFi/Bluetooth, локальная печать и т.д.). Мониторинг и/или блокирование попыток копирования информации на внешние устройств, снятие теневых копий "сливаемой" информации.
- *Шифрование* - дополнительный уровень защиты мобильных носителей на случай их потери или кражи. Даже если носитель попадет к злоумышленнику, то данные на нем будут надежно зашифрованы.
- *Платформа управления, хранения информации об инцидентах и ее анализа* - управление политиками безопасности, сбор и хранение деталей инцидентов для дальнейшего анализа офицером безопасности или передачи доказательной базы в судебные органы [4].

Рисунок 3 – Концепция современной защиты от утечек

Если на уровне конечных точек в самом простейшем случае можно обойтись просто политиками работы с внешними устройствами, то на уровне сети все гораздо сложнее - утечку нужно обнаружить в потоке трафика. Здесь мы как раз упираемся в различия существующих технологий, как по их эффективности, так и по области применимости. На рис. 4 приведено условное разделение существующих технологий обнаружения утечек на несколько поколений по их эффективности. В первое поколение попали самые примитивные технологии - детектирование по ключевым словам, регулярным выражениям и словарям. Во второе - все существующие в настоящее время на рынке технологии - лингвистический анализ,

цифровые отпечатки, цифровые метки, контекстный анализ. Третье поколение - это гибридный анализ, который совмещает в себе несколько различных технологий второго поколения [8].

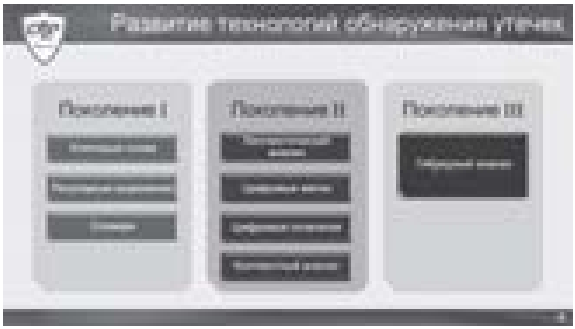


Рисунок 4 – Развитие технологий обнаружения утечек

Различные технологии обнаружения утечек по-разному эффективны для различных категорий информации. Ключевым разделением здесь является новизна конфиденциальной информации и ее изменяемость со временем. Поэтому рассматривать эффективность различных технологий стоит в разрезе защиты статических (например, медиа-файлы, исходные коды программ, старые и редко изменяемые документы) и динамических данных (e-mail, IM, сообщения в форумах, блогах, новейшие и активно изменяемые на этапе подготовки документы). Представленные сегодня на рынке DLP-продукты используют различные технологии второго поколения, а значит по-разному эффективны для предотвращения утечек статических или динамических данных. На рис. 5 наглядно видно, что цифровые отпечатки и метки более эффективны для предотвращения утечек статических данных, в то время как лингвистика и контекстный анализ лучше справляется с утечками динамических данных. Эффективность гибридного анализа, например, если он включает в себя технологии цифровых отпечатков и контекстного анализа, не зависит от типа защищаемых данных.

Он становится одинаково эффективен для защиты как динамической, так и для статической конфиденциальной информации. Его эффективность должна быть даже выше за счет синергетического эффекта от интеграции нескольких технологий (рисунок 6).

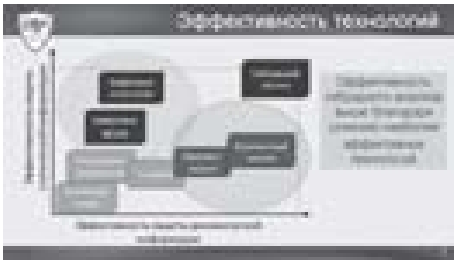


Рисунок 5 – Эффективность технологий анализа DLP – систем

Напомню, что технология цифровые отпечатков используется в продуктах Websense DSS или Symantec DLP, цифровые метки в McAfee Host DLP, а лингвистический и контекстный анализ - в продуктах InfoWatch или SearchInform [8].

Рисунок 6 – Развитие технологий DLP

В перспективе гибридные анализ в DLP-системах должен включать в себя три ключевые составляющие:

- Детектор объектов на базе регулярных выражений (детектор кредитных карт, счетов, номеров паспортов и т.п.).
- Защита статических данных на базе цифровых отпечатков (реактивная защита).
- Защита новых и динамических данных на базе контентного и контекстного анализа (проактивная защита).

Таким образом, на смену множеству разрозненных и неполноценных по отдельности технологий придет гибридный анализ, эффективный на всем жизненном цикле конфиденциальной информации.

Другими вариантами возможного развития следует рассматривать следующие направления.

Во-первых, сближение функционала DLP с системами контроля использования сотрудниками рабочего времени. Появление подобного функционала было предрешено: все исходные данные в системе уже есть (перечень запускаемых программ, снимки экранов,

журналы ввода данных и обращений к ресурсам сети Интернет и т. д.), необходимы только небольшой «модуль анализа» и интерфейс. В некоторых современных DLP- системах этот функционал уже реализован или его реализация анонсирована.

Во-вторых - модули для интеграции со сложными корпоративными системами. Интеграция с корпоративными системами (на базе 1С, SAP, Lotus и др.) позволит повысить уровень информационной безопасности без внесения доработок в эксплуатируемые системы.

Модуль может реализовать ведение подробных журналов действий пользователей (когда и с какой информацией работал, как долго, с какого рабочего места, копировал ли информацию), сопоставлять активность пользователя в корпоративных системах и отправку данных на внешнюю электронную почту или копирование на внешний носитель, оценивать общую осведомленность сотрудника по отдельным вопросам за длительный период [6].

В-третьих - расширение перечня поддерживаемых платформ. Прежде всего, это поддержка мобильных платформ (различные версии iOS и Android имеют максимальный приоритет), которые все глубже проникают в корпоративную среду. Потребность в контроле мобильных устройств будет только возрастать.

В-четвёртых - анализ голоса и интеграция с традиционной телефонией. DLP-системы уже располагают агентами для перехвата трафика клиентов IP-телефонии, агентами для работы с микрофоном.

Существующие модули распознавания речи, в зависимости от используемых алгоритмов, могут:

- выполнять идентификацию абонентов по голосу;
- оценивать по интонациям эмоциональное состояние собеседников;
- восстанавливать, с определенными ограничениями, стенограмму беседы.

В – пятых, анализ поведения пользователей (для идентификации и выявления аномалий). Поведенческий анализ позволит выявлять случаи, когда кто-то работает с чужими учетными данными или использует чужое оборудование, выполняет нетипичные действия.

В - шестых, сближение или интеграция с IDM-системами. Управление учетными данными (IDM) тесно связано с задачами DLP. Интеграция с базами данных службы персонала, системами электронных проходных и др. позволит поднять качество работы на новый,

более высокий уровень [8].

В – седьмых, сближение или интеграция с IDS-системами. Интеграция в DLP некоторых свойств систем обнаружения вторжений (IDS) как в виде собственной реализации, так и путем использования функционала существующих решений (OpenSource версии Snort или Suricata), позволит выявлять нестандартные каналы утечки информации, такие как DNS-, ICMP- и SMTP-туннелирование.

В – восьмых, встроенный VPN. Функционал VPN необходим, главным образом, для защиты от перехвата информации, передаваемой соответствующими агентами. В ситуации, когда агенты перехвата установлены на мобильных устройствах, без VPN персоналу невозможно организовать безопасную передачу данных через открытые каналы связи в свою организацию. В некоторых DLP-системах функционал VPN уже присутствует.

В – девятых, коробочные решения для организаций малого и среднего бизнеса. Для организаций малого и среднего бизнеса, где сложно выделить финансовые и людские ресурсы на внедрение и обслуживание полноценной DLP-системы, удобен более простой продукт с невысокой стоимостью [7].

В – десятых, атаки на DLP-системы. Вполне возможно появление инструментов для проведения атак на DLP-системы. Атаки могут быть направлены на различные ее компоненты от анализаторов протоколов до хранилища. Типы атак также могут варьироваться от простого отказа в обслуживании до подделки управляющих сообщений, заражения вредоносным кодом и получения управления всей системой или отдельными компонентами.

В – одиннадцатых, сторонние разработки. Помимо, собственно, DLP-систем, могут появляться и развиваться сторонние программные продукты, которые будут использовать DLP-системы как источник данных [3].

Таким образом, в настоящей статье были очерчены наиболее перспективные, на наш взгляд, направления развития DLP-систем:

- расширение перечня поддерживаемых платформ;
- модули для интеграции со сложными корпоративными системами;
- анализ голоса и интеграция с современной телефонией;
- анализ поведения пользователя, сближение и интеграция с IDM- и IDS-системами;
- встроенный VPN и некоторые другие направления.

Особенно стоит выделить развитие гибридных DLP-систем. Гибридный анализ конфиденциальности информации наиболее перспективный и точный вид анализа, входящий в третье поколение технологий обнаружения утечек информации. Какие именно из перечисленных направлений развития в итоге будут иметь приоритет, а какие так и останутся нереализованными, будет зависеть от запросов заказчиков и, несомненно, умения специалистов по маркетингу убедить заказчиков в необходимости приобретения модулей с новыми функциональными возможностями.

Литература

1. Эдуард Гордеев, Александр Астахов, «Как организовать эффективную систему предотвращения утечки конфиденциальной информации из коммерческой организации» М.: ООО «СамИздат», 2008
2. Майкл А. Лектер, «Защити свой главный актив», М.: ООО «Попурри», 2004
3. Машечкин И. В., Петровский М. И., Трошин С. В. Мониторинг и анализ поведения пользователей компьютерных систем //УкрПРОГ'2008: шестая международная конференция по программированию, Украина, К.: 2008.: Сборник докладов.
4. В.Ю. Станкевич, «Обзор DLP-систем». Технологии безопасности, No3, 2011.
5. Дэн Яхин, «InfoWatch: Многоуровневый подход к обнаружению и предотвращению утечек информации», whitepaper, 2005
6. Информационно-методический журнал Inside, №2 2015, статья «Направление развития DLP-систем»
7. nahna, «Защита информации от инсайдеров с помощью программных средств», SecurityLab.ru, 2007
8. http://www.anti-malware.ru/dlp_hybrid статья «С утечками данных будут бороться гибридные технологии» 10.06.2009
9. Соляной В.Н., Сухотерин А.И. Модульно-ориентированный подход формирования базовых дисциплин ФГОС ВО 3+ как основа реализации профессиональной подготовки бакалавров в области информационной безопасности Научно-практический журнал №25, том 2 2015г. Информационное противодействие угрозам терроризма Материалы XIX Пленума учебно-методического объединения по образованию в области информационной безопасности «учебно-методическое обеспечение образовательных программ в области

информационной безопасности» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН.ФЕД.УНИВ, 2015.-332 с. ISSN 2219-8792
10. Соляной В.Н., Сухотерин А.И. Становление направления «Радиоэлектронная безопасность информационных объектов» в системе дополнительного профессионального по информационной безопасности. Научно-практический журнал №25, том 2 2015г. Информационное противодействие угрозам терроризма Материалы XIX Пленума учебно-методического объединения по образованию в области информационной безопасности «учебно-методическое обеспечение образовательных программ в области информационной безопасности» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН.ФЕД.УНИВ, 2015.-332 с. ISSN 2219-8792

АНАЛИЗ СОВРЕМЕННЫХ СТАНДАРТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Бородулина Анна Алексеевна, студентка 1 курса кафедры Информационной безопасности
Научный руководитель: **Соляной Владимир Николаевич,** к.воен.н., доцент, заведующий кафедрой Информационной безопасности

Информационная безопасность в настоящее время играет огромную роль в области высоких технологий, где информация (особенно цифровая) становится как "продукт и сырье". Её производят, используют, продают, и, к сожалению, часто крадут. С постоянно растущими задачами в области информационной безопасности в современном информационном обществе (государстве) усиливается потребность в разработке и принятии специальных требований защиты данных. Такие требования действуют по стандартам информационной безопасности.

Информационная безопасность, технологии, защита информации, стандарты информационной безопасности.

ANALYSIS OF MODERN STANDARDS INFORMATION SECURITY

Borodulina Anna, 1st year student of the Department of information security
Scientific adviser: **Solaynoy Vladimir,** Candidate of Military Sciences, Associate Professor, Head of the Department of information security

Information security now play a huge role in the field of high technology, where it is the information (especially digital) becomes both

"product and raw materials". Its manufacture, process, sell, and, unfortunately, often steal. With an ever-increasing tasks in the field of information security in the modern information society (state) amplifies the need for developed and adopted by the special requirements of data protection. As such claims just the same and act on information security standards.

Information security, technology, protection of information, information security standards.

Стандарты информационной безопасности – это обязательные или рекомендуемые к выполнению документы, в которых определены подходы к оценке уровня ИБ и установлены требования к безопасным информационным системам. Стандарты в области информационной безопасности выполняют следующие важнейшие функции:

- выработка понятийного аппарата и терминологии в области информационной безопасности;
- формирование шкалы измерений уровня информационной безопасности;
- согласованная оценка продуктов, обеспечивающих информационную безопасность;
- повышение технической и информационной совместимости продуктов, обеспечивающих ИБ;
- накопление сведений о лучших практиках обеспечения информационной безопасности и их предоставление различным группам заинтересованной аудитории – производителям средств ИБ, экспертам, ИТ-директорам, администраторам и пользователям информационных систем;
- функция нормотворчества – придание некоторым стандартам юридической силы и установление требования их обязательного выполнения.

Стандарты информационной безопасности имеют несколько классификаций (рис.1).

Более подробно целесообразно рассмотреть классификацию современных стандартов по территории их распространения. В соответствии с *международными* и *национальными* стандартами обеспечение информационной безопасности в любой компании предполагает следующее:

•определение целей обеспечения информационной безопасности систем;

•создание эффективной системы управления информационной безопасностью;

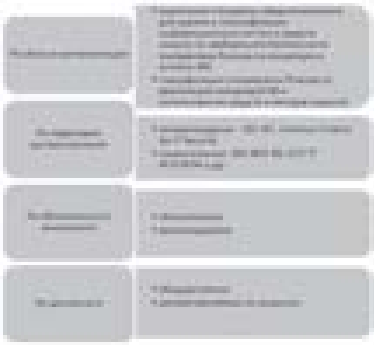


Рисунок 1 - Классификация стандартов ИБ

• расчет совокупности детализированных качественных и количественных показателей для оценки соответствия информационной безопасности целям;

• применение инструментария обеспечения информационной безопасности и оценки ее текущего состояния;

• использование методик управления безопасностью, позволяющих объективно оценить защищенность информационных активов и управлять информационной безопасностью компании.

Международные стандарты широко используются во всём мире. Можно выделить несколько уровней их применения:

1. Применение МСФО в качестве национальных стандартов.

2. Национальные организации по разработке стандартов финансовой отчетности используют МСФО как ориентир для разработки собственных стандартов (большинство развитых стран и постоянно растущее число развивающихся стран и стран с переходной экономикой).

3. Фондовые биржи и регулирующие органы, обязывающие или разрешающие компаниям предоставлять консолидированную финансовую отчётность в соответствии с МСФО (среди них практически все ведущие биржи в мире: Нью-Йоркская фондовая биржа, NASDAQ, Лондонская, Токийская и Франкфуртская биржи – всего около 70 фондовых бирж из 50 стран мира). Примерно в половине случаев основной причиной применения МСФО называется

необходимость привлечения финансирования на международных рынках капитала.

4. Наднациональные организации, например, Европейский Союз, который заявил о введении МСФО с 2005 года для компаний, котирующихся на международных фондовых рынках; некоторые организации используют МСФО при составлении своей отчётности (Европейский банк реконструкции и развития, Международная организация комиссий по ценным бумагам, Международный Олимпийский комитет, ОЭСР, Мировой Банк).

5. Сами компании – по информации КМФСО в настоящее время уже около тысячи компаний предоставляют финансовую отчётность в полном соответствии с МСФО, что подтверждено аудиторским заключением. Среди них такие гиганты как Microsoft, Nestle, Allianz, ENI, Nokia, Air France, Renault, Deutsche Bank, Olivetti, Roche, Fiat, Volkswagen, Lufthansa, Adidas и т.д.

Рассмотрим наиболее известные международные стандарты в области защиты информации, которые могут быть использованы в отечественных условиях. Международный стандарт ISO/IEC 17799:2000 (BS 7799-1:2000) «Управление информационной безопасностью — Информационные технологии» («Information technology — Information security management*) является одним из наиболее известных стандартов в области защиты информации. Данный стандарт был разработан на основе первой части Британского стандарта BS 7799—1:1995 «Практические рекомендации по управлению информационной безопасностью» («lnformation security management — Part 1: Code of practice for information security management*) и относится к новому поколению стандартов информационной безопасности компьютерных ИС. Текущая версия стандарта ISO/IEC 17799:2000 (BS 7799—1:2000) рассматривает следующие актуальные вопросы обеспечения информационной безопасности организаций и предприятий:

- необходимость обеспечения информационной безопасности;
- основные понятия и определения информационной безопасности;
- политика информационной безопасности компании;
- организация информационной безопасности на предприятии;
- классификация и управление корпоративными информационными ресурсами;
- кадровый менеджмент и информационная безопасность;

- физическая безопасность;
- администрирование безопасности КИС;
- управление бизнес-процессами компании с точки зрения информационной безопасности;
- внутренний аудит информационной безопасности компании.

Национальный стандарт Российской Федерации — стандарт, утвержденный национальным органом Российской Федерации по стандартизации. Вид стандарта — характеристика, определяющаяся его содержанием в зависимости от объекта стандартизации. ГОСТ Р 1.0 установил следующие основные виды стандартов (рис.2).

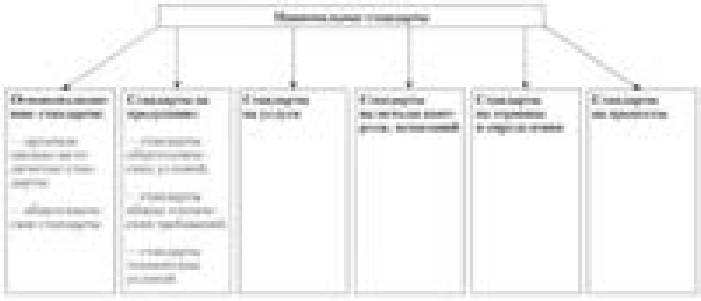


Рисунок 2 - Виды национальных стандартов по ИБ

Современные стандарты в области информационной безопасности базируются на качественном подходе. В пример достаточно привести банковское предприятие, которое как раз таки и держится на том, чтобы вся информация стояла под защитой. Иначе последовали бы неблагоприятные последствия. Банковская сфера РФ держится на четырёх основных составляющих:

1. Стратегия ИБ;
2. Концепция ИБ;
3. Политика ИБ;
4. Регламент ИБ.

Международные стандарты в области информационной безопасности приобрели такие черты, как стратегию, регламент и концепцию. Здесь используется количественно-качественный подход эффективности информационной безопасности (в этом заключается положительная сторона международных стандартов). Национальные же стандарты – политику и регламент. Положительность этих стандартов в том, что используется качественно-колличественный

подход эффективности ИБ. На основе этого можно сделать вывод о том, что современной науке необходимо вырабатывать навыки стратегии, а также политики для усовершенствования стандартов и эффективности работы на любых предприятиях.

Литература

1. Галатенко В.А. Стандарты информационной безопасности –М.: Гелиос, 2004.
2. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации 2-е изд. стер. –М.: Гелиос,2008.
3. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Некоторые перспективы применения систем контроля и управления доступом в региональных ВУЗАХ. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУЗов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
4. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Развитие сотрудничества российских и зарубежных ВУЗОВ по защите информационного ресурса. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУЗов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
5. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
6. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях.

Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
7. Соляной В.Н., Сухотерин А.И Выработка коммуникативной компетенции при подготовке профессионалов по информационной безопасности с использованием технологии модерации. «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7
8. Соляной В.Н., Сухотерин А.И, Антоненко В.И. Проблемно-ориентированная подготовка специалистов по информационной безопасности с использованием имитационного метода (мозговой штурм). «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7.
9. Ярочкин В.И. Информационная безопасность 5-е изд.- М.: Мир, 2010.

ОСОБЕННОСТИ ПРИМЕНЕНИЯ КВАНТОВОЙ КРИПТОГРАФИИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Васильев Сергей Юрьевич, Эпельфельд Иван Ильич, студенты 3 курса кафедры Информационной безопасности
Научный руководитель: **Сухотерин Александр Иванович**, к.воен.н., доцент кафедры Информационной безопасности

Квантовые компьютеры и связанные с ними технологии в последнее время становятся все актуальнее. Исследования в этой области не прекращаются уже десятилетия, и ряд революционных достижений налицо. Квантовая криптография - одно из них.

Как известно, одним из ключевых вопросов обеспечения безопасности информации, хранимой и обрабатываемой в информационных системах, а также передаваемой по линиям связи является защита ее от несанкционированного доступа. Для защиты

информации применяются различные меры и способы, начиная с организационных и кончая применением сложных программно-аппаратных комплексов.

Одним из путей решения проблемы защиты информации, а точнее - решения небольшой части вопросов из всего спектра мер защиты, является криптографическое преобразование информации, или шифрование.

Информационная безопасность, квантовая криптография, квантовое шифрование, крипто анализ, шифротекст.

FEATURES OF THE APPLICATION OF QUANTUM CRYPTOGRAPHY IN THE FIELD OF INFORMATION SECURITY

Vasilyev Sergey, Epelfeld Ivan, 3d year students of the Department of information security
Scientific adviser: **Sukhoterin Alexander,** Candidate of Military Sciences, Associate Professor of the Department of information security

Quantum computers and related technology have recently become more urgent. Research in this area do not stop for decades, and a number of breakthroughs there. Quantum cryptography - one of them.

As you know, one of the important issue of security of information stored and processed in information systems and transmitted over the communication lines is to protect it from unauthorized access. Various measures and methods used for the protection of information, starting with the organizational and ending the use of complex software and hardware systems.

One way to solve the problem of information security - or rather, a small part of the solution of the issues of the entire spectrum of protection measures is a cryptographic transformation of the information, or encryption

Information security, quantum cryptography, quantum encryption, crypto analysis of the ciphertext.

Криптография - это наука о шифрах. Она представляет собой огромное количество методов изменения открытого сообщения для того, чтобы передаваемое сообщение стало бесполезным для криптоаналитика.

Основным достоинством квантовых методов шифрования является то, что они обеспечивают высокую гарантированную стойкость защиты, которую можно рассчитать и выразить в числовой форме (средним числом операций или временем, необходимым для раскрытия зашифрованной информации или вычисления ключей).

Сущность технологии квантового шифрования

Основным видом криптографического преобразования информации является шифрование. Под шифрованием понимается процесс преобразования открытой информации в зашифрованную информацию (шифртекст) или процесс обратного преобразования зашифрованной информации в открытую. Процесс преобразования открытой информации в закрытую получил название зашифровывание, а процесс преобразования закрытой информации в открытую - расшифровывание.

Современные методы шифрования должны отвечать следующим требованиям:

-стойкость шифра противостоять криптоанализу (криптостойкость) должна быть такой, чтобы вскрытие его могло быть осуществлено только путем решения задачи полного перебора ключей;

-криптостойкость обеспечивается не секретностью алгоритма шифрования, а секретностью ключа;

-шифртекст не должен существенно превосходить по объему исходную информацию;

-ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации;

-время шифрования не должно быть большим;

-стоимость шифрования не должная превышать стоимость зашифровываемой информации.

В качестве примера удачного метода шифрования можно привести шифры DES (Data Encryption Standard), применяемый в мире, а так же отечественный стандарт шифрования данных ГОСТ 28147-89. Алгоритм шифрования не является секретным и был опубликован в открытой печати. За все время использования этого шифра не было обнародовано ни одного случая обнаружения слабых мест в алгоритме шифрования [1, 2, 13-15].

В результате развития квантовых компьютеров на свет появлялось квантовое шифрование. Оно обладает неоспоримыми преимуществами. Возьмем, к примеру, известный шифр RSA (Rivest,

Shamir, Adleman). В основе системы RSA лежит предположение о том, что решение математической задачи о разложении больших чисел на простые множители на классических компьютерах невозможно - оно требует экспоненциально большого числа операций и астрономического времени. Для решения этой задачи был разработан квантовый алгоритм, который дает возможность вычислить простые множители больших чисел за практически приемлемое время и взломать шифр RSA. Процедура квантового шифрования может быть применена ко всем классическим шифросистемам. Остается только создать квантовый компьютер достаточной мощности.

Хотелось бы отметить, что последние разработки в области квантового шифрования позволяют создавать системы, обеспечивающие практически 100%-ю защиту ключа и ключевой информации. Используются все лучшие достижения по защите информации как из классической криптографии, так и из новейшей "квантовой" области, что позволяет получать результаты, превосходящие все известные криптографические системы. Можно с уверенностью говорить, что в ближайшем будущем вся криптографическая защита информации и распределение ключей будут базироваться на квантово-криптографических системах [1, 2, 12-15].

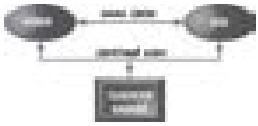


Рисунок 1 – Схема работы симметричных криптосистем

Симметричная криптосистема генерирует общий секретный ключ и распределяет его между доверенными пользователями. С помощью этого ключа производится как шифрование, так и дешифрование сообщения.

В технологии симметричных ключей абоненты используют один и тот же ключ, как для шифрования, так и для расшифровывания данных.

Следует выделить следующие преимущества криптографии с симметричными ключами:

- относительно высокая производительность алгоритмов;
- высокая криптографическая стойкость алгоритмов на

единицу длины ключа.

К недостаткам криптографии с симметричными ключами следует отнести:

- необходимость использования сложного механизма распределения ключей;
- технологические трудности обеспечения безотказности [1, 8-15].

Асимметричные криптосистемы предполагают использование двух ключей - открытого и секретного.

В таких системах для зашифровывания сообщения используется один ключ, а для расшифровывания - другой.

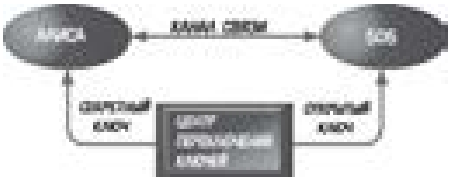


Рисунок 2 – Схема работы ассиметричных криптосистем

Асимметричные криптосистемы используют для работы два ключа. Первый, открытый, доступен всем пользователям системы, с помощью которого зашифровывается сообщение. Второй, секретный, должен быть известен только получателю сообщений.

Первый ключ является открытым и может быть опубликован для использования всеми пользователями системы, которые зашифровывают данные. Расшифровывание сообщения с помощью открытого ключа невозможно. Для расшифровывания данных получатель зашифрованного сообщения применяет второй ключ, секретный. Ключ расшифровывания не может быть определен из ключа зашифровывания [1-15].

Безопасность любого криптографического алгоритма определяется используемым криптографическим ключом. Для получения ключей используются аппаратные и программные средства генерации случайных значений ключей. Как правило, применяют датчики псевдослучайных чисел. Однако степень случайности генерации чисел должна быть достаточно высокой.

Важной задачей при работе с ключами является их распределение. В настоящее время известны два основных способа

распределения ключей: с участием центра распределения ключей и прямой обмен ключами между пользователями.

Подводя итоги, можно сказать, что квантовые методы шифрования обеспечивают безопасность на достаточно высоком уровне. Несомненно, что данное направление будет быстро развиваться с появлением новых коммуникационных аппаратно-программных средств [1-10].

Из всего изложенного следует, что надежная криптографическая система на квантовой основе должна удовлетворять таким требованиям:

- процедуры зашифровывания и расшифровывания должны быть "прозрачны" для пользователя;
- дешифрование закрытой информации должно быть максимально затруднено;
- содержание передаваемой информации не должно сказываться на эффективности криптографического алгоритма;

В процессе эксплуатации системы квантовой криптографии специалист по ИБ может столкнуться с такими проблемами, как:

- значительные затраты ресурсов (времени, производительности процессоров) на выполнение криптографических преобразований информации;
- трудности совместного использования зашифрованной (подписанной) информации, связанные с управлением ключами (генерация, распределение и т.д.);
- высокие требования к сохранности секретных ключей и защиты открытых ключей от подмены.

На сегодняшний день криптография применяется практически во всех отраслях человеческой деятельности, что является немаловажной задачей в более детальном ее изучении и дальнейшем развитии.

Литература

1. А. Корольков, Квантовая криптография, или как свет формирует ключи шифрования. Компьютер в школе, № 7, 1999
2. Алферов А.П. Основы Криптографии/ А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин -- М.: Гелиос, 2005., с.5 - 53.
3. A.K. Ekert, " Quantum Cryptography Based on Bell's Theorem", Phys. Rev. lett. 67, 661 (2000).

4. Квантовая криптография: [Электронный ресурс] // Re-Tech. URL: http://www.re-tech.narod.ru/inf/crypto/qq.htm /
5. Квантовая криптография (шифрование): [Электронный ресурс] // TADVISTER. URL: http://www.tadviser.ru/index.php
6. «Технологический университет делится опытом информационной безопасности». Газета «Подмосковье» от 13 марта 2015 года. Пятница. №43 (3468).
7. Соляной В.Н., Сухотерин А.И. Практика применения инновационного научно-образовательного комплекса по подготовке бакалавров и магистров в области информационной безопасности. Научно-практический журнал №25, том 1 2015г. Информационное противодействие угрозам терроризма. материалы XIX пленума учебно-методического объединения по образованию в области информационной безопасности «опыт и передовые практики образовательных организаций по формированию и использованию в учебном процессе специализированной учебно- лабораторной базы» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН.ФЕД.УНИВ, 2015.-416 с. ISSN 2219-8792
8. Соляной В.Н., Сухотерин А.И. Модульно-ориентированный подход формирования базовых дисциплин ФГОС ВО 3+ как основа реализации профессиональной подготовки бакалавров в области информационной безопасности Научно-практический журнал №25, том 2 2015г. Информационное противодействие угрозам терроризма Материалы XIX Пленума учебно-методического объединения по образованию в области информационной безопасности «учебно-методическое обеспечение образовательных программ в области информационной безопасности» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН.ФЕД.УНИВ, 2015.-332 с. ISSN 2219-8792
9. Соляной В.Н., Сухотерин А.И. Становление направления «Радиоэлектронная безопасность информационных объектов» в системе дополнительного профессионального по информационной безопасности. Научно-практический журнал №25, том 2 2015г. Информационное противодействие угрозам терроризма Материалы XIX Пленума учебно-методического объединения по образованию в области информационной безопасности «учебно-методическое обеспечение образовательных программ в области информационной безопасности» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН.ФЕД.УНИВ, 2015.-332 с. ISSN 2219-8792

10. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Некоторые перспективы применения систем контроля и управления доступом в региональных ВУЗАХ. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» При поддержке Посольства Туркменистана в Российской Федерации. Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
11. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Развитие сотрудничества российских и зарубежных ВУЗОВ по защите информационного ресурса. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» При поддержке Посольства Туркменистана в Российской Федерации. Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
12. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
13. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
14. Соляной В.Н., Сухотерин А.И Выработка коммуникативной компетенции при подготовке профессионалов по информационной безопасности с использованием технологии модерации. «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической

Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7
15. Соляной В.Н., Сухотерин А.И, Антоненко В.И. Проблемно-ориентированная подготовка специалистов по информационной безопасности с использованием имитационного метода (мозговой штурм). «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7.

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ НА ПРЕДПРИЯТИИ ПРИ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Гаранин Николай Борисович, студент 4 курса кафедры Информационной безопасности
Научный руководитель: **Соляной Владимир Николаевич**, к.воен.н., доцент, заведующий кафедрой Информационной безопасности

Современные интеллектуальные системы видеонаблюдения — это возможность значительно повысить эффективность мер безопасности. При всех преимуществах стандартных систем видеонаблюдения, нельзя не отметить их недостатка, который заключается в «человеческом факторе». Как правило, уже через 20 минут беспрерывного просмотра мониторов специалист теряет концентрацию внимания, из-за чего может не заметить противоправных действий, даже если их четко фиксирует одна из камер. Чем больше мониторов — тем больше рассеивается внимание охранника и тем меньше эффективность наблюдения.

Мониторинг, видеоаналитика, интеллект, интеллектуальные системы видеонаблюдения, анализ, принятие решений.

INTELLIGENT VIDEO SYSTEM ANALYZE THE BEHAVIOR OF EMPLOYEES ENTERPRISES WHILE ENSURING INFORMATION SECURITY

Garanin Nikolay, 4th year student of the Department of information security

Scientific adviser: **Solyanoy Vladimir,** Candidate of Military Sciences, Associate Professor, Head of the Department of information security

Modern intelligent video surveillance system - it is possible to significantly increase the effectiveness of security measures. With all the advantages of standard video surveillance systems, not to mention their lack of which is the "human factor". Usually, within 20 minutes of continuous viewing monitors specialist loses concentration, because of what may not notice illegal acts, even if they clearly captures one of the cameras. The more monitors - the more scattered the attention of the guard and the lower the efficiency of supervision.

Monitoring, video analytics, intelligence, intelligent video surveillance systems, analysis, decision-making.

Современные системы интеллектуального видеонаблюдения являются неотделимой, ключевой частью общей структуры информационной безопасности на любом предприятии. Спектр задач, которые они могут решать, весьма разнообразен. Это и видеоконтроль периметра и внутренней территории с функцией принятия решений, и противопожарная безопасность, и контроль доступа, и многое другое.

Современный уровень развития технологий позволяет использовать аппаратуру разного предназначения, различных производителей. Интегрированная многоуровневая архитектура и комплексное ПО дает возможность одновременного управления всеми устройствами.

Управленческие функции должны реализовываться вне зависимости от места установки, модели, марки производителя, характеристик и топологии структуры видеонаблюдения [4, 7, 9].

Структура системы интеллектуального видеонаблюдения (рис. 1) состоит из нескольких составляющих.

Цифровая система видеонаблюдения, в стандартизированной обезличенной форме, может состоять из следующих компонентов.

Сервер – программно-аппаратные устройства, которые предназначены для приема и дальнейшей обработки аудио и видеосигнала, поступающего с аналоговых и цифровых камер.

Рабочее место администратора — программно-аппаратная платформа, которая предназначена для удаленного управления системой видеонаблюдения.

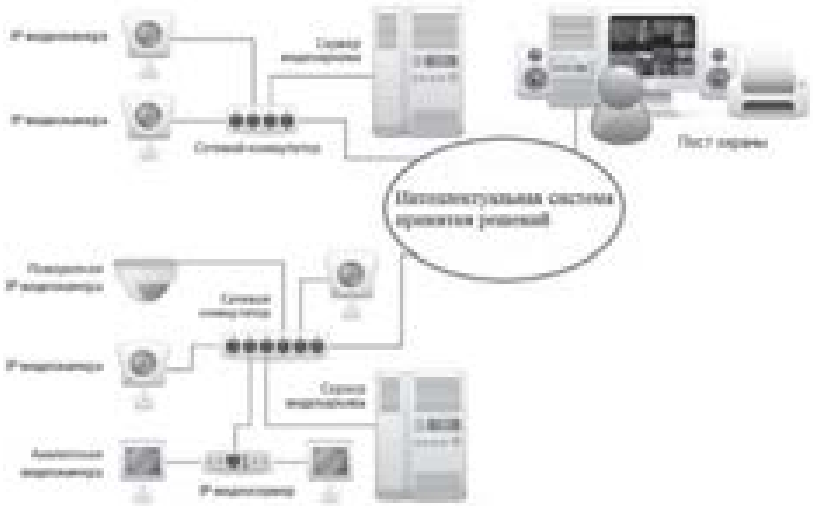


Рисунок 1 – Структура системы интеллектуального видеонаблюдения

Может быть использовано в качестве специализированного устройства: видеошлюз, удаленный сервер архивирования, удаленный Web-сервер и т. д.

Рабочее место мониторинга — программно-аппаратная платформа, которая используется в качестве рабочего места на посте охраны. Предоставляет оператору возможность удаленного видео и аудио контроля объекта охраны. Объединение всех элементов в структуре происходит в соответствии с требованиями безопасности и функциональности системы, техническими особенности охраняемого объекта.

В соответствии с требованиями, выдвигаемыми структуре, она может состоять из нескольких подсетей, которые взаимодействуют между собой через специально предназначенные шлюзы – сервера и станции администрирования.

Распределенная архитектура таких сложных сетей должна обеспечивать полное взаимодействие между различными компонентами [3, 4, 9].

Основными критериями являются:

- обеспечение синхронизации обмена данными;
- идентичность настроек основных параметров;

Таблица 1 - Функции интеллектуальной системы видеонаблюдения и задачи их реализации

Функции	Задачи
1	2
Обзорное и ситуационное видеонаблюдение	Автоматическое выявление и информирование о следующих событиях: • несанкционированный проход в запрещенные зоны метрополитена (служебные помещения и т. п.) • образование скопления людей (толпы) • быстрое движение (бег) • появление оставленных (бесхозных) предметов
Биометрическое видеонаблюдение	Автоматическое обнаружение и распознавание лиц пассажиров в зонах биометрического видеонаблюдения, в том числе: • автоматическая фиксация изображений всех работников • автоматическое выявление фактов прохода через турникеты • формирование сигнала тревоги о факте фиксации лица, входящего в список нарушителей и другие списки • прогнозирование на основе данных о времени фиксации распознанного лица в зонах биометрического видеонаблюдения траектории движения зафиксированного лица
Информационно – аналитическая подсистема	Предоставление функций анализа статистики (в виде таблиц и графиков): • общий подсчет людей • количество людей в зоне (скопление людей)
Управление и мониторинг	Подсистема должна обеспечивать: • контроль оборудования • представление детальной информации по каждому контролируемому устройству • мониторинг качества предоставляемых видеопотоков • оповещение персонала в случае ЧП
Управление службой охраны	• оперативное уведомление о всех тревожных событиях в зоне ответственности службы охраны • оперативная проверка по базе лиц нарушителей, включая фотографирование подозрительного лица, формирования запроса в подсистему биометрического видеонаблюдения и автоматической проверки по спискам зафиксированных ранее нарушителей
Информационная безопасность	Выявление основных видов угроз информационной безопасности: • противоправные действия третьих лиц • ошибочные действия пользователей и обслуживающего персонала • отказы и сбои программных средств • вредоносные программно-технические воздействия на средства вычислительной техники и информацию

- обмен командами между разнесенными компонентами одной системы;
- параллельное отображение тревожных событий на локальном рабочем месте и в центре обработки информации.

Интеллектуальная система безопасности и видеонаблюдения имеет в своем составе следующие элементы:

- система принятия решений при видеоанализе;
- СКУД на охраняемой территории;
- устройства телеметрии;
- оборудование для отображения и сохранения сигнала;
- подсистемы сигнализации различного предназначения: пожарные, охранные.

Обычная структура имеет ограничения, как в выявлении действий нарушителей, так и в реакции на них. Фактически это всего лишь визуальное выявление и подача звукового или видеосигнала на пульт охраны [1-16].

Система интеллектуального видеонаблюдения будет объединять в себе шесть основных подсистем, с задачами которых вы можете ознакомиться в табл. 1.

Интеллектуальная система видеонаблюдения глубоко взаимно интегрированная с системой безопасности имеет намного больший функционал. Возможности выявления нарушений гораздо шире: использование детекторов движения и звука, датчиков объемной сигнализации, размыкания и разбития [6].

Возможности интеллектуальных систем видеонаблюдения:

- контроль обработки, анализ и ранжирование важности событий для принятия дальнейших мер;
- удобный интерфейс, возможность получать на мобильные устройства сообщения о событиях;
- большие, почти неограниченные функциональные возможности, возможно подключать модули от различных разработчиков;
- возможность интегрирования и совместной работы всех подсистем: наблюдения, системы определения подвижных объектов и т.п.;
- работа в автоматическом или полуавтоматическом режиме;
- возможность фиксации событий с записью информации на носитель.

Ответные действия так же весьма разнообразны: блокировка дверей, активация камер с выведением на экран и динамики предупреждающего сигнала, включение записи, является реакцией [16].

В зависимости от поставленных задач, интеллектуальная видеоаналитика может реализовать как одну, так и несколько функций:

- Распознавание автомобильных номеров. Система предназначена для автоматического считывания государственных регистрационных знаков транспортных средств. Аналитика распознавания автомобильных номеров применяется при въезде на платные участки дорог, для мониторинга проезжающих транспортных средств на автодорогах различного уровня, для контроля въезда/выезда автомобилей с охраняемой территории (парковки, платные стоянки, территория предприятий и пр.).
- Определение лиц. Аналитика «Определение лиц» обнаруживает и автоматически выделяет из живого потока видео оптимальные изображения лиц для распознавания, сохранения в базе данных и последующей идентификации по биометрическим параметрам в режиме реального времени или при работе с архивами.

Данная функция позволяет каталогизировать по спискам сотрудников, посетителей, нежелательных лиц, подозреваемых и т.п., создавать группы, а также осуществлять импорт и экспорт отдельных изображений и карточек событий.

- Подсчет посетителей. Аналитика подсчета посетителей позволяет определять количество вошедших и вышедших людей в реальном времени, а также строить отчеты о находящихся в помещении посетителях за любой промежуток времени по одной или нескольким камерам.
- Подсчет количества объектов, пересекающих определенную зону. Применяется для подсчета количества объектов по заданным параметрам (размеры и форма настраиваются), пересекающих контролируемую зону (в одну сторону или в обоих направлениях). Можно создавать отчеты в форматах XML, HTML, Excel, CSV с возможностью автоматической отправки по электронной почте за выбранный период (каждый час, день, месяц, день недели).
- Движение в кадре. Задается область слежения в кадре (контрольная линия или произвольная зона), при пересечении которой подается тревожный сигнал, или можно задать минимальное и максимальное время пребывания объекта в заданной зоне и т.п. Возможна гибкая настройка на выдачу сигналов оповещения по заранее заданным условиям. Расширенный вариант данной аналитики

позволяет осуществлять поиск по выбранному направлению движения объекта [10].

В процессе разработки структуры системы видеонаблюдения и ее последующей инсталляции нужно предусмотреть логику автоматического функционирования, согласно общей концепции безопасности организации.

Принцип работы интеллектуальной системы видеонаблюдения показан на рис. 2.

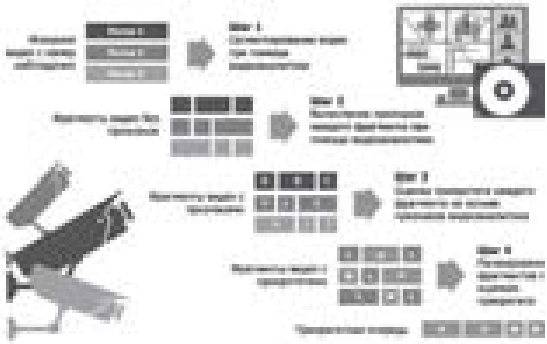


Рисунок 2 – Алгоритм работы функции видеоаналитики

Исходное видео поступает с камер в виде непрерывного видеопотока. Далее этот видеопоток разделяется на фрагменты при помощи системы видеоаналитики. Каждый фрагмент соответствует объекту или событию, которые представляют интерес для службы охраны. Алгоритмы видеоаналитики выделяют признаки каждого фрагмента, и по этим признакам каждому фрагменту назначается свой приоритет (степень важности). Далее все фрагменты можно поместить в приоритетную очередь и обрабатывать в порядке важности: записывать на диск или показывать оператору.

Для удобства восприятия информации количество мониторов на рабочем месте наблюдателя должно соответствовать уровню активности на объекте. Если активность низкая, то один оператор способен проанализировать информацию с большего количества источников. Для повышения эффективности можно произвести тематическую группировку выводимой информации на отдельных мониторах. Система должна автоматизировать процесс как можно больше. В идеале участие оператора должно ограничиться контролем над работоспособностью устройств, и подтверждением правильности уже запрограммированных реакций на внешние события.

Новые технологии дают возможность удаленного управления системой видеонаблюдения, а распределенность архитектуры позволяет не зависеть от месторасположения ключевых командных модулей.

При различных конфигурациях и сложной структуре сетей, большой разбросанности охраняемых участков, для обеспечения устойчивости к сбоям целесообразно построение контролирующей системы с децентрализованным средним уровнем управления. Централизованно же будет применяться мониторинг управляющих систем. Составные части смогут функционировать через глобальные сети, телефонные коммуникации или разветвленные локальные сети, с помощью технологии «тонкого клиента». Такая «распределенная» архитектура даст возможность структуре не зависеть от расположения объектов, контролирующего оборудования и модулей взаимодействия. Это позволяет создать неограниченное количество рабочих мест как удаленных, так и локальных [4, 15].

Преимущества интеллектуальной видеосистемы:

- возможность принятия определенных решений по противодействию НСД в контролируемой зоне;
- анализ длительности пребывания объекта в зоне видимости. Если объект находится дольше определенного времени — на пульт службы охраны посылается соответствующий сигнал;
- определение скоплений людей;
- выявление нетипичного поведения людей: система реагирует на резкие перемещения, драки, падения и т.п.;
- оповещение об опасной ситуации в зоне наблюдения (например, оставленного у входа неизвестного пакета)

Таким образом, интеллектуальная система видеонаблюдения существенно упрощает работу службы охраны, а так же позволяет минимизировать риски информационной безопасности в сравнении с обычными ТВ - системами действия которых направляются только на наблюдение на объектами.

Литература

1. Алаухов С.Ф, Коцеруба В.Я. Вопросы создания систем физической защиты для крупных промышленных объектов // Системы безопасности, 2001, № 41, С. 93.
2. Барсуков В. С. Интегральная защита информации // Системы безопасности, 2002. №5, 6.

3. Белый В.М., Белый Р.В. Эффективность информационных систем и информационных технологий: учебник – Королёв МО; ФТА, 2013 – 396 с.
4. Вихорев С., А. Ефимов, Практические рекомендации по информационной безопасности. Jet Info, № 10-11, 1996.
5. Воронов В.А., Тихонов В.А. «Концептуальные основы создания и применения системы защиты объектов» - Издательство «Горячая линия – Телеком», 2012. – 196 с.
6. Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации на предприятии: учеб. пособие для ВУЗов - М.: ИЦ Академия, 2009г. - 416 с.
7. Дербенцева Е. Инсайдеры и корпоративная безопасность.//PC WEEK/RE. №42, 2006, с. 46-47.
8. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты: учеб. пособие для ВУЗов – М.: ТИД Диа Софт,2002 г. – 688 с.;
9. Завгородний В. И. Концепция создания ЭВМ защищенной архитектуры//Безопасность информационных технологий. №1, 2006, с. 15 – 20.
10. Малюк А.А. «Информационная безопасность: концептуальные и методологические основы ЗИ» Учеб. пособие для ВУЗов. – М.: Горячая линия-Телеком, 2004 г. - 280 с.
11. Петренко С. А., Симонов С. В. Управление информационными рисками. Экономически оправданная безопасность. − М.: АйТи-Пресс, 2004. − 384 с.
12. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
13. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Некоторые перспективы применения систем контроля и управления доступом в региональных ВУЗАХ. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной

научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
14. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Развитие сотрудничества российских и зарубежных ВУЗОВ по защите информационного ресурса. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
15. Тарасюк М. В. Защищенные информационные технологии. Проектирование и применение. М.:Слон-пресс, 2004.
16. Тихонов В А., Райх В. В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Уч. пособие. М.: Гелиос АРВ, 2006.

СПОСОБЫ РЕАЛИЗАЦИИ УГРОЗ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В БЕСПРОВОДНЫХ СЕТЯХ ОБМЕНА ИНФОРМАЦИЕЙ

Гаранин Николай Борисович, студент 4 курса кафедры Информационной безопасности
Научный руководитель: **Журавлев Сергей Иванович**, к.т.н., доцент кафедры Информационной безопасности

Угрозы безопасности информации имеют различные способы реализации и могут реализовываться по отношению к БСПД, к информации, передаваемой по БСПД, а также по отношению к защищаемым ресурсам проводной сети организации, подключенной к подсистеме сетевой коммутации БСПД. Как правило, наиболее значимой угрозой безопасности информации является УНК информации, передаваемой по БСПД.

Информационная безопасность, угрозы, информация, доступность, несанкционированный доступ, способы.

INTELLIGENT VIDEO SYSTEM ANALYZE THE BEHAVIOR OF EMPLOYEES ENTERPRISES WHILE ENSURING INFORMATION SECURITY

Garanin Nikolay, 4th year student of the Department of information security
Scientific adviser: **Zhuravlev Sergey,** Candidate of Technical Sciences, Associate Professor of the Department of information security

Information security threats are different ways to implement and can be implemented with respect to BSPD to information transmitted by BSPD and in relation to protected resources networking wired connected to a network subsystem BSPD switching. As a rule, the most significant threat to the security of information is UNK information transmitted by BSPD.

Information Security, treats, information, availability, unauthorized access, ways.

Угрозы безопасности информации имеют различные способы реализации и могут реализовываться по отношению к БСПД, к информации, передаваемой по БСПД, а также по отношению к защищаемым ресурсам проводной сети организации, подключенной к подсистеме сетевой коммутации БСПД. Как правило, наиболее значимой угрозой безопасности информации является УНК информации, передаваемой по БСПД [1, 4, 5, 7].

Возможны 3 угрозы НСД к информации, содержащейся в информационной системе, при применении БСПД:

- угроза несанкционированного ознакомления с информацией, передаваемой по БСПД (далее – УНК);
- угроза нарушения целостности и доступности БСПД и передаваемой по ней информации (далее – УНЦД);
- угроза несанкционированного использования БСПД (далее – УНИС).

Для реализации угроз безопасности информации вероятные нарушители могут использовать каналы непосредственного (физического) доступа к оборудованию БСПД, а также каналы связи БСПД (проводные и беспроводные).

Следует отметить, что нарушение доступности БСПД может быть не связано со злонамеренными действиями нарушителя, а быть вызвано интерференцией сигналов рядом стоящих точек беспроводного доступа, наличием на объекте размещения беспроводного оборудования генераторов электромагнитного поля, работающих на частотах БСПД (например, микроволновых печей, Bluetooth устройств, средств электромагнитного зашумления и др.), а

также может быть вызвано большой поглощающей способностью материалов, используемых в конструкции здания, на котором разворачивается БСПД [2, 3, 5, 6].

Есть много способов реализации угроз несанкционированного доступа к информации, содержащейся в информационной системе, при применении беспроводных сетей передачи данных

В таблице 1 перечислены основные способы реализации угроз НСД к информации, содержащейся в информационной системе, при применении БСПД.

Возможность использования того или иного способа реализации угроз зависит от следующих условий:

- доверенности используемой аппаратной и программной платформы оборудования БСПД;
- применяемых на объекте размещения оборудования БСПД организационных мер по защите информации;
- «подконтрольности» БСПД;
- установленных на оборудование БСПД средств защиты информации от НСД и корректности их настройки;
- используемых встроенных в оборудование БСПД механизмов защиты информации от НСД и корректности их настройки;
- наличия подключения БСПД к внешним сетям (в т.ч. недоверенным).

Угрозы безопасности информации и способы их реализации, представленные в настоящем дипломном проекте, являются всеобъемлющими и не учитывают меры по защите информации, принятые на конкретном объекте размещения БСПД и используемые на объекте технологии обработки информации. Формирование перечня обоснованных угроз безопасности информации должно выполняться на этапе разработки системы защиты информации БСПД конкретного объекта по результатам выполнения анализа рисков и разработки модели угроз безопасности информации. Разработка модели угроз безопасности информации должна осуществляться с учетом условий функционирования БСПД, а также требований по защите информации, установленных нормативными правовыми актами в области защиты информации, либо предъявляемых заказчиком разработки системы защиты информации.

Обозначения, используемые в таблице 1:

«+» – способ, указанный в строке таблицы, используется для реализации угрозы НСД к информации, указанной в столбце таблице;

«–» – способ, указанный в строке таблицы, не используется для реализации угрозы НСД к информации, указанной в столбце таблице.

Таблица 1 - Способы реализации угроз НСД к информации, содержащейся в информационной системе, при применении БСПД

№ п/п	Способы реализации угроз НСД к информации, содержащейся в информационной системе, при применении БСПД	Угроза НСД		
		УНК	УНЦД	УНИС
	Способы, реализация которых зависит от доверенности используемой аппаратной и программной платформы оборудования БСПД			
1.	Использование внедренных в оборудование БСПД программных и/или аппаратных закладок (электронных устройств негласного получения информации, «жучков», «бэкдоров» и др.)	+	+	+
2.	Использование недоверенного программного обеспечения телекоммуникационного оборудования и АУ (в т.ч. программного обеспечения BIOS и микроконтроллеров) с возможностями дистанционного управления и измерения	+	+	+
	Способы, реализация которых зависит от применяемых на объекте размещения оборудования БСПД организационных мер по защите информации			
3.	Скрытное копирование/модификация/блокирование защищаемой информации, обрабатываемой оборудованием БСПД	+	+	–
4.	Скрытное копирование/модификация/блокирование конфигурационной информации БСПД, навязывание ложных (специально сформированных нарушителем) команд управления	+	+	–
5.	Самовольная установка/подмена/хищение оборудования БСПД, отключение его от линий связи, электропитания и заземления	+	+	–
6.	Нарушения целостности проводных каналов связи, линий электропитания и заземления	–	+	–
7.	Несанкционированное подключение к проводным каналам связи	+	–	
8.	Получение информации о системе защиты информации БСПД (в т.ч. парольной и ключевой информации)	+	–	–
	Способы, реализация которых зависит от «подконтрольности» БСПД			
9.	Подключение к БСПД из-за пределов контролируемой зоны	–	–	+
10.	Установка ложных точек доступа	–	+	–
11.	Сканирование и/или перехват трафика, передаваемого по БСПД (выполняемые, например, с использованием программного обеспечения NetStumbler, Wellenreiter и др.)	+	–	–
12.	Подмена MAC-адреса АУ нарушителя на MAC-адрес зарегистрированного пользователя	–	+	–
13.	Выполнение атак типа DoS (выполняемые, например, с использованием программного обеспечения WLANjack, hunter_killer)	–	+	–
14.	Реализация атак типа Man-in-The-Middle	+	–	–
15.	Реализация атак типа ARP-spoofing	+	–	–

№ п/п	Способы реализации угроз НСД к информации, содержащейся в информационной системе, при применении БСПД	Угроза НСД		
		УНК	УНЦД	УНИС
	Способы, реализация которых зависит от установленных на оборудование БСПД средств защиты информации от НСД и корректности их настройки			
16.	Загрузка нештатной операционной системы с внешнего носителя информации	+	–	–
17.	Подбор параметров учетной записи пользователя	+	–	–
18.	Подбор ключей шифрования, используемых наложенными средствами защиты информации	+	–	–
19.	Выполнение доступа к защищаемой информации в обход используемых механизмов разграничения доступа	+	–	–
20.	Искажение обрабатываемой и/или передаваемой информации	–	+	–
21.	Внедрение вредоносного программного обеспечения	+	+	+
22.	Установка недоверенного программного обеспечения (в т.ч. вредоносного)	–	+	–
23.	Реализация сетевых атак	+	+	–
	Способы, реализация которых зависит от используемых, встроенных в оборудование БСПД, механизмов защиты информации от НСД и корректности их настройки			
24.	Подключение к БСПД без ввода необходимых учетных данных	–	–	+
25.	Получение параметров учетной записи пользователя, используемых для доступа к БСПД (выполняемое, например, с использованием программного обеспечения ASLEAP, THC-LEAPCracker)	+	–	–
26.	Получение ключей шифрования, используемых в БСПД (выполняемое, например, с использованием программного обеспечения AirCrack, WEPWedgie, WEPCrack, WepAttack, AirSnort)	+	–	–
27.	Подключение к БСПД с использованием ключевой информации, указанной в технической документации на оборудование БСПД	–	–	+
28.	Подключение к оборудованию БСПД с использованием учетной записи пользователя, указанной в технической документации на оборудование БСПД	–	–	+
	Способы, реализация которых зависит от наличия подключения БСПД к внешним сетям (например, к сети Интернет)			
29.	Выполнение сетевых атак со стороны внешней сети (атак на информационные ресурсы БСПД и/или на информационные ресурсы проводной сети организации, подключенной к подсистеме сетевой коммутации БСПД)	+	+	–

Как видно из таблицы 1 способы реализации угроз безопасности информации обладают следующими особенностями:

• один способ реализации угроз безопасности информации может использоваться для реализации различных угроз безопасности информации;

• для реализации какой-либо угрозы безопасности информации может потребоваться комбинация нескольких способов реализации угроз.

Так, для реализации доступа из-за пределов контролируемой зоны к информационным ресурсам проводной сети организации, подключенной к БСПД (УНК), нарушителю из числа лиц категории IV может, например, потребоваться (рис. 1):

• выполнить сканирование трафика для получения MAC-адреса АУ зарегистрированного пользователя (способ 11);

• выполнить подмену MAC-адреса АУ нарушителя на MAC-адрес зарегистрированного пользователя (способ 12);

• получить параметры учетной записи пользователя, используемые для доступа к БСПД (способ 25) и/или получить ключи шифрования, используемые в БСПД (способ 26);

• подобрать ключи шифрования, используемые наложенными средствами криптографической защиты информации, передаваемой по БСПД (способ 18);

• выполнить подключение к БСПД из-за пределов контролируемой зоны (способ 9);

• реализовать сетевую атаку на периметровые средства защиты информации проводной сети организации (способ 23);

• получить доступ к защищаемой информации проводной сети организации в обход используемых механизмов разграничения доступа (способ 19).

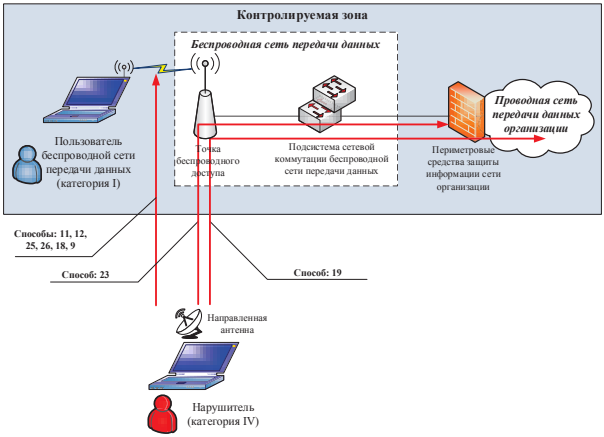


Рисунок 1 – Пример реализации УНК

Следует отметить, что описанная угроза может быть реализована и с использованием других способов реализации угроз НСД к информации, содержащейся в информационной системе, при применении БСПД [1, 2, 8, 7].

Литература

1. Журавлев С.И., Мирсаитов Р.С. Один из подходов статистического анализа защищенного трафика ведомственных IP-сетей. Статья в журнале «Двойные технологии» № 1, 2015, с. 34-39.
2. Зайцев А.П., Шелупанов А.А., Технические средства и методы защиты информации. - М.: Машиностроение, 2009. – 507 с.
3. Малюк А.А. Информационная безопасность: концептуальные и методологические основы ЗИ. Учеб. пособие для ВУЗов. – М.: Горячая линия-Телеком, 2004 г. - 280 с.
4. Осипова Г.Л., Юдина Е.Я., Снижение шума в зданиях и жилых районах – М.: Стройиздат, 1987.
5. Тарасюк М. В. Защищенные информационные технологии. Проектирование и применение. М.: Слон-пресс, 2004.
6. Торокин А.А., Инженерно-техническая защита информации. – М.: Гелиос АРВ, 2005. – 960 с.
7. Хорев А.А., Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. – М.: Гостехкомиссия РФ, 1998. – 320 с.
8. Хорев А.А., Способы и средства защиты информации. Учебное пособие. – М.: МО РФ, 2000. – 316 с.

ОСНОВЫ ОПРЕДЕЛЕНИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ

Гахраманов Андрей Павлович, студент 1 курса кафедры Информационной безопасности
Научный руководитель: **Соляной Владимир Николаевич,** к.воен.н., доцент, заведующий кафедрой Информационной безопасности

Сегодня не вызывает сомнений необходимость вложений в обеспечение информационной безопасности современного крупного бизнеса. Основной вопрос современного бизнеса - как оценить необходимый уровень вложений в ИБ для обеспечения максимальной эффективности инвестиций в данную сферу. Для решения этого вопроса существует только один способ - применять системы анализа рисков, позволяющие оценить существующие в системе

риски и выбрать оптимальный по эффективности вариант защиты (по соотношению существующих в системе рисков / затрат на ИБ).

Информационная безопасность, анализ, эффективность защиты.

BASED ON CERTAIN INFORMATION SECURITY RISKS IN THE MODERN CONDITIONS

GahramanovAndrey, 1st year student of the Department of information security
Scientific adviser: **Solyanoy Vladimir,** Candidate of Military Sciences, Associate Professor, Head of the Department of information security

Today there is no doubt the need for investment in information security provision for modern big business. The main question of modern business - how to evaluate the necessary level of investment in information security to ensure maximum efficiency of investments in this area. To address this issue there is only one way - to apply a risk analysis system that allows to assess the existing risks in the system and to choose optimal variant of protection efficiency (the ratio existing in the system risk / information security costs)

Information security analysis, the effectiveness of protection.

Для подтверждения факта актуальности задачи обеспечения безопасности бизнеса, воспользуемся отчетом ФБР за последние годы. Данные были собраны на основе опроса 530 американских компаний (средний и крупный бизнес). Статистика инцидентов области ИТ секьюрити неумолима. Согласно даннымФБР (рис.1) в 2003 году 56% опрошенных компаний подвергались атаке [1-8].

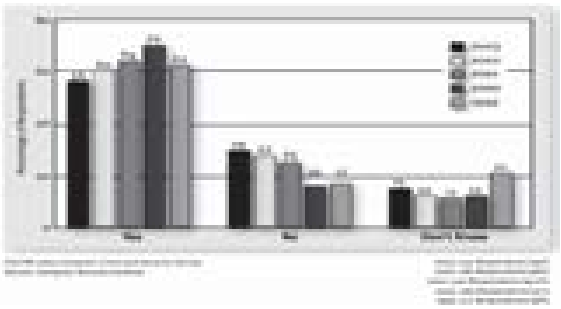


Рисунок 1 – Статистика опросов компаний

Потери от разного вида информационных воздействий показаны на следующем рис.2 [3].

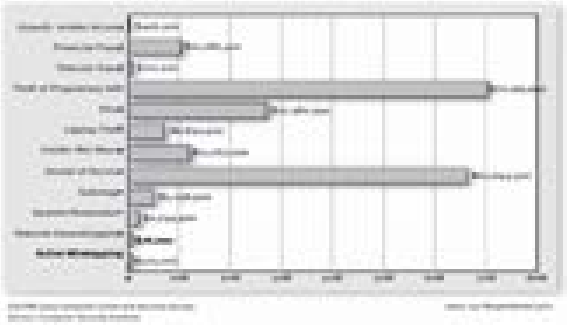


Рисунок 2 - Статистика информационных заражений

Цель управления ИБ состоит в сохранении конфиденциальности, целостности и доступности информации. Вопрос только в том, какую именно информацию необходимо охранять и какие усилия прилагать для обеспечения ее сохранности.

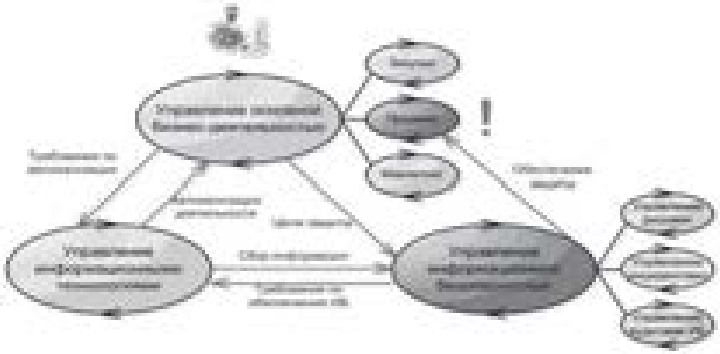


Рисунок 3 - Взаимосвязь процессов управления и защиты в организации

Любое управление основано на осознании ситуации, в которой оно происходит. В терминах анализа рисков осознание ситуации выражается в инвентаризации и оценке активов организации и их окружения, т.е. всего того, что обеспечивает ведение бизнес-деятельности. С точки зрения анализа рисков ИБ к основным активам относятся непосредственно информация, инфраструктура, персонал, имидж и репутация компании. Без инвентаризации активов на уровне бизнес-деятельности невозможно ответить на вопрос, что именно

нужно защищать. Очень важно понять, какая информация обрабатывается в организации и где выполняется ее обработка [1-8].

В условиях крупной современной организации количество информационных активов может быть очень велико. Если деятельность организации автоматизирована при помощи ERP-системы, то можно говорить, что практически любому материальному объекту, использующемуся в этой деятельности, соответствует какой-либо информационный объект. Поэтому первоочередной проблемой является задача управления рисками информационной безопасности.

Решить эту задачу невозможно без привлечения менеджеров основного направления деятельности организации как среднего, так и высшего звена. Оптимальна ситуация, когда высший менеджмент организации лично задает наиболее критичные направления деятельности, для которых крайне важно обеспечить информационную безопасность. Мнение высшего руководства по поводу приоритетов в обеспечении ИБ очень важно и ценно в процессе анализа рисков, но в любом случае оно должно уточняться путем сбора сведений о критичности активов на среднем уровне управления компанией [1-8]. При этом дальнейший анализ целесообразно проводить именно по обозначенным высшим менеджментом направлениям бизнес-деятельности. Полученная информация обрабатывается, агрегируется и передается высшему менеджменту для комплексной оценки ситуации (но об этом чуть позже).

Ключевыми процедурами при определении информационных рисков следует рассматривать: оценка рисков; анализ рисков и управление рисками [1-8].

Оценка информационных рисков. Идентифицировать и локализовать информацию можно на основании описания бизнес-процессов, в рамках которых информация рассматривается как один из типов ресурсов. Задача несколько упрощается, если в организации принят подход регламентации бизнес-деятельности (например, в целях управления качеством и оптимизации бизнес-процессов). Формализованные описания бизнес-процессов служат хорошей стартовой точкой для инвентаризации активов. Если описаний нет, можно идентифицировать активы на основании сведений, полученных от сотрудников организации. После того как активы идентифицированы, необходимо определить их ценность.

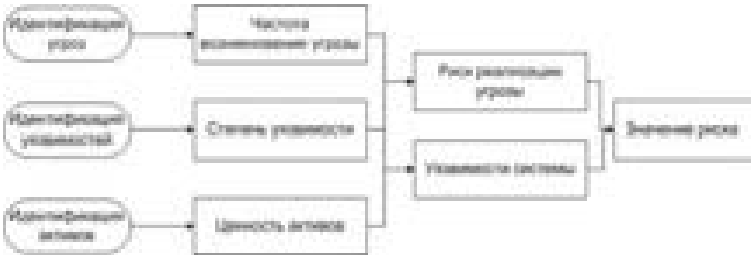


Рисунок 4 - Процесс оценки информационных рисков

Работа по определению ценности информационных активов в разрезе всей организации одновременно наиболее значима и сложна. Именно оценка информационных активов позволит начальнику отдела ИБ выбрать основные направления деятельности по обеспечению информационной безопасности.

Ценность актива выражается величиной потерь, которые понесет организация в случае нарушения безопасности актива. Определение ценности проблематично, потому что в большинстве случаев менеджеры организации не могут сразу же дать ответ на вопрос, что произойдет, если, к примеру, информация о закупочных ценах, хранящаяся на файловом сервере, уйдет к конкуренту. Вернее сказать, в большинстве случаев менеджеры организации никогда не задумывались о таких ситуациях [1-8].

Но экономическая эффективность процесса управления ИБ во многом зависит именно от осознания того, что нужно защищать и какие усилия для этого потребуются, так как в большинстве случаев объем прилагаемых усилий прямо пропорционален объему затрачиваемых денег и операционных расходов. Управление рисками позволяет ответить на вопрос, где можно рисковать, а где нельзя. В случае ИБ термин «рисковать» означает, что в определенной области можно не прилагать значительных усилий для защиты информационных активов и при этом в случае нарушения безопасности организация не понесет значимых потерь. Здесь можно провести аналогию с классами защиты автоматизированных систем: чем значительнее риски, тем более жесткими должны быть требования к защите [1-8].

Чтобы определить последствия нарушения безопасности, нужно либо иметь сведения о зафиксированных инцидентах аналогичного характера, либо провести сценарный анализ. В рамках сценарного анализа изучаются причинно-следственные связи между событиями

нарушения безопасности активов и последствиями этих событий для бизнес-деятельности организации. Последствия сценариев должны оцениваться несколькими людьми, итерационным или совещательным методом. Следует отметить, что разработка и оценка таких сценариев не может быть полностью оторвана от реальности. Всегда нужно помнить, что сценарий должен быть вероятным. Критерии и шкалы определения ценности индивидуальны для каждой организации. По результатам сценарного анализа можно получить информацию о ценности активов.

Если активы идентифицированы и определена их ценность, можно говорить о том, что цели обеспечения ИБ частично установлены: определены объекты защиты и значимость поддержания их в состоянии информационной безопасности для организации. Пожалуй, осталось только определить, от кого необходимо защищаться [1-8].

Идентифицировать и оценить активы, разработать модель нарушителя и модель угроз, идентифицировать уязвимости — все это стандартные шаги, описание которых должно присутствовать в любой методике анализа рисков. Все перечисленные шаги могут выполняться с различным уровнем качества и детализации. Очень важно понять, что и как можно сделать с огромным количеством накопленной информации и формализованными моделями. На наш взгляд, этот вопрос наиболее важен, и ответ на него должна давать используемая методика анализа рисков.

Полученные результаты необходимо оценить, агрегировать, классифицировать и отобразить. Так как ущерб определяется на этапе идентификации и оценки активов, необходимо оценить вероятность событий риска. Как и в случае с оценкой активов, оценку вероятности можно получить на основании статистики по инцидентам, причины которых совпадают с рассматриваемыми угрозами ИБ, либо методом прогнозирования — на основании взвешивания факторов, соответствующих разработанной модели угроз [1-8].

Хорошей практикой для оценки вероятности станет классификация уязвимостей по выделенному набору факторов, характеризующих простоту эксплуатации уязвимостей. Прогнозирование вероятности угроз проводится уже на основании свойств уязвимости и групп нарушителей, от которых исходят угрозы.

В качестве примера системы классификации уязвимостей можно привести стандарт CVSS — commonvulnerabilityscoringsystem. Следует отметить, что в процессе идентификации и оценки уязвимостей очень важен экспертный опыт специалистов по ИБ, выполняющих оценку рисков, и используемые статистические материалы и отчеты по уязвимостям и угрозам в области информационной безопасности [1-8].

1. Анализ информационных рисков. Величину (уровень) риска следует определить для всех идентифицированных и соответствующих друг другу наборов «актив — угроза». При этом величина ущерба и вероятности не обязательно должны быть выражены в абсолютных денежных показателях и процентах; более того, как правило, представить результаты в такой форме не удается. Причина этого — используемые методы анализа и оценки рисков информационной безопасности: сценарный анализ и прогнозирование.

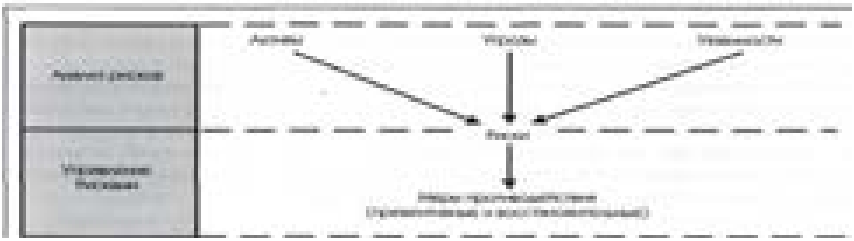


Рисунок 5 - Анализ информационных рисков

Делая вывод можно сказать, что анализ рисков это достаточно трудоемкая процедура. В процессе анализа рисков должны применяться методические материалы и инструментальные средства. Однако для успешного внедрения повторяемого процесса этого недостаточно; еще одна важная его составляющая — регламент управления рисками. Он может быть самодостаточным и затрагивать только риски ИБ, а может быть интегрирован с общим процессом управления рисками в организации.

В процессе анализа рисков задействованы многие структурные подразделения организации: подразделения, ведущие основные направления ее деятельности, подразделение управления информационной инфраструктурой, подразделение управления ИБ. Кроме того, для успешного проведения анализа рисков и эффективного использования его результатов необходимо привлечь

высший менеджмент организации, обеспечив тем самым взаимодействие между структурными подразделениями [1-8].

Одной лишь методики анализа рисков или специализированного инструментального средства для оценки рисков ИБ недостаточно. Необходимы процедуры идентификации активов, определения значимости активов, разработки моделей нарушителя и угроз, идентификации уязвимостей, агрегирования и классификации рисков. В различных организациях все перечисленные процедуры могут существенно различаться. Цели и масштаб проведения анализа рисков ИБ также влияют на требования, предъявляемые к сопутствующим анализу рисков процессам.

2. Управление информационными рисками. Применение метода анализа рисков для управления ИБ требует от организации достаточного уровня зрелости, на котором можно будет реализовать все необходимые в рамках анализа рисков процессы.

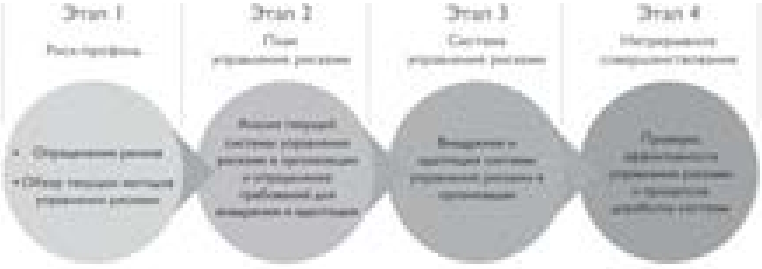


Рисунок 6 - Система управления информационными рисками

Управление рисками позволяет структурировать деятельность отдела ИБ, найти общий язык с высшим менеджментом организации, оценить эффективность работы отдела ИБ и обосновать решения по выбору конкретных технических и организационных мер защиты перед высшим менеджментом [1-8].

Процесс управления рисками непрерывен, так как верхнеуровневые цели обеспечения ИБ могут оставаться неизменными на протяжении длительного времени, а информационная инфраструктура, методы обработки информации и риски, связанные с использованием ИТ, постоянно меняются.

Отдел ИБ и организация в целом в случае структурирования своей деятельности путем непрерывного управления рисками получают следующие весьма значимые преимущества [1-8]:

-идентификация целей управления;

-определение методов управления;

-эффективность управления, основанная на принятии обоснованных и своевременных решений.

В связи с управлением рисками и управлением ИБ необходимо отметить еще несколько моментов.

Оценка и анализ рисков, управление инцидентами и аудит ИБ неразрывно связаны друг с другом, поскольку связаны входы и выходы перечисленных процессов. Разработку и внедрение процесса управления рисками необходимо вести совместное управлением инцидентами и аудитами ИБ.

Установленный процесс управления рисками — это обязательное требование стандарта СТО-БР ИББС-1.0-2006 по обеспечению информационной безопасности в банковской сфере.

Постановка процесса управления рисками необходима организации, если в ней принято решение о прохождении сертификации на соответствие требованиям международного стандарта ISO/IEC 27001:2005.

Таким образом, установление режима защиты конфиденциальных данных неразрывно связано с оценкой, анализом и управлением информационными рисками, так как все перечисленные процессы защиты информации используют сходные методы идентификации и оценки активов, разработки модели нарушителя и модели угроз в интересах снижения ожидаемых информационных рисков.

Литература

1. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум- 2012. С.16-25.

2. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА- 2012. С.132-140.

3. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. - М.: МГИУ- 2013 ,С.51-

4. Соляной В.Н., Сухотерин А.И Выработка коммуникативной компетенции при подготовке профессионалов по информационной безопасности с использованием технологии модерации. «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7

5. Соляной В.Н., Сухотерин А.И, Антоненко В.И. Проблемно-ориентированная подготовка специалистов по информационной безопасности с использованием имитационного метода (мозговой штурм). «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7.
6. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
7. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
8. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Некоторые перспективы применения систем контроля и управления доступом в региональных ВУЗАХ. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
9. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Развитие сотрудничества российских и зарубежных ВУЗОВ по защите информационного ресурса. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной

научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.

НОВЫЕ ТЕХНОЛОГИИ ЗЛОВРЕД ВЫМОГАТЕЛЬСТВА В ЗАЩИЩАЕМОЙ ИНФОРМАЦИОННОЙ СФЕРЕ

Житник Владислав Русланович, студент 1 курса кафедры Информационной безопасности
Научный руководитель: **Соляной Владимир Николаевич,** к.воен.н., доцент, заведующий кафедрой Информационной безопасности

В настоящее время зловреды-вымогатели (Ransomware) являются наиболее активно развивающимся классом вредоносного ПО. За последние годы они прошли большой путь от обычной блокировки экрана с требованием выкупа до опаснейших шифровальщиков. На данный момент шифровальщики составляют основу класса Ransomware. Они представляют собой троянскую программу, которая скрыто шифрует принадлежащие владельцу данные с заданными расширениями. За их расшифровку злоумышленники запрашивают немалые суммы. Примерами таких зловредов являются Cryprolocker, GpCode, ACCDFISA.

Зловред-вымогатели, шифровальщики, CTB-Locker.

NEW TECHNOLOGIES OF THE RANSOMWARE IN THE PROTECTED INFORMATION SPHERE

Zhitnik Vladislav, 1st year student of the Department of information security
Scientific adviser: **Solyanoi Vladimir,** Candidate of Military Sciences, Docent, Head of the Department of information security

Today the ransomware is the most rapidly evolving class of malware. In recent years they have come a long way from the usual lock screen with the ransom demand to a dangerous cryptographer. Cryptographers are the basic of the class Ransomware at this moment. They are a Trojan, which covertly encrypts data of the owner with given extensions. Attackers request a considerable sum for decryption. Examples of such malware are Cryptolocker, GpCode, ACCDFISA.

Ransomware, cryptographer, CTB-Locker.

Летом 2014 года был обнаружен новый троянец, который нельзя было отнести ни к одному известному семейству, его авторское название – CTB-Locker [4].

Аббревиатура CTB в названии зловреда означает Curve Tor Bitcoin. Первое слово сообщает о том, что вымогатель использует нестандартный алгоритм шифрования (Elliptic Curve Diffie-Hellman). Второе: управляющие сервера зловреда спрятаны в анонимной сети Tor. Наконец, третье: выкуп у своих жертв злоумышленники требуют в электронной валюте Bitcoin.

При работе троянец использует следующий высокоуровневый алгоритм (рис. 1):

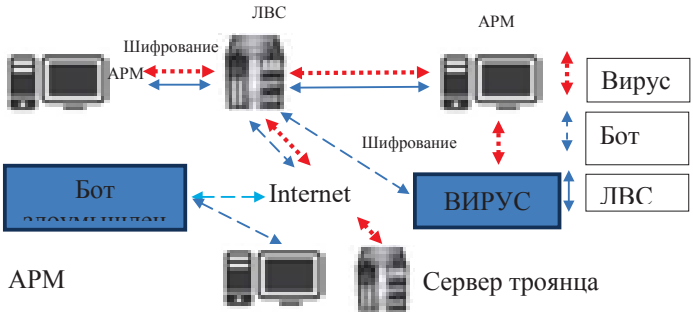


Рисунок 1 – Алгоритм работы троянца

- запуск файла с троянцем, для этого достаточно прав пользователя;
- происходит генерация ключей по протоколу Диффи-Хеллмана. Но на компьютере пользователя сохраняется только публичный ключ, с помощью которого расшифровать файлы нельзя;
- троянец шифрует абсолютно все файлы, предварительно их сжимая, с заданными расширениями (рис.2), при этом он пытается это делать на жестких дисках, съемных носителях и в общих сетевых ресурсах;
- после шифрования всех файлов, зловед выводит пользователю окно с описанием его проблемы и схемой оплаты;
- производится запрос на сервер и передачу зашифрованного ключа или сообщение пользователю адреса сервера либо специального кода, по которому он может произвести оплату вручную;

- в ответ на это сервер генерирует Bitcoin-адрес, на который надо произвести оплату, причем для каждого пользователя этот адрес уникален;
- сервер производит мониторинг транзакций Bitcoin на предмет поступления денег на счет. Как только транзакция полностью проходит, то боту вычисляется и сообщается секретный ключ. Если же был произведен ручной ввод кода для оплаты, то пользователю отдается небольшой exe-декриптор с зашитым ключом, которым он может починить только свой компьютер. Размер декриптора не превышает 30 килобайт;

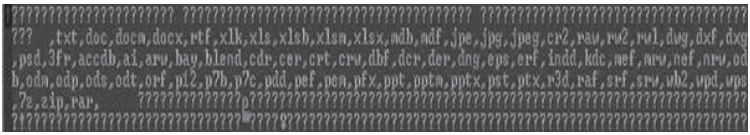


Рисунок 2 - Фрагмент данных, содержащих список расширений для шифрования

- бот производит расшифровывание всех файлов и самоудаляется;
- деньги с локального кошелька после проверки транзакции выводятся на основной Bitcoin-адрес. В случае утраты сервера деньги не потеряются.

При этом в CTB-Locker реализованы новые решения, которые не использовались в ранних семействах вымогателей:

- зловред использует стойкую криптографию на основе эллиптических кривых. В связи с этим расшифровать файлы без оплаты невозможно. Стойкость эквивалента RSA-3072, что превышает все аналоги. При этом скорость шифрования значительно выше;
- все ключи одноразовые, абсолютно случайны. У аналогов они в шиты в locker или сервер, что позволяет их собрать;
- размещение командного сервера в onion-домене, закрыть домен нельзя, практически невозможно отследить владельца и отключить сервер;
- связь с сервером происходит только после шифрования всех файлов. Невозможно раннее обнаружение по трафику, невозможно блокировать работу locker'а. Блокирование Tor мешает

только оплате пользователю, а не программе. Аналоги соединяются с сервером до шифрования и их можно блокировать;

- оплата производится биткойнами со всеми вытекающими последствиями: невозможность блокировать или изъять кошелек злоумышленника;
- пользователю предоставлена возможность оплатить код с другого компьютера. Длина кода не превышает 150 символов, это позволяет переписать их на любой носитель информации. Другие семейства шифровальщиков не предоставляют такой возможности, либо оплата кода офлайн довольно проблематична.

А теперь о некоторых решениях, реализованных в CTB-locker, поподробнее.

В CTB-Locker была организована необычайная техническая организация доступа к сети Tor.

Ранние семейства шифровальщиков если и общались с Tor, то делали это через легальный файл tor.exe.

CTB-Locker не использует этот файл. Весь код, необходимый для общения с анонимной сетью Tor статистически связан с исполняемым файлом шифровальщика и запускается в отдельном протоколе.

Когда связь с Tor установлена и поднят локальный tor proxy сервер по адресу 127.0.0.1, выставляется глобальный флаг can_complete_circuit, который проверяется в потоке.

Как только это произошло, зловред осуществляет сетевую коммуникацию именно с этим локальным адресом. Запрос, посылаемый зловредом на сервер, содержит данные, необходимые для расшифровки файлов жертвы (рис. 3).

Рисунок 3 - Данные, отправляемые на командный сервер

В ответ сервер возвращает данные о стоимости разблокировки в биткойнах и долларах США, а также адрес кошелька для оплаты (рис. 4).

Так же хочется заметить, что перед шифрованием зловред производит сжатие данных.

Рисунок 4 - Данные, возвращаемые командным сервером

Для сжатия файлов зловред использует следующий алгоритм:

- файл жертвы перемещается во временный файл с помощью API-функции MoveFileEx;
- временный файл считывается с диска поблочно;
- каждый блок сжимается при помощи свободно распространяемой библиотеки Zlib;
- после сжатия блок шифруется и записывается на диск;
- в начало готового файла помещается служебная информация, которая понадобится для расшифровки;
- зашифрованный файл получает расширение ctbl.

Не менее интересным является тот факт, что зловред использует необычную схему шифрования.

Большинство семейств шифровальщиков используют для шифрования связку алгоритмов AES+RSA, но CTB-Locker отличился и здесь. В нем используется асимметричный протокол Диффи-Хеллмана на эллиптической кривой.

Первоначальный алгоритм Диффи-Хеллмана (так называемый протокол разделения секрета) был придуман достаточно давно и опубликован в 1976 г. знаменитыми криптографами Уитфилдом Диффи и Мартином Хеллманом.

Основные принципы работы протокола:

- существует возможность сгенерировать пару ключей — секретный (private) и открытый (public);
- из своего секретного и чужого открытого ключа можно сгенерировать так называемый разделяемый **(**общий**)** секрет (shared secret);
- если 2 абонента обменялись открытыми ключами (секретные ключи не передаются) и каждый независимо от другого вычислил разделяемый секрет из чужого открытого и своего секретного ключа, у обоих получится одно и то же значение;

- полученный разделяемый секрет можно использовать как ключ для любого симметричного алгоритма шифрования.

Высокоуровневая криптографическая схема зловреда выглядит следующим образом.

Генерация ключей:

- зловред генерирует пару master-public (открытый ключ) + master-private (секретный ключ);
- master-private вместе с другими данными в защищенном виде отправляется на сервер, а на клиенте не сохраняется;
- на каждый шифруемый файл генерируется новая пара session-public + session-private;
- вычисляется разделяемый секрет session-shared = ECDH(master-public, session-private).

Шифрование файла жертвы

- файл сжимается при помощи библиотеки Zlib;
- после сжатия Zlib каждый файл шифруется алгоритмом AES, в качестве ключа используется хэш SHA256(session-shared);
- после шифрования ключ session-public сохраняется в файл, а session-private не сохраняется;
- вычисленный разделяемый секрет session-shared также не сохраняется.

Расшифровка файла жертвы

По свойствам протокола Диффи-Хеллмана, верно следующее равенство: ECDH (master-public, session-private) = session-shared = ECDH(master-private, session-public). Именно это равенство является принципом, лежащим в основе работы зловреда.

При условии, что троянец не сохранил session-private и session-shared, остается всего 1 способ расшифровки – нужно вычислить ECDH(master-private, session-public). Чтобы это сделать, необходим ключ master-private (отправлен на сервер злоумышленников) и session-public (сохранен в начале зашифрованного файла). Других вариантов не существует, то есть без знания master-private не обойтись.

Передаваемый ключ возможно перехватить, но это все равно не позволит расшифровать файл, так как злоумышленники для шифрования сетевого трафика применили тот же самый протокол Диффи-Хелмана.

Данный зловред распространяется следующим образом. Бот Andromeda получает команду загрузить и запустить на зараженной

машине другой зловред Joleee. Тот, помимо своего основного функционала по рассылке почтового спама, поддерживает и выполнение ряда команд от злоумышленников, в том числе загрузку и запуск исполняемого файла. Как раз Joleee и скачивает на зараженную машину шифровальщика.

В настоящее время от этой угрозы существуют всего два способа защиты: резервное копирование и защитные решения – антивирусы.

Резервное копирование должно быть регулярным. Более того, оно обязательно должно осуществляться на носитель, недоступный в обычное время для записи с данной машины. Если пренебречь этим требованием, сохраненные резервные копии будут точно так же зашифрованы зловредом, как и основная версия файла.

Резервные копии необходимы в любой системе, в которой имеются файлы хоть какой-то важности. Даже если бы не было угрозы со стороны вредоносного ПО, не стоит забывать, что всегда возможен банальный отказ оборудования.

Защитный продукт – антивирус должен быть постоянно включен, никакие его компоненты не должны быть приостановлены, особенно «мониторинг системы» и «мониторинг активности», продукт должен иметь свежие базы. Но в большинстве случаев антивирусные программы определяют только устаревшие версии зловредов-вымогателей.

В заключение хочется сказать, что зловреды-вымогатели всегда представляли угрозу защищаемой информационной сфере, но на сегодняшний день они являются опаснейшим классом вредоносного ПО, который прошел огромный путь от обычно блокировки экрана, до шифрования абсолютно всех файлов, до которых он может дотянуться. При этом хочется отметить, что в последних семействах зловредов-вымогателей используются абсолютно новые решения, которые не позволяют отыскать злоумышленников или расшифровать свои данные без оплаты ключа. В настоящее время от этих угроз существует лишь один способ защиты – резервное копирование данных на переносной носитель, так как защитный продукт не всегда сможет определить новую версию зловреда.

Литература

1. Введение в информационную безопасность: учебное пособие для вузов [Текст]/Под ред. В.С.Горбатова / В. Фомичев, А. Малюк, В. Горбатов и др. – М.: Горячая линия-Телеком, 2011.

2. Галатенко В.А. Основы информационной безопасности: курс лекций: учебное пособие [Текст]/ Издание третье/ Галатенко В.А. под редакцией академика РАН В.Б.Бетелина/ - М.: ИНТУИТ.РУ, 2006
3. Синицын Ф. Новое поколение вымогателей. [Электронный ресурс] // SECURELIST [сайт]. URL: https://securelist.ru/analysis/obzor/21090/novoe-pokolenie-vymogatelej/ (дата обращения 22.11.2015)
4. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-
5. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
6. Соляной В.Н., Сухотерин А.И Выработка коммуникативной компетенции при подготовке профессионалов по информационной безопасности с использованием технологии модерации. «Инновационные технологии в современном образовании» // Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7
7. Соляной В.Н., Сухотерин А.И, Антоненко В.И. Проблемно-ориентированная подготовка специалистов по информационной безопасности с использованием имитационного метода (мозговой штурм). «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7.

8. Brian Donohue Луковое горе: новая версия трояна-вымогателя. [Электронный ресурс] // Kaspersky Lab Daily[сайт]. URL: https://blog.kaspersky.ru/new-version-ctb-locker/6792/ (дата обращения 22.11.2015)
9. Kaspersky Lab: Twitter [Интернет-портал]. URL: https://twitter.com/Kaspersky_ru/status/492558630672429056?ref_src=twsrc%5Etfw (дата обращения: 22.11.2015)
10. Zloy team: компьютерный форум [Интернет-портал]. URL: https://forum.zloy.bz/showthread.php?t=145783 (дата обращения: 22.11.2015)

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННОГО ПРОДУКТА VIPNET ДЛЯ ЗАЩИТЫ МОБИЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ПРЕДПРИЯТИЯ

Захаров Максим Вячеславович, студент 1 курса кафедры Информационной безопасности
Научный руководитель: **Соляной Владимир Николаевич,** к.воен.н., доцент, заведующий кафедрой Информационной безопасности

Ни для кого не секрет, что в настоящее время мобильные устройства оказывают все большее влияние на нашу повседневную жизнь. Растет спрос на мобильные устройства, параллельно с ним растут и угрозы информационной безопасности. Основные проблемы в этой области: очень быстрый рост вредоносного софта; хакерское программное обеспечение (ПО) стало более «умным; взломы производится при помощи вредоносных приложений.

Мобильные устройства, информационная безопасность, защита информации.

USING MODERN VIPNET PRODUCT TO PROTECT MOBILE ENTERPRISE INFORMATION SYSTEMS

Zakharov Maxim, 1st year student of the Department of information security
Scientific adviser: **Solyanoy Vladimir,** Candidate of Military Sciences, Assistant Professor, Head of the Department of information security

It's no secret that the current mobile devices are having an increasing influence on our daily lives. There is a growing demand for

mobile devices, in parallel with it grow and threats to information security. The main problems in this area: very rapid growth of malicious software; hacker software (software) has become more "intelligent; hacking is done by malicious applications.

Mobile devices, information security, information protection.

Появление планшетов, коммуникаторов и телефонов, при помощи которых стало возможно пользоваться многочисленными сетевыми сервисами и приложениями, сильно изменило корпоративные сети. Многие компании дали возможность своим сотрудникам и гостям офисов подключать мобильные устройства к сети при помощи Wi-Fi, пользователи стали повсевместно пользоваться Интернет по технологии 3G, корпоративные приложения стали доступны пользователям мобильных устройств. Такой подход удобен для бизнеса, но несет в себе целый ряд рисков информационной безопасности. Поскольку операционные системы и прикладное программное обеспечение мобильных устройств не обладают необходимыми функциями защиты информации и легко взламываются хакерами, при применении мобильных устройств в корпоративных сетях необходимо использовать специализированные средства защиты [1-11].

Компания «Инфотекс», российский разработчик программных, программно-аппаратных VPN-решений и средств криптографической защиты информации, объявила о выпуске нового приложения для мобильных устройств ViPNet Connect. ViPNet Client for Android — это приложение, работающее под управлением операционной системы Android, предназначенное для обеспечения защиты устройства от сетевых атак, и позволяющее получить доступ посредством защищенного технологиями ViPNet VPN туннеля, к ресурсам корпоративной сети.

Поддержка последней операционной системы Android, новинка позволит корпоративным пользователям обмениваться важной бизнес-информацией по защищенным каналам с помощью чата, ViPNet Client for Android, который стал первым в России сертифицированным ФСБ продуктом для ОС Android, реализующим шифрование IP-трафика на алгоритме ГОСТ 28147-89. Данное положение и определяет новизну работы.

ViPNet Client for Android после установки на устройство перехватывает любой IP трафик, обеспечивая его прозрачное

шифрование. Выпуск ViPNet Connect for Android стал следующим логичным шагом в части развития продуктов для обеспечения безопасности в корпоративной мобильной среде. Так же Новинка позволит корпоративным пользователям обмениваться важной бизнес-информацией по защищенным каналам с помощью чата, а также при голосовых вызовах, сообщили. Компания представила программный комплекс ViPNet Client for Android, который стал первым в России сертифицированным ФСБ продуктом для ОС Android, реализующим шифрование IP-трафика на алгоритме ГОСТ 28147-89, что и позволяет использовать мобильные устройства при подключении к корпоративным сетям государственных учреждений [1-11].

По словам разработчиков, ViPNet Connect представляет собой альтернативу использованию в корпоративных целях мессенджеров публичных сервисов Skype, Facebook, «ВКонтакте», WhatsApp, Viber и др., которые несут множество рисков для безопасности организации.

Рисунок 1 - Меню Vipnet

Продукт дополняет ранее выпущенный программный комплекс ViPNet Client for Android, который также получил крупное обновление: в частности, расширен список поддерживаемых мобильных устройств (в том числе работающих на базе архитектуры x86), оптимизирована интеграция с другими продуктами линейки ViPNet, возможна установка на устройство без прав администратора (root-прав). Важным отличием программного комплекса ViPNet Connect от известных мессенджеров является возможность

обеспечения защиты точка-точка, без задействования промежуточных серверов при передаче конфиденциальных данных, указали в компании. Сегодня для установки на мобильные устройства доступна версия ViPNet Connect for Android 1.1, в которой реализованы наиболее востребованные по отзывам потенциальных клиентов функции чата и голосовых вызовов. В следующих версиях запланировано добавление функций видеоконференцсвязи и передачи файлов и контента, возможности «приземлить» звонок на стационарный номер. При совместной установке ViPNet Client for Android и ViPNet Connect составляют комплексное решение для защиты конфиденциальных данных, сочетающее в себе удобство установки и использования, современный графический интерфейс, безопасность в соответствии с требованиями российского законодательства.

Рисунок 2 – Функции Vipnet

Дополнительно корпоративные пользователи смогут защищать с помощью шифрования и электронной подписи файлы любого формата, передаваемые по открытым каналам связи, с помощью бесплатного продукта ViPNet CryptoFile for Android. Шифрование и подпись файлов осуществляется с использованием алгоритмов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012, на базе технологии PKI. Отправка защищенного документа доступна из приложения любыми доступными каналами: почта, WhatsApp, Viber, Telegram и т.д. Продукты ViPNet Client for Android и ViPNet Connect поддерживают работу в ОС Android версии 4.x. и 5.x. При этом поддерживаются современные устройства производства Yota Devices (YotaPhone) и широкий список устройств Samsung. Дополнительно доступна версия ViPNet Connect для установки на компьютер под управлением ОС Windows, OS X. Приложение ViPNet Connect реализует информационный обмен между пользователями через защищенную

ViPNet-сеть, исключая возможность перехвата конфиденциальной и навязывания ложной информации [1-11].

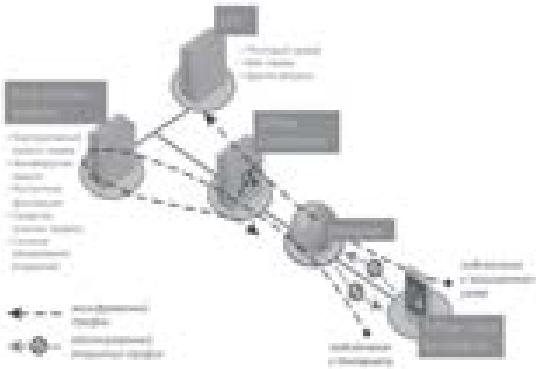


Рисунок 3 - Особенности работы VIPnet

После активации защитных функций ViPNet Client for Android доступ к открытым ресурсам Интернет возможен только с использованием защищенных корпоративных proxy-серверов, доступных через VPN-туннель. Обеспечивается эффективная многоуровневая защита мобильного устройства – антивирусная защита и контентная фильтрация, причем без установки дополнительного программного обеспечения на каждое, что немаловажно, учитывая ограниченные возможности автономной работы мобильных устройств. Для управления функциями ViPNet Client for Android используется графический интерфейс, дизайн которого выполнен в стандартах операционной системы Android, существует возможность использовать виджеты на рабочий стол, отображающие текущий статус подключения.

В качестве вывода в данной работе можно отметить что продукт был проанализирован и на основе этого можно назвать конкретные недостатки и преимущества:

Преимущества Vipnet:

- безопасное подключение к корпоративной сети из любых публичных Wi-Fi-сетей, а также сетей связи 2G/3G/4G;
- наличие сертификата ФСБ;
- использование российского алгоритма шифрования ГОСТ 28147-89;
- наличие дополнения ViPNet Connect for Android для организации защищенных коммуникаций;
- переключение между IP-сетями без разрыва сеанса связи;

- оптимизация зашифрованных потоков данных;
- интеграция с другими продуктами, входящими в инфраструктуру ViPNet.

Недостатки Vipnet:

- гарантированная корректная работа только для небольшого списка совместимых устройств;
- ViPNet Connect for Android пока имеет минимальный набор функций, однако разработчики обещает в скором времени добавить сервис обмена файлами и режим конференции.

Литература

1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус.-2013. С.15-16.
2. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс- 2010.С. 34-40
3. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ.- 2010. С.112-130
4. Соляной В.Н., Сухотерин А.И. Практика применения инновационного научно-образовательного комплекса по подготовке бакалавров и магистров в области информационной безопасности. Научно-практический журнал №25, том 1 2015г. Информационное противодействие угрозам терроризма. Материалы XIX Пленума учебно-методического объединения по образованию в области информационной безопасности «опыт и передовые практики образовательных организаций по формированию и использованию в учебном процессе специализированной учебно - лабораторной базы» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН.ФЕД.УНИВ, 2015.-416 с. ISSN 2219-8792
5. Соляной В.Н., Сухотерин А.И. Модульно-ориентированный подход формирования базовых дисциплин ФГОС ВО 3+ как основа реализации профессиональной подготовки бакалавров в области информационной безопасности Научно-практический журнал №25, том 2 2015г. Информационное противодействие угрозам терроризма Материалы XIX Пленума учебно-методического объединения по образованию в области информационной безопасности «учебно-методическое обеспечение образовательных программ в области информационной безопасности» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН.ФЕД.УНИВ, 2015.-332 с. ISSN 2219-8792

6. Соляной В.Н., Сухотерин А.И. Становление направления «Радиоэлектронная безопасность информационных объектов» в системе дополнительного профессионального по информационной безопасности. Научно-практический журнал №25, том 2 2015г. Информационное противодействие угрозам терроризма Материалы XIX Пленума учебно-методического объединения по образованию в области информационной безопасности «учебно-методическое обеспечение образовательных программ в области информационной безопасности» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН.ФЕД.УНИВ, 2015.-332 с. ISSN 2219-8792
7. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Некоторые перспективы применения систем контроля и управления доступом в региональных ВУЗАХ. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУЗов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
8. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Развитие сотрудничества российских и зарубежных ВУЗОВ по защите информационного ресурса. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУЗов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
9. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
10. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества.

Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
11. Соляной В.Н., Сухотерин А.И Выработка коммуникативной компетенции при подготовке профессионалов по информационной безопасности с использованием технологии модерации. «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7
12. Соляной В.Н., Сухотерин А.И, Антоненко В.И. Проблемно-ориентированная подготовка специалистов по информационной безопасности с использованием имитационного метода (мозговой штурм). «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7.

ТЕХНОЛОГИЯ АКТИВНОЙ ЗАЩИТЫ PROTECT В ЯНДЕКС-БРАУЗЕРЕ

Звездов Артём Рудольфович, Аникин Артём Анатольевич,
студенты 1 курса кафедры Информационной безопасности
Научный руководитель: **Соляной Владимир Николаевич,** к.воен.н., доцент, заведующий кафедрой Информационной безопасности

Интернет уже давно стал частью повседневной жизни, и практически все явления окружающего мира в нём так или иначе присутствуют. В том числе не самые приятные. Мошенники тоже используют сеть: крадут чужие пароли и денежные средства, выманивают у пользователей личные данные, рассылают спам с чужих адресов и аккаунтов. Браузер — основная программа для связи с Интернетом. В таких условиях ему недостаточно быть удобным, быстрым и надёжным. Одним из важнейших требований становится безопасность. Браузер должен предотвращать угрозы заранее, ещё до того, как данным или устройству нанесён ущерб.

Интернет, безопасность, защита, Яндекс Браузер, Protect.

THE TECHNOLOGY OF ACTIVE PROTECTION YANDEX BROWSER

Zvezdov Artyom, Anikin Artyom, 1st year students of the Department of information security
Scientific adviser: **Solaynoy Vladimir**, Candidate of Military Sciences, Associate Professor, Head of the Department of information security

Internet has already become a part of daily life, so there is no wonder that almost all the phenomena of the world are related with it one way or another, including not the most pleasant of them. Hackers use the Web too, stealing other's passwords and money, spamming on behalf of other users.

The browser is a main program for the internet connection. In such cases it can't be easy-to-use, high speed and safe. That is why security is one of the most important requirements. The browser should prevent all the threats before it can cause damage to the device.

Internet, security, protection, Yandex Browser, Protect.

В данной работе рассмотрены новая комплексная технология обеспечения безопасности – Protect. Яндекс Protect – новая технология активной защиты пользователей от различных интернет угроз. Данная технология встроена в новой версии Яндекс.Браузера и защитит от четырех основных типов интернет угроз:

- антифишинг – защита от кражи паролей;
- защита Wi-Fi соединений;
- блокирование запуска вирусных страниц;
- проверка на вирусы загружаемых файлов.

Первой ключевой частной технологией реализуемой с использованием системы Protect является защита паролей от кражи. Всё важное в интернете защищено паролями. Они открывают доступ к переписке, файлам в облачном хранилище, денежным средствам на банковском счёте. Для кражи паролей злоумышленники используют в том числе «фишинговые» сайты. Жертва получает письмо якобы от службы поддержки какого-нибудь популярного сайта и по ссылке переходит на страницу, которая выглядит точь-в-точь как этот сайт. Часто письмо пугает блокировкой аккаунта или заморозкой средств на счёте — от волнения пользователь теряет бдительность и вводит свой пароль, который попадает владельцу сайта-клона.

Яндекс.Браузер предостерегает пользователей, когда они начинают вводить пароль на подозрительных страницах. У Браузера есть список важных сайтов, пароли от которых нужно защищать: почтовые сервисы, социальные сети, сайты банков и платёжных систем. В него попадают и сервисы, пароли от которых пользователь сохранил сам. Также в браузере хранятся хеши паролей для этих сайтов. Хеш — это своего рода отпечаток пароля, строка фиксированной длины из цифр и латинских букв, получаемая в ходе криптографического преобразования.

Как только пользователь устанавливает курсор мыши в поле для ввода пароля на любом сайте, которого нет в списке, активируется система защиты. Когда пароль набран до конца, Яндекс.Браузер вычисляет его хеш и временно блокирует отправку данных в сеть. Если полученный хеш совпадает с одним из отпечатков, хранящихся в браузере — то есть пользователь вводит пароль от важного сайта на другой странице — показывается предупреждение (рис.1).

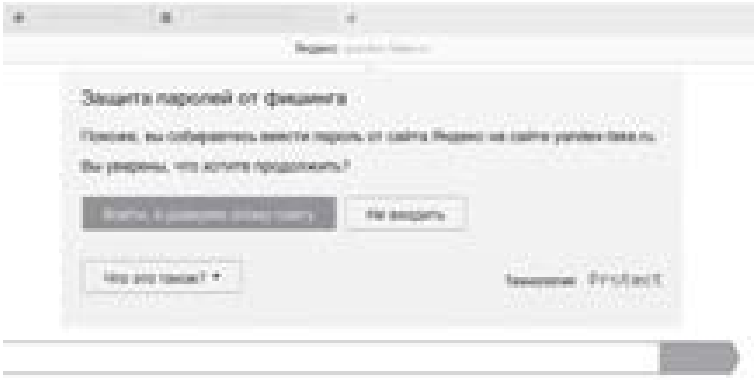


Рисунок 1 - Фрагмент интерфейса Яндекс по организации защиты паролей от фишинга

Если пользователь знаком с этим ресурсом и доверяет ему, то уже введённый пароль передаётся на сайт и происходит авторизация. При отказе от входа заполненное поле очищается, поэтому пароль не могут перехватить.

Защита Wi-Fi соединений – вторая технология данной системы. Публичные сети Wi-Fi — например, бесплатный интернет в ресторанах, торговых центрах, аэропортах и других общественных местах — часто полностью открыты и не требуют пароля для

подключения или защищены крайне ненадёжным WEP-шифрованием (Рис.2).

Подключаясь к такому Wi-Fi, пользователь делит сеть со всеми окружающими. Незнакомец за соседним столиком в кафе может запустить на своём компьютере, планшете или даже телефоне специальную программу-сниффер— она перехватывает все данные, которые передают другие участники сети. Или он может использовать своё устройство в режиме точки доступа, развернув сеть с распространённым названием — например, FREE_WiFi_Guest. Все, кто раньше пользовался настоящей сетью с таким именем, даже в другом месте, подключатся к поддельному Wi-Fi автоматически, просто оказавшись в радиусе его действия. Данные ничего не подозревающих людей будут проходить через устройство злоумышленника.

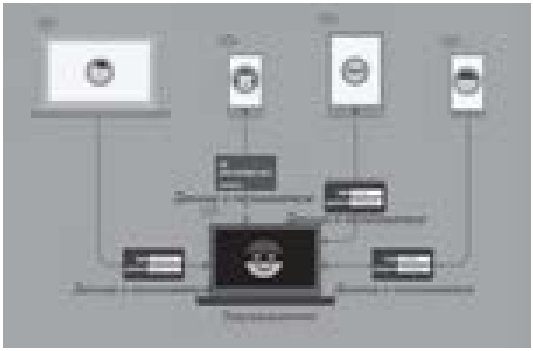


Рисунок 2 – Взлом публичной сети Wi-Fi

Сегодня большинство крупных сайтов (Яндекс, Google, Mail.Ru, Facebook, ВКонтакте) используют защищённый протокол HTTPS с шифрованием, который исключает подобное вмешательство. Но очень многие ресурсы в интернете по-прежнему используют стандартный HTTP-протокол без какой-либо защиты. Авторизуясь на таких сайтах через публичный Wi-Fi, пользователь фактически отправляет свой логин и пароль в открытом виде, и перехватить их не составляет никакого труда. С ними злоумышленники нередко могут проникнуть и в основной почтовый ящик жертвы, на который зарегистрированы все важные аккаунты, ведь многие люди ради удобства используют одинаковые пароли на разных сайтах.

В Яндекс.Браузере для компьютера и мобильных устройств есть защитная функция под названием «Безопасный Wi-Fi». В ней

применяется та же технология, что и в режиме Турбо. При активации «Безопасного Wi-Fi» трафик со всех сайтов, где используется обычный HTTP, проходит через сервер Яндекса, только никак не обрабатывается и не сжимается. Фактически сервер выступает в роли шлюза — Яндекс.Браузер подключается к нему по защищённому HTTPS-протоколу, и обмен информацией между устройством пользователя и сайтом происходит через это надёжно зашифрованное подключение.

Данные с тех сайтов, которые поддерживают HTTPS, передаются напрямую — они уже зашифрованы, поэтому дополнительный шлюз для их безопасной передачи не требуется. Режим «Безопасный Wi-Fi» включается автоматически, как только пользователь оказывается в беспроводной сети без пароля или со слабым шифрованием (рис. 3).

Рисунок 3 - Фрагмент интерфейса Яндекс по организации защиты Wi-Fi соединений

Третья ключевая часть защиты — блокирование запуска вирусных страниц. Яндекс ежедневно проверяет десятки миллионов страниц на наличие вредоносного кода — это происходит одновременно с индексированием интернета. Помимо сайтов, специально созданных для распространения вирусов, опасность могут представлять и добропорядочные ресурсы: периодически злоумышленникам удаётся взламывать даже очень популярные и высокорейтинговые сайты и распространять через них вредоносные программы. Кроме того, поисковый робот Яндекса умеет определять страницы, связанные с смс-мошенничеством. Для этого разработан специальный алгоритм, который хранится в тайне — чтобы мошенники не могли придумать способ его обойти.

Адреса заражённых и мошеннических сайтов попадают в специальную базу данных, которая обновляется несколько раз в сутки и включает сотни тысяч ссылок. При попытке открыть любую из них через Браузер загрузка сайта блокируется, а пользователь видит

предупреждение (рис. 4), после которого можно открыть безопасную копию сайта или уйти со страницы.

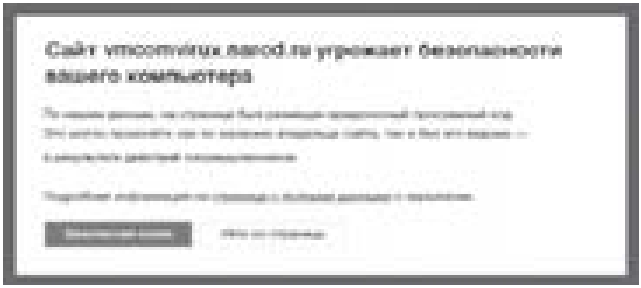


Рисунок 4 - Пример блокировки вредоносного сайта

Это универсальная технология, которая используется не только в Яндекс Браузере, но и в результатах поиска, Элементах Яндекса, сервисе Яндекс DNS. Более того, выводить такие предупреждения для своих пользователей может создатель любого сайта или приложения — доступ к технологии открыт для всех.

Заключительной технологией данной системы является проверка на вирусы загружаемых файлов. Любой скачанный в интернете файл может содержать в себе вредоносный код. Поэтому технология Protect включает в себя проверку всех загружаемых файлов. Антивирус работает в облаке на серверах Яндекса и проводит анализ по множеству критериев.

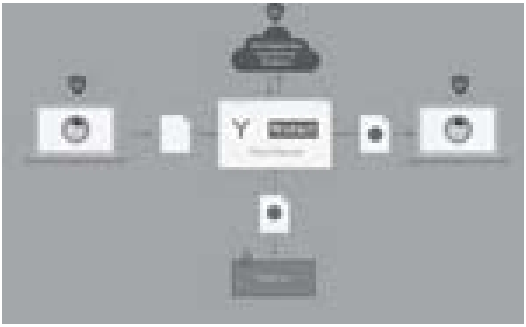


Рисунок 5 - Проверка загружаемых файлов на наличие вредоносных программ

Проверка файла начинается ещё в процессе загрузки. Яндекс Браузер выделяет некоторые его характеристики и отправляет их для проверки в антивирусное облако. В большинстве случаев этих сведений достаточно, чтобы определить наличие вредоносного

содержимого. Весь файл целиком не передаётся, поэтому проверка проходит максимально быстро. В более сложных случаях антивирус сам запрашивает у браузера дополнительные сведения о файле или его фрагменты для тщательного анализа.

Если файл опасен, Яндекс Браузер показывает предупреждение. Одновременно меняется расширение файла, чтобы обезвредить его на то время, пока пользователь решает его дальнейшую судьбу. Аналогичным образом действуют обычные антивирусные программы, помещая обнаруженные на компьютере заражённые файлы в «карантин».

Таким образом, в данном выступлении представлена новая комплексная технология активной защиты Protect в Яндекс Браузере, которая позволяет предупреждать пользователя до того, как произошло что-то неприятное. Protect — первая комплексная технология защиты среди браузеров, которая оберегает сразу от большинства неприятностей: потери своих аккаунтов из-за украденного пароля, заражения компьютера на вредоносной странице, вмешательства посторонних при работе в общественной сети. Кроме этого, Protect активно развивается, и в будущих версиях Яндекс Браузера его защита будет дополнена новыми механизмами для предотвращения других угроз.

Литература

1. Малюк А.А. Введение в информационную безопасность. - М.: Горячая линия - Телеком, 2011

2. Белов Е.Б. Основы информационной безопасности. - М.: Горячая линия - Телеком, 2006

3. Хорев А.А. Защита информации от утечки по техническим каналам: Учебн. пособие. - М.: МО РФ, 2006

4. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Некоторые перспективы применения систем контроля и управления доступом в региональных ВУЗАХ. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.

5. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Развитие сотрудничества российских и зарубежных ВУЗОВ по защите информационного ресурса. «Перспективы организационные формы и

эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
6. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
7. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
8. Соляной В.Н., Сухотерин А.И Выработка коммуникативной компетенции при подготовке профессионалов по информационной безопасности с использованием технологии модерации. «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7
9. [Электронный ресурс]. Режим доступа: http://www.comss.info/
10. [Электронный ресурс]. Режим доступа: https://yandex.ru/

ВЛИЯНИЕ ГЕОПАТОГЕННЫХ ЗОН НА ЭФФЕКТИВНОСТЬ ТЕХНОЛОГИЙ ЗАЩИТЫ ИНФОРМАЦИИ

Зирина Мария Алексеевна, студентка 4 курса кафедры Информационной безопасности
Научный руководитель: **Соляной Владимир Николаевич**, к.воен.н., доцент, заведующий кафедрой Информационной безопасности

Активность пространства - это показатель скорости протекания различных процессов. Геопатогенная зона представляет собой локальную геофизическую аномалию в виде слабых электромагнитных полей Земли естественного происхождения, а также техногенного происхождения (связанные с деятельностью человека). Физические процессы, протекающие в геопатогенных зонах, во многом связаны с формированием в них так называемых волн, которые сбивают собственные биоритмы организма, а так же способны повлиять на ход работы технического оборудования.

Геопатогенная зона, активность пространства, резонанс, человек, техника.

INFLUENCE OF GEOPATHIC ZONES ON THE EFFECTIVENESS OF INFORMATION SECURITY TECHNOLOGIES

Zirina Maria, 4rd year student of the Department of information security
Scientific adviser: **Solaynoy Vladimir,** Candidate of Military Sciences, Associate Professor, Head of the Department of information security

Active space - a measure of the speed of various processes. Geopathogenic zone is a local geophysical anomalies in the form of weak electromagnetic fields of the Earth naturally occurring and man-made origin (associated with human activity). Physical processes in the geopathogenic zones, largely due to the formation in them the so-called waves who knocked own biorhythms of the body, as well as able to influence the course of the technical equipment.

Geopathic zone, activity space, resonance, human, machinery.

Земная поверхность, в зависимости от рельефа местности, качества залегаемых пород, наличия под поверхностью водных жил и пустот, своеобразно концентрирует и перераспределяет полученную из Космоса энергию (рис.1). В результате этого процесса над

поверхностью земли образуются особые энергетические зоны, которые могут отрицательно, положительно или нейтрально влиять на здоровье человека. Зоны с отрицательной для человека энергетикой называют «геопатогенными зонами» [5].

Некоторые геопатогенные зоны обладают такой энергетикой, что в них разрушаются строительные конструкции.

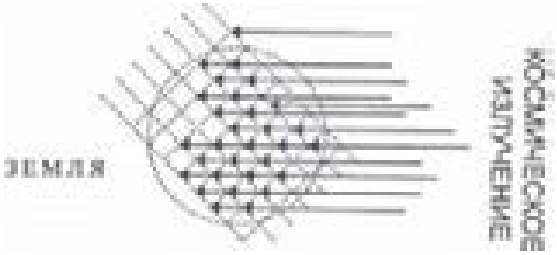


Рисунок 1 - Происхождение земной геобиологической сетки

Прежде всего необходимо определить, что мы будем понимать под «технологией защиты информации».

Рисунок 2 – Элементы информационных технологий, подлежащие исследованию

Физические процессы, протекающие в геопатогенных зонах, во многом связаны с формированием в них так называемых автоволн, которые сбивают собственные биоритмы организма. При длительном воздействии это приводит к невозможности функционирования организма в оптимальном режиме [6]. Организм человека, проживающего в геопатогенной зоне, вынужден постоянно тратить повышенное количество энергии, следствием чего являются заболевания центральной нервной системы.

Результаты широкомасштабных исследований в Швейцарии, Бельгии, Франции, Австрии, Чехословакии показывают, что от 50 до 80% онкологических заболеваний связаны с тем, что больные

длительное время проводили в местах воздействия геопатогенных излучений.

Люди, проводящие много времени в патогенной зоне, жалуются на бессонницу или состояние глубокого мертвоподобного сна, пробуждаясь от которого, человек чувствует себя наутро полностью истощенным [4]. Влияние геопатогенных зон на биополе человека:

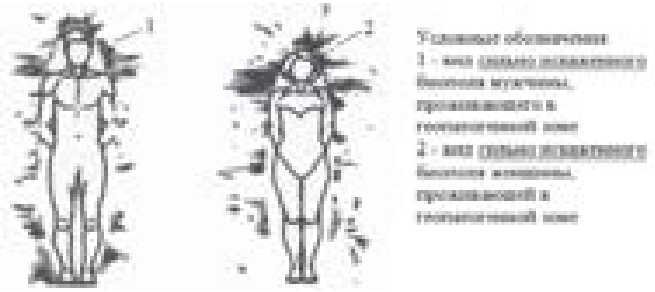


Рисунок 2 - Биополя молодой пары, проживающей в геопатогенной зоне

Длительное нахождение людей в геопатогенной зоне приводит к сильному искажению их биополей.

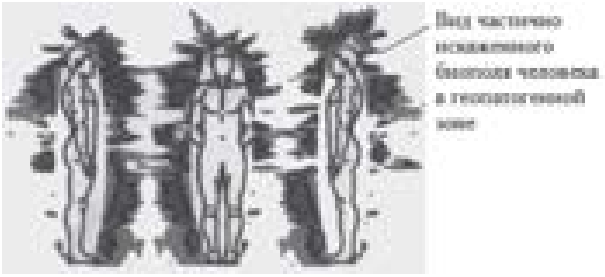


Рисунок 3 - Биополе человека после 8 часов сна в геопатогенной зоне

Длительное пребывание людей в геопатогенных зонах вызывает следующие общие симптомы:

- чувство дискомфорта;
- общую слабость, сонливость или бессонницу;
- головные боли;
- нервозность, чувство страха;
- жжения и покалывания в теле;
- судороги в ногах, охлаждение конечностей;
- антипатию к спальному месту;

— усталость и утомление утром после сна.

Активность пространства - это показатель скорости протекания различных процессов. Как его можно себе представить? Проведём умственный эксперимент: посадим в двух различных помещениях с одинаковыми микроклиматическими условиями в идентичные горшки с одинаковой почвой семена какого-нибудь цветка. Будем поливать оба горшка по одинаковому расписанию и одним и тем же количеством воды из идентичного источника. В результате, после прохождения определённого времени мы увидим, что в одном помещении цветки всходят раньше и растут быстрее, а также дают более красивые и большие цветы по сравнению со цветами в другом помещении.

Исходя из этого умственного опыта, мы можем сказать, что в одном помещении уровень активности пространства выше (где цветы росли быстрее), чем в другом. Однако при желании в подобном эксперименте скептик найдёт очень много оправданий полученных результатов, при этом исключая понятие активности пространства.

До последнего времени не существовало научного (так называемого, объективного) метода для непосредственной оценки активности пространства. Приходилось довольствоваться мнениями лозоходцев или же результатами подобных вышеприведенному экспериментов, которые посредственно (скорость всхождения семян, скорость развития биообъектов и пр.) позволяли определять уровень активности [2, 3].

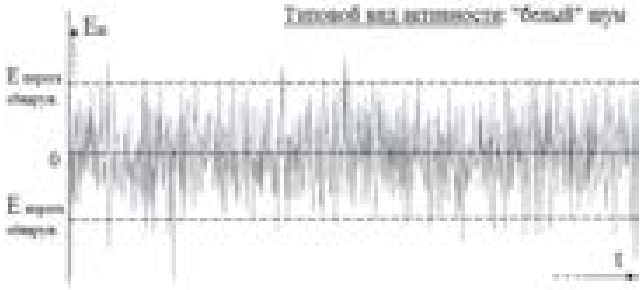


Рисунок 4 - Графическое представление активности пространства, находящегося вне геопатогенной зоны

Проведя сравнение рис.3 и рис.4, можно сделать вывод, что геопатогенная зона характеризуется наличием необъяснимых, отличающихся от общего фона активности пространства, волн.

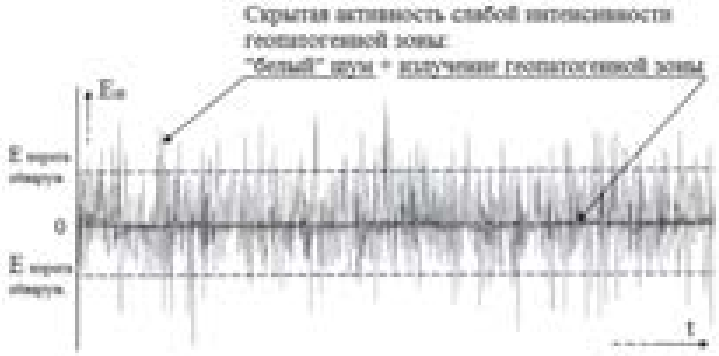


Рисунок 5 - Графическое представление скрытой активности слабой интенсивности пространства геопатогенной зоны

Влияние геопатогенных зон может носить как скрытый, так и явный характер. Почему же это происходит? Одним из возможных ответов на вопрос о проявлении действий геопатогенных зон может быть наличие эффекта резонанса в пространстве. В таком случае не имеющие проявления волны, действующие в геопатогенной зоне, за счет резонансного эффекта начинают проскакивать на фоне общей активности пространства (рис.6).

Рисунок 6 - Графическое представление резонансной активности пространства геопатогенной зоны

Резона́нс — явление резкого возрастания амплитуды вынужденных колебаний, которое наступает при совпадении частоты собственных колебаний с частотой колебаний вынуждающей силы.

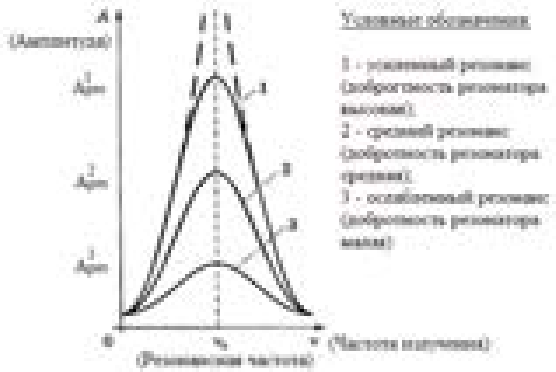


Рисунок 7 - Эффект резонанса для разных частот внешнего воздействия

На проявление активности таких зон может влиять:

1)Электромагнитный резонанс;

2) Механический резонанс.

Рассмотрим влияние механического резонанса на примере комнаты. Комнату (рис.9) можно сравнить с резонатором на основе волновода прямоугольного типа (рис.8). Волновод можно использовать не только как канал передачи электромагнитной энергии, но и в качестве резонатора – высокодобротного СВЧ колебательного контура [1]. Резонансная частота такого устройства определяется числом волн, укладывающихся по разным стенкам волновода. Таким же образом полуволны геопатогенных зон укладываются по стенам комнаты, вызывая ощутимое проявление.

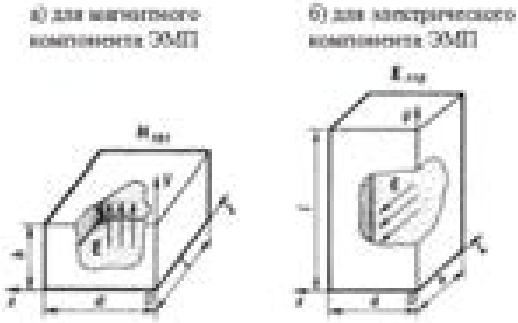


Рисунок 8 - Резонаторы на основе волновода прямоугольного типа

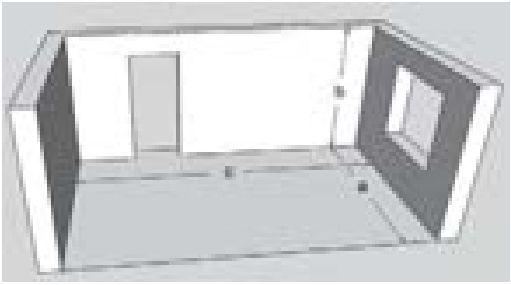


Рисунок 9 - Схематическое представление комнаты, как объемного резонатора

В таком случае длины резонансных волн определяются выражением (1)

$$л_{p} = \frac{2}{\sqrt{(\frac{m}{a})^2+(\frac{n}{b})^2+(\frac{p}{c})^2}}, \qquad (1)$$

где **m, n, p** – целые положительные числа, **a, b,c** –ширина, высота и длина объекта [1].

Данную формулу (1) можно использовать при работе с техникой, например, системный блок так же имеет формулу параллелепипеда, что позволяет его представить в качестве резонатора. Отдельные радиоэлектронные компоненты (резисторы, транзисторы и др.) так же можно рассматривать как некие объемные резонаторы, и в определенных условиях в них проявляется аналогичные резонансные процессы, приводящие к механическому разрушению.

Зная параметры механических компонентов защищаемых информационных систем, можно прогнозировать деструктивное проявление различных геомагнитных излучений. При этом, можно обосновывать различные защитные механизмы в целях противодействия вышеуказанным резонансным эффектам от геопатогенных зон, что является достаточно актуальной исследовательской задачей и в дальнейшем предусматривается проведения дополнительных исследований по данном направлению.

Сделаем несколько выводов:

1. Геопатогенные зоны способны влиять на человека, технику и процессы, в виде скрытых деструктивных излучений (малой интенсивности).

2. Причиной усиления деструктивного влияния геопатогенных зон на человека, технику и процессы следует рассматривать наличие резонансного эффекта.

3. Результатом воздействия геопатогенных зон на: а) человека - ухудшение жизненных показателей; б) технику – выход из строя, нарушение работы; в) процессы – искажение привычного хода работы всех систем.

4. В качестве резонатора могут выступать помещения, техническое оборудование и другие объемные объекты, участвующие в процессе обработки, хранения, передачи защищаемой информации.

Таким образом, в работе показаны характеристики геопатогенных зон и наличие скрытых воздействий от них за счет резонансного эффекта на субъект и технику, которые являются основными компонентами технологии ИБ.

Литература

1. Каганов В.И. Радиотехника: учеб. пособие для студ. сред. проф. образования. – М. : Издательский центр «Академия», 2006. – 352 с.

2. Орлов Д.В., Коротков К.Г. Измерение энергетических характеристик пространства методом газоразрядной визуализации. / VIII международная Крымская конференция «Космос и Биосфера» (Судак, 28 сент.–3окт. 2009 г.): тезисы. С. 251–253.

3. Орлов Д.В., Петрова Е.Н., Чайкун К.Е. Параметрические зависимости частотно-резонансных оптоэлектронных контуров. // Научно-технический вестник СПбГУ ИТМО. 2008. № 48. С. 225–232.

4. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.

5. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский

Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
6. Соляной В.Н., Сухотерин А.И Выработка коммуникативной компетенции при подготовке профессионалов по информационной безопасности с использованием технологии модерации. «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7
7. Соляной В.Н., Сухотерин А.И, Антоненко В.И. Проблемно-ориентированная подготовка специалистов по информационной безопасности с использованием имитационного метода (мозговой штурм). «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. – М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7.
8. Электронный ресурс. Режим доступа: http://gamma7.m-l-m.info/zashhita-ot-elektromagnitnogo-izlucheniya/vliyanie-elektromagnitnogo-izlucheniya-na-cheloveka/geopatogennye-zony/
9. Электронный ресурс. Режим доступа: http://www.aurastudia.ru/stat/52.
10. Электронный ресурс. Режим доступа: http://www.geopatogennizony.com
11. Электронный ресурс. Режим доступа: ru/geopatogennie-zoni

ДЕСТАБИЛИЗИРУЮЩЕЕ ВОЗДЕЙСТВИЕ ИНФРАЗВУКА НА ПЕРСОНАЛ ПРЕДПРИЯТИЯ КАК НОСИТЕЛЕЙ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

Клюшина Евгения Александровна, студентка 1 курса кафедры Информационной безопасности
Научный руководитель: **Соляной Владимир Николаевич**, к.воен.н., доцент, заведующий кафедрой Информационной безопасности

Статья посвящена проблеме защиты персонала и руководства предприятия от негативного воздействия инфразвука. Выделяются и описываются характерные особенности инфразвука и его источники. Показано что инфразвук имеет способность негативно влиять на организм человека, подрывая тем самым его

деятельность. На основе исследования выявлены способы защиты человека от вредного воздействия инфразвука.

Инфразвук, информационные объекты, инфразвуковое оружие.

THE DESTABILIZING EFFECTS OF INFRASOUND ENTERPRISE PERSONNEL AS CARRIERS OF INFORMATION TO BE PROTECTED

Klyushina Evgenia, 1st year student of the Department of information security
Scientific adviser: **Solaynoy Vladimir**, Candidate of Military Sciences, Associate Professor, Head of the Department of information security

This article is devoted to the protection of personnel and leadership from negative impact of infrasound. Stand and describes the characteristics of infrasound and its sources. Found that infrasound has an ability to affect on the human organism negatively, by that undermining his activity. On the base of the research identified ways of protection human from harmful effect of infrasound.

Infrasound, information objects, infrasound weapons.

В современном мире в связи с ростом количества малых, средних и крупных предприятий заметно возрос уровень конкуренции. Вследствие чего компании пытаются избавиться от конкурентов. Одним из способов подрыва деятельности предприятия является воздействие инфразвука на персонал, а так же руководство данного предприятия [1-12].

Инфразвук (от лат. infra — ниже, под) — упругие волны, аналогичные звуковым, но имеющие частоту ниже воспринимаемой человеческим ухом. За верхнюю границу частотного диапазона инфразвука обычно принимают 16—25 колебаний в секунду (Гц), за нижнюю же границу инфразвукового диапазона принимают 0,001 Гц (см. рис. №1).

Рисунок 1-частотные диапазоны звуков

Общеизвестно, что инфразвук подчиняется общим закономерностям, характерным для звуковых волн, однако в связи с наличием у него низкой частоты колебаний упругой среды обладает целым рядом особенностей представленных в таблице №1.

Таблица 1- Особенности взаимодействия инфразвука со средой

н\п	Основные характеристики инфразвука по взаимодействию со средой
1	Инфразвук имеет гораздо большие амплитуды колебаний в сравнении с равномощным слышимым человеком звуком (скрытое воздействие высокой мощности на информационные объекты: сотрудники и руководство предприятия)
2	Инфразвук гораздо дальше распространяется в воздухе, поскольку поглощение инфразвука атмосферой незначительно (дистанционное воздействие на персонал предприятия: руководящий состав, штатные сотрудники)
3	Благодаря большой длине волны для инфразвука характерно явление дифракции, вследствие чего он легко проникает в помещения и огибает преграды, задерживающие слышимые звуки (Высокая проникаемость на закрытые информационные объекты: служебные здания и помещения предприятия)
4	Инфразвук вызывает вибрацию крупных объектов (зданий, техники), так как входит в резонанс с ними (Резкое возрастание деструктивного воздействия на информационные объекты).

Выше перечисленные особенности инфразвука затрудняют борьбу с ним, поскольку обычные способы противошумовой борьбы (звукопоглощение, звукоизоляция, удаление от источника звука, акустическая обработка поверхностей помещения) против инфразвука являются низкоэффективными.

В качестве основных техногенных источников инфразвука можно рассматривать мощное оборудование - тяжёлые станки, ветрогенераторы, вентиляторы, электродуговые печи, поршневые компрессоры, турбины, виброплощадки, сабвуферы, водосливные плотины, реактивные двигатели, судовые двигатели и т.д. Природные источники мощного инфразвука – волны, землетрясения, ураганы, извержения вулканов, резкие колебания давления в атмосфере и пр. В настоящее время в этой вредной области инфразвука человек быстро догоняет природу и в ряде случаев уже перегнал ее. Поэтому в наше время все чаще можно услышать о том, что инфразвук можно умышленно использовать как оружие.

Инфразвуковое оружие (рис. № 2) — одно из видов ОМП (оружия массового поражения), использующее в качестве поражающего элемента частоту инфразвука, ниже 20 Гц. В зависимости от мощности инфразвукового влияния результатами могут быть возникновения у объекта от ощущения некомфортного состояния до соматических расстройств.

Рисунок 2 - Инфразвуковое оружие - Sonic Devestator: «пистолет», испускающий звуковые волны частотой от 15 до 30 килогерц, и вызывающий боль и дискомфорт у жертвы

В ходе многочисленных исследований выявлено, что звуковые колебания с частотой 19 Гц, воздействуют на глазные яблоки, тем самым являясь причиной расстройства зрения и видений различного рода. К примеру, изучение плохого самочувствия сотрудников конструкторского бюро, расположенного недалеко от полигона, на котором испытывались реактивные двигатели для самолета «Конкорд» показало, что во время испытаний двигателей в помещении устанавливался высокий уровень интенсивности инфразвука. Другими словами, необычные симптомы, возникавшие у людей, были обусловлены низкочастотными компонентами звука, присутствовавшими в спектре шумов реактивного двигателя.

По данным исследований, проведенных в некоторых странах, инфразвуковые колебания могут оказывать влияние на центральную нервную и пищеварительные системы, тем самым вызывая паралич, рвоту и спазмы, приводить к общему недомоганию и болевым ощущениям внутренних органов. При более же высоких уровнях на частотах в единицы герц инфразвук приводит к головокружению, тошноте, потере сознания, а иногда к слепоте и даже смерти.

Также инфразвуковое оружие может вызывать у людей паническое состояние, потерю контроля над собой и непреодолимое желание укрыться от источника поражения. Определённые частоты могут воздействовать на среднее ухо, вызывая вибрации, которые становятся причиной ощущениям укачивания и морской болезни. Дальность его действия определяется излучаемой мощностью, значением несущей частоты, шириной диаграммы направленности и условиями распространения акустических колебаний в реальной среде [1-12].

Проводя исследования, французский ученый Гавро обнаружил, что инфразвук определенных частот может вызвать у человека тревожность и беспокойство. Инфразвук с частотой 7 Гц смертелен для человека. Действие инфразвука может вызвать головные боли, снижение работоспособности и внимания, а так же нарушение функции вестибулярного аппарата. Это связано с тем, что ритмы характерные для большинства систем организма человека лежат в инфразвуковом диапазоне (см. таблицу №2)

Таблица 2 - Резонансные частоты некоторых частей тела человека

Орган	Ритмы органов (Гц)
Сокращения сердца	1-2
Желудок	2–3
Вестибулярный аппарат	0.5–13
Кишечник	2–4
Голова	20–30
Глаза	19
Брюшная полость	4–8
Почки	6–8
Руки	2–5
Позвоночник	6

При совпадении частот внутренних органов и инфразвука, соответствующие органы начинают вибрировать, что может сопровождаться сильнейшими болевыми ощущениями, а в дальнейшем их повреждение.

Рисунок 3 - Способы защиты персонала от инфразвука

Довольно эффективно, в смысле влияния на человека, задействование механического резонанса упругих колебаний с частотами ниже 16 Гц, так как оно обычно не воспринимаемыми на слух, что означает, что его не так-то просто обнаружить. Самым опасным считается промежуток от 6 до 9 Гц. Значительные психотронные эффекты сильнее всего выказываются на частоте 7 Гц, созвучной альфаритму природных колебаний мозга, причем любая умственная работа в этом случае делается невозможной, поскольку кажется, что голова вот - вот разорвется на мелкие кусочки [1-12].

Звук небольшой интенсивности вызывает тошноту и звон в ушах, а также ухудшение зрения и безотчетный страх. Звук средней мощности расстраивает органы пищеварения и мозг, создавая паралич, общую слабость, а иногда слепоту. Упругий мощный инфразвук способен повредить, и даже полностью остановить сердце. Обычно неприятные ощущения начинаются со 120 дБ напряженности, травмирующие - со 130 дБ. Инфрачастоты около 12 Гц при силе в 85-110 дБ, наводят приступы морской болезни и головокружение, а колебания частотой 15-18 Гц при той же интенсивности внушают чувства беспокойства, неуверенности и, наконец, панического страха.

Можно с уверенностью сказать, что способов борьбы с инфразвуком не так уж и много, так как инфразвук имеет ряд особенностей представленных ранее. Исходя из данных свойств, все-таки можно выделить некоторые способы защиты человека от инфразвука, представленные в рисунке №3.

В работе представлен обзор результатов исследований восприятия человеком инфразвуковых колебаний. Как выяснилось, человеческий организм и человеческая психика крайне подвержены воздействию неслышимых для уха частот, и инфразвуковые волны оказывают заметное влияние на восприятие человеческим мозгом окружающей действительности.

Учитывая выше сказанное можно выделить основные способы защиты от инфразвукового воздействия:

1. Использование глушителей.
2. Предоставление 20 минутных перерывов каждые 2 часа.

И так как защититься от инфразвука на уровне изоляционных материалов довольно сложно, так как он имеет высокую проникающую способность, позволю себе предположить, что данное

направление является наиболее перспективным в области защиты человеческого организма и психики от внешнего воздействия.

Литература

1. Гигиена труда : учебник Под ред. Н. Ф. Измерова, В. Ф. Кириллова. — М. : ГЭОТАР-Медиа, 2010. — 592 с.
2. Жуков А. И., Иванников А. Н., Фрайман Б. Я. О необходимости изучения пространственной структуры звукового поля при оценке действия низкочастотного шума. «Борьба с шумом и звуковой вибрацией», М., 1989 г., стр 53-59.
3. Жуков А. И., Иванников А.Н, Ларюков А. С., Нюнин Б. Н.,Павлов В. И., Фрайман Б. Я. Определение аномально активной зоны вредного действия инфразвуковых шумов в жилых и административных помещениях. «Проблемы акустической экологии», Ленинград, Стройиздат, 1990 г. стр. 13-21.
4. Краткие тезисы докладов всероссийской конференции «Шум и шумовая болезнь»: Вопросы профилактики. – Л.: изд-во ЛСГМИ, 1973.
5. Соляной В.Н., Сухотерин А.И Выработка коммуникативной компетенции при подготовке профессионалов по информационной безопасности с использованием технологии модерации. «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7
6. Соляной В.Н., Сухотерин А.И, Антоненко В.И. Проблемно-ориентированная подготовка специалистов по информационной безопасности с использованием имитационного метода (мозговой штурм). «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. – М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7.
7. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский

Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
8. Соляной В.Н., Сухотерин А.И. Модульно-ориентированный подход формирования базовых дисциплин ФГОС ВО 3+ как основа реализации профессиональной подготовки бакалавров в области информационной безопасности Научно-практический журнал №25, том 2 2015г. Информационное противодействие угрозам терроризма Материалы XIX Пленума учебно-методического объединения по образованию в области информационной безопасности «учебно-методическое обеспечение образовательных программ в области информационной безопасности» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН. ФЕД.УНИВ, 2015.-332 с. ISSN 2219-8792
9. Соляной В.Н., Сухотерин А.И. Практика применения инновационного научно-образовательного комплекса по подготовке бакалавров и магистров в области информационной безопасности. Научно-практический журнал №25, том 1 2015г. Информационное противодействие угрозам терроризма. Материалы XIX Пленума учебно-методического объединения по образованию в области информационной безопасности «опыт и передовые практики образовательных организаций по формированию и использованию в учебном процессе специализированной учебно- лабораторной базы» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН.ФЕД.УНИВ, 2015.-416 с. ISSN 2219-8792
10. Соляной В.Н., Сухотерин А.И. Становление направления «Радиоэлектронная безопасность информационных объектов» в системе дополнительного профессионального по информационной безопасности. Научно-практический журнал №25, том 2 2015г. Информационное противодействие угрозам терроризма Материалы XIX Пленума учебно-методического объединения по образованию в области информационной безопасности «учебно-методическое обеспечение образовательных программ в области информационной безопасности» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН.ФЕД.УНИВ, 2015.-332 с. ISSN 2219-8792
11. Физическая энциклопедия. Гл. ред. А.М. Прохоров, том 2, М.: Советская энциклопедия, 1990.
12. Фрайман Б.Я., Безруков В.Е. Условия, при которых осуществляется прямое действие инфразвука на стенку кровеносного сосуда. Воронеж: 1983 г. стр. 1-13. Рукопись депонирована во ВНИИМИ 16.09.83. №Д-6783.

КОМПЛЕКСНЫЙ МОНИТОРИНГ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ В СИСТЕМЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Кочергин Алексей Сергеевич, Руденко Ростислав Александрович, студенты 4 курса кафедры Информационной безопасности,
Козлова Татьяна Сергеевна, магистрант 1 курса кафедры Информационной безопасности
Научный руководитель: **Соляной Владимир Николаевич**, к.воен.н., доцент, заведующий кафедрой Информационной безопасности

На сегодняшний день по статистике 80% взломов производится изнутри, то есть сотрудниками самой организации. Исходя из таких данных, актуальным является проводить мониторинг действий пользователей. В работе затрагивается проблема автоматизации мониторинга действий пользователей на крупных предприятиях. На основе рассмотренных систем, предлагается система комплексного мониторинга действий пользователей в системе информационной безопасности типового предприятия.

Мониторинг информационных систем, система разграничения доступа, система обнаружения вторжений, система управления событиями информационной безопасности.

INTEGRATED MONITORING USER ACTIONS IN THE SYSTEM OF INFORMATION SECURITY

Kochergin Aleksey, Rostislav Rudenko, 4th year students of the Department of information security,
Kozlova Tatiana, 1 undergraduate course of the Department of information security
Scientific adviser: **Solaynoy Vladimir**, Candidate of Military Sciences, Associate Professor, Head of the Department of information security

Today, according to statistics 80% of burglaries carried out from within, that is, employees of the organization. Based on such data it is urgent to monitor user activity. The article addresses the issue of automation of monitoring user activity in large enterprises. On the basis of considered systems, proposes a system of complex monitoring user activity in the system of information security of the typical enterprise.

Monitoring information systems, Identify and Access Management system, User Administration and Provisioning, Identity and Access governance, Intrusion Detection Systems, Security information and event management-system.

В настоящее время задачи по мониторингу событий информационной безопасности и оперативному реагированию на инциденты выходят на первый план. По мере развития современных информационных систем IT-инфраструктуры любой компании становится все более сложной, разнообразной и приобретает распределенный характер. Невозможно предоставить себе современную компанию, весь бизнес которой сосредоточен в одном месте и не требует автоматизации. Наиболее характерной картиной на сегодняшний день является наличие сотен пользователей, десятков серверов приложений, сетевого оборудования, средств и систем безопасности, и как следствие – миллионов событий от них. В связи с этим задача сбора, обработки и хранения событий информационной безопасности становится все более актуальной [1-14]. Для ее решения необходима эффективная система комплексного мониторинга действий пользователей в системе информационной безопасности. В работе предложен один из вариантов реализации такой системы.

Под **Identify and Access Management (IAM)** понимают набор технологий и программных продуктов, отвечающих задачам управления жизненным циклом учетных записей и управления доступом к различным системам в компании (рис. 1).

Рисунок 1 - Функциональный цикл IAM-систем

Аналитические агентства (Gartner, Forrester, Kuppinger Cole) и разработчики IAM-систем выделяют как минимум две области внутри IAM: **User Administration and Provisioning (UAP)** и **Identity**

and Access governance (IAG). Современное IAM-решение должно предоставлять функциональность в обеих областях [14].

User Administration and Provisioning решает задачи автоматизации создания, изменения и удаления учетных записей в информационных системах организации, а также обеспечивает доступ к приложениям и ресурсам, которые нужны пользователю для работы.

Целесообразно рассмотреть процесс организации доступа к IT-ресурсам (приложения, данные, сервисы) в компании без автоматизации. Сотрудника при приеме на работу отдел кадров вносит в 1С. Затем информация о нем попадает в ИТ-отдел. IT-отдел создает учетную запись в службе каталогов Active Directory. Доступ к папкам, приложениям, рассылкам новый работник получает, обратившись к системному администратору или в службу поддержки по электронной почте, в некоторых случаях требуется согласие руководителя или владельца ресурса. При этом сотрудник никогда не просит «отобрать доступ» и за годы работы в компании может «обрасти» доступом в различные системы [5].

После появления учетной записи в кадровой системе UAP-решение автоматически создает учетные записи в подключенных системах, выдает доступ на основе атрибутов пользователя (например, должность и отдел) и групп. UAP-система позволяет проверять значения атрибутов на соответствие правилам и запрещать создание «неправильных записей», в частности, с незаполненной должностью. При изменениях достаточно внести их в одном месте – и они автоматически будут отражены во всех подключенных системах.

Допустим, требуется использовать Adobe Photoshop на рабочем компьютере. Сначала пользователь отправляет заявку в службу техподдержки. Ее сотрудники ждут подтверждения руководителя, который добавляется в переписку [14]. В результате пользователь получает установленное приложение, потратив на это пару дней. Бывает, что в согласовании участвует несколько человек (так, чтобы получить новый ноутбук, нужно подтверждение руководителя и директора).

Identity and Access governance-решения предлагают автоматизацию подобных процессов с помощью веб-портала, где можно запросить ресурс, затем запустится «невидимый» процесс, который при необходимости запросит подтверждение руководителя и

после его получения автоматически произведет требуемые изменения [1-17].

IAG-система позволяет руководителю или сотруднику службы безопасности увидеть, к каким системам у пользователя есть доступ, и также управлять этим доступом.

Доступ может предоставляться и на основе «вычисляемых» правил, то есть если сотрудника назначили работать над конкретным проектом и у него появилась соответствующая роль, он автоматически получит доступ к требуемой документации, что позволит избежать «ручных согласований».

Если у пользователя появились лишние права (например, администратор Active Directory добавил пользователя в группу), которые не соответствуют его роли, служба безопасности получит уведомление об этом и может подтвердить исключение или принять меры к его устранению.

Системы обнаружения вторжений (IDS - Intrusion Detection Systems) - один из важнейших элементов систем информационной безопасности сетей любого современного предприятия. Рост в последние годы числа проблем, связанных с компьютерной безопасностью, привёл к тому, что системы обнаружения вторжения очень быстро стали ключевым компонентом любой стратегии сетевой защиты (рис. 2).

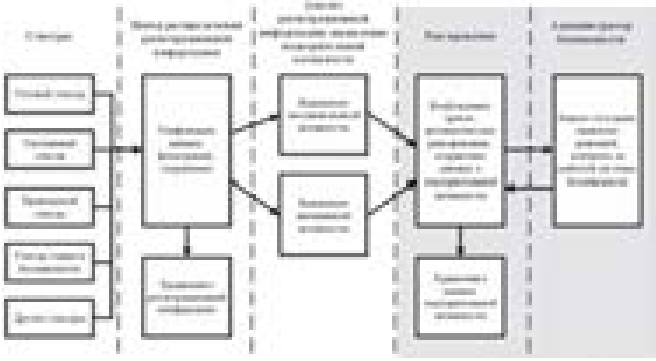


Рисунок 2 - Функциональный цикл IDS-систем

За последние несколько лет их популярность значительно возросла, поскольку продавцы средств защиты значительно улучшили качество и совместимость своих программ [4].

Системами обнаружения вторжений (СОВ) называют множество различных программных и аппаратных средств, объединяемых одним

общим свойством - они занимаются анализом использования вверенных им ресурсов и, в случае обнаружения каких-либо подозрительных или просто нетипичных событий, способны предпринимать некоторые самостоятельные действия по обнаружению, идентификации и устранению их причин.

В заключении хотелось бы ещё раз подчеркнуть, что IDS – это лишь одно из средств хорошей архитектуры обеспечения безопасности сети и многоуровневой стратегии её защиты. Они имеют свои преимущества и недостатки, развить первые и сгладить последние можно, применяя IDS в комплексе с другими средствами обеспечения безопасности информации.

SIEM (Security information and event management) – объединение двух терминов, обозначающих область применения ПО: SIM - Security information management - управление информационной безопасностью и SEM - Security event management - управление событиями безопасности. Технология SIEM обеспечивает анализ в реальном времени событий (тревог) безопасности, исходящих от сетевых устройств и приложений. SIEM представлено приложениями, приборами или услугами, и используется также для журналирования данных и генерации отчетов в целях совместимости (с прочими бизнес-данными) (рис. 3).

SIEM — это Security Information and Event Management. Как видно из названия — она «сама по себе» не способна что-то предотвращать или защищать. Данная система предназначена для анализа информации, поступающей от различных других систем, таких как DLP, IDS, антивирусов, различных железок (Fortinet, маршрутизаторы и т.д.) и дальнейшего выявления отклонения от норм по каким-то критериям. Как только мы выявили отклонение — генерируем инцидент. В основе работы SIEM лежит, как ни странно, почти голая математика и статистика. Каких-либо защитных функций «голая» SIEM в себе не несет.

Функциональность SIEM:

- **Агрегация данных:** управление журналами данных; данные собираются из различных источников сетевые устройства и сервисы, датчики систем безопасности, серверы, базы данных, приложения; обеспечивается консолидация данных с целью критических событий.
- **Корреляция:** поиск общих атрибутов, связывание событий в значимые кластеры. Технология обеспечивает применение

различных технических приемов для интеграции данных из различных источников для превращения исходных данных в значащую информацию. Корреляция является типичной функцией подмножества Security Event Management.

- **Оповещение:** автоматизированный анализ коррелирующих событий и генерация оповещений (тревог) о текущих проблемах. Оповещение может выводиться на «приборную» панель самого приложения, так и быть направлено в прочие сторонние каналы: e-mail, GSM-шлюз итп.
- **Средства отображения** (информационные панели): отображение диаграмм помогающих идентифицировать паттерны отличные от стандартного поведения.
- **Совместимость (трансформируемость)**: применение приложений для автоматизации сбора данных, формированию отчетности для адаптации агрегируемых данных к существующим процессам управления информационной безопасностью и аудита.
- **Хранение данных**: применение долговременного хранилища данных в историческом порядке для корреляции данных по времени и для обеспечения трансформируемости. Долговременное хранение данных критично для проведения компьютерно-технических экспертиз, поскольку расследование сетевого инцидента вряд ли будет проводиться в сам момент нарушения.
- **Экспертный анализ**: возможность поиска по множеству журналов на различных узлах; может выполняться в рамках программно-технической экспертизы.

Рисунок 3 - Комплексный мониторинг действий пользователей в системе информационной безопасности предприятия

Основываясь на совместимости SIEM-систем, предлагается объединенная система (рис. 3), которая будет использовать не только информацию из обычных систем обработки, программного обеспечения или данных сотрудников, но и будет задействованы

функции включенных систем: IAM и IDS, которые позволят нам обеспечивать автоматизацию управленческих задач по мониторингу. Теперь не придется следить за действиями пользователей «вручную», за всем этим будет следить предложенная интегрированная система SIEM, которая помимо слежения может выдавать предупреждающие сообщения как нарушителю (пользователю), так и администратору по безопасности. Все эти действия отображаются и сохраняются в журналах

Выводы:

- Проведенный анализ существующей системы информационной безопасности предприятия выявил существующие недостатки в аудите мероприятий по защите информации: отсутствие комплексного подхода, слабая автоматизация аудита, низкий уровень подготовки внутренних аудиторов;
- В работе предложен комплексный автоматизированный мониторинг действий пользователей, который ориентирован на крупные предприятия с большим ресурсом защищаемой информации и включает в себя следующие функции: агрегация данных, корреляция данных, оповещение сотрудников и администратора безопасности, средства отображения информации, совместимость с существующими процессами управления информационной безопасностью и аудита, хранение данных, экспертный анализ;
- Обеспечение комплексного мониторинга позволит повысить эффективность системы управления информационной безопасности предприятия (является ключевым компонентом подсистемы управления информационной безопасностью), и в перспективе должен охватить так же другие подсистемы ИБ, в частности, подсистемы физической защиты, реализуемых на IP-технологиях.

Литература

1. Белый В.М., Белый Р.В. Теория эффективности информационных систем и информационных технологий: монография. – Королёв МО: ФТА, 2012.
2. Малюк А.А. Информационная безопасность. Концептуальные и методологические основы защиты информации. –М.: Горячая линия-Телеком, 2004.
3. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации //Режим доступа: http://bezopasnik.org

4. Прохоров С.А., Федосеев А.А., Иващенко А.В. "Автоматизация комплексного управления безопасностью предприятия". Самара: СНЦ РАН, 2008 – 55 с.
5. Скиба В.Ю., Курбатов В.А., Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Питер, 2008.
6. Соляной В.Н., Сухотерин А.И Выработка коммуникативной компетенции при подготовке профессионалов по информационной безопасности с использованием технологии модерации. «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7
7. Соляной В.Н., Сухотерин А.И, Антоненко В.И. Проблемно-ориентированная подготовка специалистов по информационной безопасности с использованием имитационного метода (мозговой штурм). «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. – М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7.
8. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
9. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
10. Соляной В.Н., Сухотерин А.И. Модульно-ориентированный подход формирования базовых дисциплин ФГОС ВО 3+ как основа реализации профессиональной подготовки бакалавров в области

информационной безопасности Научно-практический журнал №25, том 2 2015г. Информационное противодействие угрозам терроризма Материалы XIX Пленума учебно-методического объединения по образованию в области информационной безопасности «учебно-методическое обеспечение образовательных программ в области информационной безопасности» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН.ФЕД.УНИВ, 2015.-332 с. ISSN 2219-8792
11. Соляной В.Н., Сухотерин А.И. Становление направления «Радиоэлектронная безопасность информационных объектов» в системе дополнительного профессионального по информационной безопасности. Научно-практический журнал №25, том 2 2015г. Информационное противодействие угрозам терроризма материалы xix пленума учебно-методического объединения по образованию в области информационной безопасности «учебно-методическое обеспечение образовательных программ в области информационной безопасности» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН. ФЕД.УНИВ, 2015.-332 с. ISSN 2219-8792
12. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Некоторые перспективы применения систем контроля и управления доступом в региональных ВУЗАХ. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» При поддержке Посольства Туркменистана в Российской Федерации. Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
13. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Развитие сотрудничества российских и зарубежных ВУЗОВ по защите информационного ресурса. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» При поддержке Посольства Туркменистана в Российской Федерации. Текст Сборник материалов III Ежегодной международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
14. Ярочкин В.И., Система безопасности фирмы — 3-е изд., перераб. и доп. — М.:Ось-89, 2003.

ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В РАСПРЕДЕЛЁННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Краснов Денис Валерьевич, студент 1 курса кафедры Информационной безопасности
Научный руководитель: **Соляной Владимир Николаевич,** к.воен.н., доцент, заведующий кафедрой Информационной безопасности

Концентрация информации в компьютерах — аналогично концентрации наличных денег в банках — заставляет все более усиливать контроль в целях защиты информации. Юридические вопросы, частная тайна, национальная безопасность — все эти соображения требуют усиления внутреннего контроля в коммерческих и правительственных организациях. Работы в этом направлении привели к появлению новой дисциплины: безопасность информации.

Сложность создания системы защиты информации определяется тем, что данные могут быть похищены из компьютера и одновременно оставаться на месте; ценность некоторых данных заключается в обладании ими, а не в уничтожении или изменении.

Распределённые информационные системы, проблемы защиты информационной безопасности, оценки уровня защиты информационной безопасности.

PROBLEMS OF INFORMATION PROTECTION IN DISTRIBUTED INFORMATION SYSTEMS

Krasnov Denis, 1st year student of the Department of information security
Scientific adviser: **Solyanoy Vladimir,** Candidate of Military Science, Associate Professor, Head of the Department of information security

The concentration of information in computers — the same concentrations of cash in banks — is forcing more and more strengthen controls to protect information. Legal issues, personal privacy, national security — all of these considerations require strengthening of internal control in commercial and government organizations. Work in this direction has led to the emergence of a new discipline: information security.

The complexity of creating systems of information protection defined by the fact that data can be stolen from your computer and stay in place; some data value is in possession, and not to destroy or change.

Distributed information systems, the problems of protection of information security, assess the level of protection of information security.

Распределенная система – это набор независимых компьютеров, представляющийся их пользователям как единая система.

Распределенная информационная система (РИС) – это совокупность взаимодействующих друг с другом программных компонент. Каждая из таких компонент может рассматриваться как программный модуль (приложение), исполняемый в рамках отдельного процесса.

Проблема защиты компьютерных сетей от несанкционированного доступа приобрела особую остроту. Развитие коммуникационных технологий позволяет строить сети распределенной архитектуры, объединяющие большое количество сегментов, расположенных на значительном удалении друг от друга. Все это вызывает увеличение числа узлов сетей, разбросанных по всему миру, и количества различных линий связи между ними, что, в свою очередь, повышает риск несанкционированного подключения к сети для доступа к важной информации. Особенно неприятной такая перспектива может оказаться для банковских или государственных структур, обладающих секретной информацией коммерческого или любого другого характера. В этом случае необходимы специальные средства идентификации пользователей в сети, обеспечивающие доступ к информации лишь в случае полной уверенности в наличии у пользователя прав доступа к ней [1-15].

Разработано несколько методов, которые несут в себе новизну:

1) Разработан метод анализа моделей противодействия угрозам нарушения информационной безопасности, базирующийся на выборе рационального варианта реагирования, *новизна* которого заключается в принятии решения на множестве альтернатив средств и методов защиты в зависимости от определения уровня эффективности, удовлетворяющего оптимальным показателям риска возникновения угроз и затрат, необходимых на их нейтрализацию. Метод позволяет заменить традиционно применяемые оценки взломостойкости их вероятностными аналогами и оценками эффективности, а также осуществлять динамическую оптимизацию механизмов защиты.

2) Разработан метод и алгоритм оценки уровня эффективности системы защиты информации, новизна которого заключается в том, что необходимые для расчетов вероятности угрозы оцениваются на основе численных методов представления аналитического прогнозирования событий, технических характеристик средств защиты и статистических данных по инцидентам информационной безопасности, что позволяет обеспечить применимость метода и алгоритма не только на стадии создания средств защиты информации, но и выполнять анализ эффективности её функционирования в ходе эксплуатации и экспертизы инцидентов.

Существует ряд разработок, позволяющих с высокой степенью надежности идентифицировать пользователя при входе в систему. Среди них, например, есть технологии, идентифицирующие пользователя по сетчатке глаза или отпечаткам пальцев. Кроме того, ряд систем используют технологии, основанные на применении специального идентификационного кода, постоянно передаваемого по сети. Так, при использовании устройства SecureID обеспечивается дополнительная информация о пользователе в виде шестизначного кода. В данном случае работа в сети невозможна без наличия специальной карты SecureID (похожей на кредитную), которая обеспечивает синхронизацию изменяющегося кода пользователя с хранящимися на UNIX-хосте, При этом доступ в сеть и работа в ней может осуществляться лишь при знании текущего значения кода, который отображается на дисплее устройства SecureID. Однако основным недостатком этой и ей подобных систем является необходимость в специальном оборудовании, что вызывает неудобства в работе и дополнительные затраты.

В работе рассматриваются некоторые возможности обеспечения безопасности в системах — шифрование информации при передаче по каналам связи и использование надежных (достоверных, доверительных) (Trusted) систем — на примере СУБД ORACLE, а так же система защиты от несанкционированого доступа к сети Kerberos.

Очевидные достоинства баз данных в современной среде обработки данных служат гарантией их дальнейшего развития и использования. Контроль доступа в этой области важен ввиду колоссальной концентрации информации.

В настоящий момент «хребтом» базовых систем обработки информации во многих больших организациях является локальная сеть, которая постепенно занимает такое же место и в фирмах

меньшего размера. Растущая популярность локальных сетей требует соответствующей защиты информации, но исторически они были спроектированы как раз не для разграничения, а для облегчения доступа и коллективного использования ресурсов. В среде локальных сетей в пределах здания или района (городка) сотрудник, имеющий доступ к физической линии, может просматривать данные, не предназначенные для него. В целях защиты информации в различных комбинациях используются контроль доступа, авторизация и шифрование информации, дополненные резервированием.

Обеспечение безопасности информации — дорогое дело, и не столько из-за затрат на закупку или установку средств, сколько из-за того, что трудно квалифицированно определить границы разумной безопасности и соответствующего поддержания системы в работоспособном состоянии.

Если локальная сеть разрабатывались в целях совместного использования лицензионных программных средсов, дорогих цветных принтеров или больших файлов общедоступной информации, то нет никакой потребности даже в минимальных системах шифрования/дешифрования информации.

Средства защиты информации нельзя проектировать, покупать или устанавливать до тех пор, пока не произведен соответствующий анализ.

Анализ риска должен дать объективную оценку многих факторов (подверженность появлению нарушения работы, вероятность появления нарушения работы, ущерб от коммерческих потерь, снижение коэффициента готовности системы, общественные отношения, юридические проблемы) и предоставить информацию для определения подходящих типов и уровней безопасности. Коммерческие организации все в большей степени переносят критическую корпоративную информацию с больших вычислительных систем в среду открытых систем и встречаются с новыми и сложными проблемами при реализации и эксплуатации системы безопасности. Сегодня все больше организаций разворачивают мощные распределенные базы данных и приложения клиент/сервер для управления коммерческими данными. При увеличении распределения возрастает также и риск неавторизованного доступа к данным, и их искажения [1-15].

Шифрование данных традиционно использовалось правительственными и оборонными департаментами, но в связи с

изменением потребностей и некоторые наиболее солидные компании начинают использовать возможности, предоставляемые шифрованием для обеспечения конфиденциальности информации.

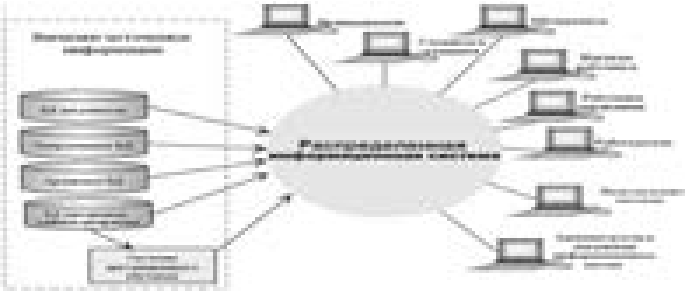


Рисунок 1 – Распределённая информационная система баз данных

Шифрование данных может осуществляться в режимах On-Line (в темпе поступления информации) и Off-Line (автономном). Остановимся подробнее на первом типе, представляющем больший интерес. Наиболее распространены два алгоритма.

Стандарт шифрования данных DES (DataEncryptionStandard) был разработан фирмой IBM в начале 70-х годов и в настоящее время является правительственным стандартом для шифрования цифровой информации. Он рекомендован Ассоциацией Американских Банкиров. Сложный алгоритм DES использует ключ длиной 56 бит и 8 битов проверки на четность и требует от злоумышленника перебора 72 квадриллионов возможных ключевых комбинаций, обеспечивая высокую степень защиты при небольших расходах. При частой смене ключей алгоритм удовлетворительно решает проблему превращения конфиденциальной информации в недоступную.

Алгоритм RSA был изобретен Ривестом, Шамиром и Альдеманом в 1976 году и представляет собой значительный шаг в криптографии. Этот алгоритм также был принят в качестве стандарта Национальным Бюро Стандартов.

DES, технически, является симметричным алгоритмом, а RSA — асимметричным, то есть он использует разные ключи при шифровании и дешифровании. Пользователи имеют два ключа и могут широко распространять свой открытый ключ. Открытый ключ используется для шифрования сообщения пользователем, но только определенный получатель может дешифровать его своим секретным ключом; открытый ключ бесполезен для дешифрования. Это делает

ненужными секретные соглашения о передаче ключей между корреспондентами. DES определяет длину данных и ключа в битах, а RSA может быть реализован при любой длине ключа. Чем длиннее ключ, тем выше уровень безопасности (но становится длительнее и процесс шифрования и дешифрования). Если ключи DES можно сгенерировать за микросекунды, то примерное время генерации ключа RSA — десятки секунд. Поэтому открытые ключи RSA предпочитают разработчики программных средств, а секретные ключи DES — разработчики аппаратуры.

Примером архитектуры клиент/сервер, которую хорошо дополняют средства шифрования, могут служить OracleServer, сетевые продукты (SQMNet) и программное обеспечение клиента.

Сетевая служба безопасности (SNS — SecureNetworkServices) предлагает стандартный, оптимизированный алгоритм шифрования DES с ключом длиной 56 бит для организаций, от которых требуется использовать стандарт DES. Для заказчиков вне пределов США или Канады SNS предлагает DES40, в котором комбинируется использование алгоритма шифрования DES с общепринятым ключом длиной 40 бит (экспорт технологий шифрования в США законодательно ограничен). Наряду с DES возможно также использование алгоритма шифрования RSA RC4.Секретный, генерируемый случайным образом ключ для каждой сессии SQL-Net сохраняет весь сетевой трафик — включая пароли, значения данных, SQL-утверждения и сохраняемые вызовы и результаты.

Для обнаружения модификации или подмены данных во время передачи SNS генерирует криптографически защищенное значение, вычисляемое по содержимому сообщения, и включает его в каждый пакет, передаваемый по сети. При получении пакета в пункте назначения SNS немедленно производит проверку целостности каждого пакета.

Устойчивость к искажению данных обеспечивается следующим образом:

1) криптографически защищенная контрольная сумма в каждом пакете SQL*Net обеспечивает защиту от модификации данных и замены операции;

2) при обнаружении нарушений операции незамедлительно автоматически завершаются;

3) информация о всех нарушениях регистрируется в журнале.

Наряду с этим обеспечивается многопротокольная перекодировка данных, т.е. полностью поддерживается OracleMultiprotocolInterchange — при работе с зашифрованной сессией можно начинать работу с одним сетевым протоколом, а заканчивать с другим, при этом не требуется дешифрование или перешифрование информации. SNS полностью поддерживается сквозными шлюзами, Oracle Transparent Gateways, и процедурными шлюзами, Oracle Procedural Gateways, которые дают возможность организовывать полностью зашифрованные сессии клиент/сервер к отличным от Oracle источникам данных, включая Adabas,CADatacom, DB2, DRDA, FOCUS, IDMS, IMS, ISAM, MUMPS, QSAM,Rdb, RMS, SAP,SQL/DS, SQL/400, SUPRA, Teradata, TOTAL, VSAM и другие.SNS работает со всеми основными протоколами, поддерживаемыми SQL* Net, включая AppleTalk, Banyan, DECnet, LU6.2, MaxSix,NetBIOS,SPX/IPX,TCP/IP,X.25 и другие.

Обеспечивается независимость от топологии сети — SNS работает во всех основных сетевых средах, поддерживаемых SQL-Net.

SNS представляет собой дополнительный продукт к стандартному пакету SQL* Net, то есть требуется предварительно приобрести лицензию на SQL* Net. Продукт надо покупать и для клиента, и для сервера.

Это означает, что при организации связи клиент/сервер используется новый протокол установления связи, в котором применяется сеансовый ключ, пригодный только для единственной попытки соединения с базой данных и используемый в качестве ключа для шифрования пароля, прежде чем он будет передан клиентам. Oracle-сервер находит зашифрованный пароль для этого пользователя и использует его в качестве ключа, которым он зашифровывает сеансовый ключ. Затем сервер пересылает этот зашифрованный сеансовый ключ клиенту. Клиент шифрует (применяя тот же самый односторонний алгоритм, который используется сервером) пароль, введенный пользователем, и с его помощью дешифрует зашифрованный сеансовый ключ. Обнаружив этот сеансовый ключ, он использует его — это становится совместным секретом клиента и сервера — для шифрования пароля пользователя. Этот зашифрованный пароль затем передается через сеть серверу. Сервер дешифрует пароль и затем зашифровывает его, используя односторонний алгоритм сервера; результат этих

вычислений сверяется со значением, хранимым в словаре данных. Если они совпадают, клиенту предоставляется доступ. Такой подход реализуется как в соединениях типа клиент/сервер, так и сервер/сервер, где сеансы устанавливаются через так называемые полномочные звенья баз данных (т.е. звенья баз данных без вложенных имен пользователей и паролей).

Ни одна компьютерная система защиты информации не является абсолютно безопасной. Однако адекватные меры защиты значительно затрудняют доступ к системе и снижают эффективность усилий злоумышленника (отношение средних затрат на взлом защиты системы и ожидаемых результатов) так, что проникновение в систему становится нецелесообразным. Ключевым элементом в системе безопасности является администратор системы. Какие бы средства вы ни приобретали, качество защиты будет зависеть от способностей и усилий этого человека.

Литература

1. Дьяченко В.И. Теория систем безопасности данных.-М.: ООО "Исток", 1995.
2. Журнал "Открытые системы" за 1997-1998 годы.
3. Журналы (№3-10) "Сети" за 1998 год.
4. Соляной В.Н., Сухотерин А.И Выработка коммуникативной компетенции при подготовке профессионалов по информационной безопасности с использованием технологии модерации. «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7
5. Соляной В.Н., Сухотерин А.И, Антоненко В.И. Проблемно-ориентированная подготовка специалистов по информационной безопасности с использованием имитационного метода (мозговой штурм). «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7.
6. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры

информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
7. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
8. Соляной В.Н., Сухотерин А.И. Модульно-ориентированный подход формирования базовых дисциплин ФГОС ВО 3+ как основа реализации профессиональной подготовки бакалавров в области информационной безопасности Научно-практический журнал №25, том 2 2015г. Информационное противодействие угрозам терроризма Материалы XIX Пленума учебно-методического объединения по образованию в области информационной безопасности «учебно-методическое обеспечение образовательных программ в области информационной безопасности» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН.ФЕД.УНИВ, 2015.-332 с. ISSN 2219-8792
9. Соляной В.Н., Сухотерин А.И. Практика применения инновационного научно-образовательного комплекса по подготовке бакалавров и магистров в области информационной безопасности. Научно-практический журнал №25, том 1 2015г. Информационное противодействие угрозам терроризма. Материалы XIX пленума учебно-методического объединения по образованию в области информационной безопасности «опыт и передовые практики образовательных организаций по формированию и использованию в учебном процессе специализированной учебно-лабораторной БАЗЫ» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН.ФЕД.УНИВ, 2015.-416 с. ISSN 2219-8792
10. Соляной В.Н., Сухотерин А.И. Становление направления «Радиоэлектронная безопасность информационных объектов» в системе дополнительного профессионального по информационной безопасности. Научно-практический журнал №25, том 2 2015г. Информационное противодействие угрозам терроризма Материалы XIX Пленума учебно-методического объединения по образованию в

области информационной безопасности «учебно-методическое обеспечение образовательных программ в области информационной безопасности» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН.ФЕД.УНИВ, 2015.-332 с. ISSN 2219-8792
11. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Некоторые перспективы применения систем контроля и управления доступом в региональных ВУЗАХ. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
12. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Развитие сотрудничества российских и зарубежных ВУЗОВ по защите информационного ресурса. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.

РАЗВИТИЕ СОВРЕМЕННОЙ ЭЛЕКТРОНИКИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кручинина Светлана Александровна, студентка 3 курса кафедры Информационной безопасности
Научный руководитель: **Сухотерин Александр Иванович,** к.воен.н., доцент кафедры Информационной безопасности

Развитие электроники является одним из ключевых факторов развития, как мировой, так и российской экономики. От уровня ее развития во многом зависят образ и качество жизни людей. В связи с этим вопрос о том, каковы же тенденции развития современной электроники является актуальным. Проанализированы основные статистические показатели и выявлены тенденции развития электроники, как в России, так и в мире в целом.

Современная электроника, тенденции развития, российская электроника, мировая электроника.

DEVELOPMENT OF MODERN ELECTRONICS IN THE FIELD OF INFORMATION SECURITY

Kruchinina Svetlana, 3d year student of the Department of information security
Scientific adviser: **Sukhoterin Alexander,** Candidate of Military Sciences, Associate Professor of the Department of information security

The development of electronics is one of the key factors of development, both global and Russian economy. From the level of its development depends largely on the image and quality of life. In this regard, the question of what are the trends in the development of modern electronics is relevant. During the analyzed basic statistics and identified development trends of electronics, both in Russia and in the world as a whole.

Modern electronics, development trends, Russian electronics, world electronics.

Обширное использование электроники во всех областях деятельности оказывает колоссальное влияние на формирование экономики и образ жизни людей, как в отдельной стране, так и в мире в целом. За счет электроники перед нами открывается множество возможностей для коммуникации друг с другом, она способствует повышению качества и доступности образования, здравоохранения. Ее развитие во многом определяет достигаемый уровень защищенности информационных объектов от различных угроз.

Развитие электронной промышленности для России особенно важно в связи с такими позициями, как [1]:

- российский рынок электроники – один из наиболее емких и бурно развивающихся рынков;
- индустрия электроники обладает большими перспективами для последующего развития;
- уровень развития электронной отрасли оказывает существенное влияние на развитие информационного общества в целом;
- ключевой элемент стоимости в электронике – интеллект и высококвалифицированный труд, следовательно, развитие электронной отрасли напрямую связано с переходом к инновационной экономике.

Таким образом, развитие электронной отрасли является одним из важнейших направлений обеспечения информационной и экономической безопасности государства, является актуальной проблемой современности.

Говоря о международной электронной промышленности, важно отметить, что ее объем составляет около 2 трлн. долларов США – это один из крупнейших в мире рынков [1]. Пик развития мировой электроники наблюдался в 60 – 80 годах, затем электронная промышленность вступила в этап зрелости, на что указывает снижение средних темпов роста (рисунок 1).

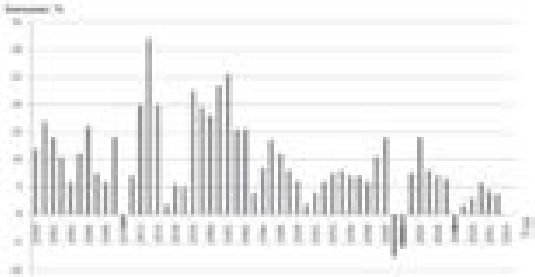


Рисунок 1 – Рост мировой электронной промышленности

Невзирая на это электроника продолжает оставаться одной из наиболее активно развивающихся сфер в международной экономике.

Одним из наиболее перспективных направлений развития электроники с точки зрения информационной безопасности является радиоэлектронная безопасность информационных объектов.

Существуют различные способы воздействия угроз на объекты информационной безопасности (далее – ИБ). Они подразделяются на информационные, программно-математические, физические, радиоэлектронные и организационно-правовые. Однако наиболее опасным является радиоэлектронное воздействие посредством радиоэлектронной разведки (рисунок 2).

Незащищенные средства передачи, приема и обработки информации, работающие от электрического тока, образуют радиоэлектронный канал утечки информации. В радиоэлектронном канале передачи носителем информации является электрический ток и электрическое поле с частотами колебаний от звукового диапазона до десятков ГГц.

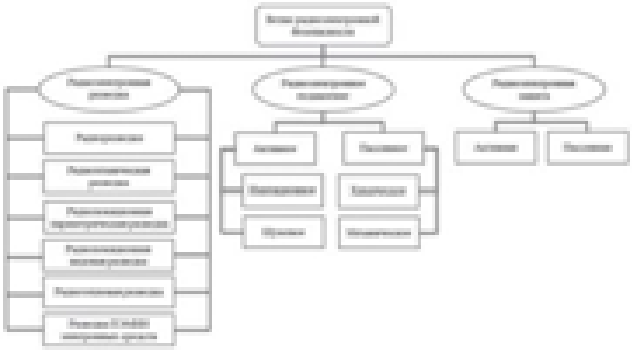


Рисунок 2 – Ветви радиоэлектронной безопасности

Радиоэлектронный канал относится к наиболее информативным каналам утечки в силу следующих его особенностей:

- независимость функционирования канала от времени суток и года, существенно меньшая зависимость его параметров по сравнению с другими каналами от метеоусловий;
- высокая достоверность добывания информации, особенно при перехвате ее в функциональных каналах связи (за исключением случаев дезинформации);
- большой объем добываемой информации;
- оперативность получения информации вплоть до реального масштаба времени;
- скрытность перехвата сигналов и радиотеплового наблюдения.

Таким образом, основной задачей радиоэлектронной разведки является: обеспечение добывания разведывательной информации на основе обнаружения, регистрации (приема) и анализа излучаемых и отраженных от объектов разведки радиосигналов, а также других излучений в радиодиапазоне электромагнитных волн, сопутствующих функционированию различных технических устройств.

В целом, можно выделить следующие современные направления развития электроники:

- постепенно осуществляется процесс глобализации;
- усиление специализации фирм и формирование рынка сервисных организаций;
- на развитие отрасли все большее влияние стал оказывать рынок потребительской электроники;

- возникновение новых индустриальных центров в развивающихся странах;
- возрастание влияния общественных потребностей на развитие электронной отрасли;
- цикличный характер развития, скачки в развитии чередуются с периодическими кризисами.

Говоря о возникновении новых индустриальных центров, стоит отметить, что за последние годы Китай и Индия стали ключевыми двигателями мирового экономического роста (рисунок 3).

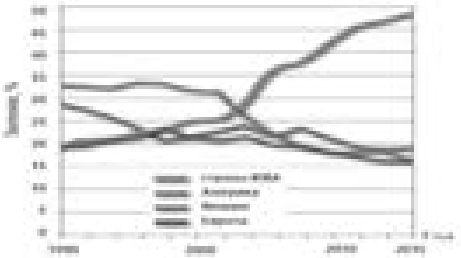


Рисунок 3 – Объемы производства электроники по регионам

Также необходимо выделить, что данные центры обладают следующими характеристиками: высокая численность населения; низкая стоимость труда; благоприятный инвестиционный климат; растущий уровень образования.

Говоря об электронной промышленности России, стоит выделить следующие характерные для нее особенности:

- преобладание государственного сектора над частным, в связи с чем, возникают «тепличные условия» для предприятий (ограниченная конкуренция, минимальное влияние внешних факторов);
- сосредоточение производства на внутреннем рынке;
- низкий уровень интеграции российской электроники с международной ареной.

С точки зрения ИБ развитие отечественной радиоэлектронной промышленности имеет особое значение, так как она (ИБ) связана с использованием различных элементов данной отрасли, необходимых для обеспечения безопасности.

Однако существуют некоторые особенности, которые осложняют процесс развития российского рынка электроники.

С одной стороны, он довольно маленький. С другой, он разделяется на две почти не зависящие друг от друга составляющие:

«внутреннюю», связанную с государственным и оборонным заказом, при этом компании данного сектора почти не выходят на открытый рынок; и «внешнюю», где фирмы работают на открытом рынке в условиях высокой конкуренции, вне сферы государственных закупок (рисунок 4).

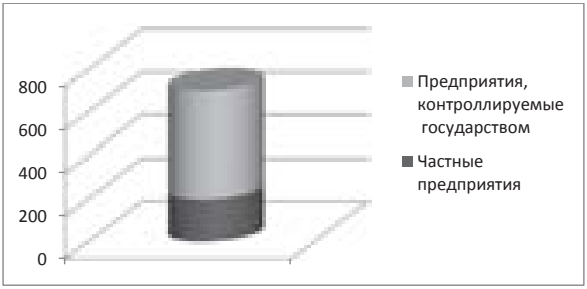


Рисунок 4 – Соотношение между государственным и частным секторами электронной отрасли России

Главная задача государства состоит в том, чтобы стимулировать предприятия, работающие с гос- и оборонзаказами выходить за их пределы на открытый рынок, увеличивать обороты и способствовать его развитию, ведь такие предприятия в нашей стране составляют лидирующее большинство [4] (рисунок 5). При отсутствии их участия маловероятно, что рынок сможет выйти на приемлемые темпы развития.

Рисунок 5 – Производство электроники в России по отраслям

Одним из наиболее перспективных предприятий является созданный в 2009 году Концерн «Радиоэлектронные технологии» (КРЭТ), который объединяет около полусотни предприятий радиоэлектронной отрасли страны [2]. Его деятельность сконцентрирована в области обеспечения госзаказа радиоэлектронными средствами; повышения операционной эффективности холдинга, выхода на новые рынки. Доля продукции

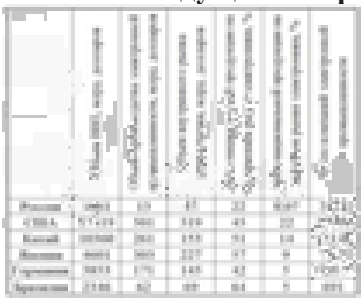
Концерна на российском рынке РЭБ составляет около 94%, на мировом РЭБ – 3% [3].

К сожалению, подобного концерна, специализирующегося на разработке радиоэлектроники, обеспечивающей безопасность информационных объектов гражданского назначения, нет.

Таким образом, для успешного развития, как на внутреннем рынке, так и на мировой арене, необходимо активное взаимодействие, как государства, так и всех участников, занимающихся производственной деятельностью в данном секторе.

В целях сопоставления уровня развития электронной отрасли России по сравнению с ведущими странами мира, далее представлена таблица, где по вертикали представлены страны мира, а по горизонтали основные показатели их деятельности в электронной отрасли [5] (таблица 1).

Таблица 1 – Сравнительная характеристика электронной промышленности России с ведущими мировыми странами



Анализ представленных статистических данных, позволяет сделать вывод, что Российская электронная промышленность существенно отстает от ведущих мировых держав.

Однако стоит отметить, что Россия обладает достаточным потенциалом и, несмотря на столь значительное отставание, она смогла бы войти в число ведущих стран мира.

Для реализации этих целей требуются поэтапные преобразования, источником которых станет государство, а результатом будет повышение конкурентоспособности и инвестиционной привлекательности российской электронной отрасли. От того, насколько государству удастся реализовать задуманное, будет зависеть его информационная и экономическая безопасность, обеспеченность отечественной элементной базой

средств обработки и защиты информации, радиоэлектронной безопасности.

В целях сокращения отставания была разработана и утверждена «Стратегия развития электронной промышленности России на период до 2025 года» (далее – Стратегия).

Направления решения проблемы развития отечественной электронной промышленности могут базироваться в рамках активного сценария на двух стратегических вариантах:

1. государственная монополизация собственности организаций электронной отрасли и централизованное управление отраслью;

2. государственно-частное партнерство в развитии отрасли, расширение всех форм международного кооперационного сотрудничества с учетом ключевых интересов государства.

Выбор того или иного варианта стратегического развития влияет на организационную структуру управления реализацией стратегии и уровень достижения результата.

Наиболее предпочтительным направлением развития российской электроники является второе – государственно-частное партнерство. Однако пока все идет по первому сценарию. Подтверждением этого являются следующие позиции.

В рамках предлагаемой по второму варианту модели развития отрасли государству отводится важнейшая роль решения проблемы безопасности в выстраивании системы государственно-частного партнерства, которую государству не удается реализовать в полной мере. В России сохраняется тенденция к перетеканию заказов на сборку электроники и, соответственно, поставок электронных компонентов в оборонно-промышленный комплекс (рисунок 6).

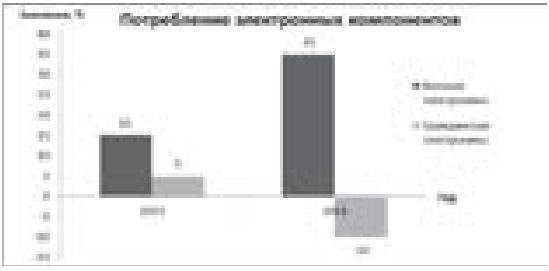


Рисунок 6 – Потребление электронных компонентов

Военная электроника вытесняет с рынка гражданскую (рисунок 7). Если в 2009 г., по данным Центра современной электроники, на

гражданский сектор в России приходилось примерно 80% поставок электронных компонентов, то в 2014 г. – около 55% [8].

Рисунок 7 – Поставка электронных компонентов по секторам

Гражданское производство сокращается. Внутри России основной заказчик гражданской микроэлектроники – государство, инициирующее такие крупные проекты, как универсальная электронная карта, социальные и транспортные карты, биометрические загранпаспорта и другие.

Государство отдает предпочтение технологиям двойного и специального – военного назначения [7] (рисунок 8). Это обуславливает наличие большого числа средств радиоэлектроники военного назначения и крайне малого числа средств радиоэлектроники, обеспечивающей безопасность информационных объектов гражданского назначения.

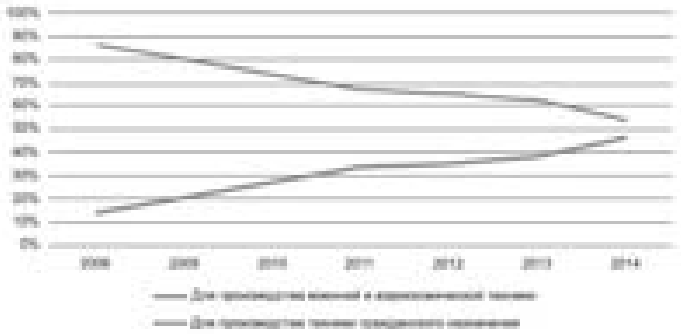


Рисунок 8 – Объемы поставок электронных компонентов для производства оборудования гражданского и специального назначения

Стоит отметить, разработанная Минпромторгом система поддержки электронной промышленности фактически применима

только к предприятиям с госучастием. В результате стимулов для создания массовых продуктов гражданского назначения нет – частные компании утрачивают интерес к бизнесу в сфере электроники.

Однако наблюдаются и положительные тенденции. В течение 2014 года шел активный процесс реструктуризации радиоэлектронной отрасли России. По его итогам был осуществлен ввод в эксплуатацию новых, реконструированных и технически перевооруженных производств.

В 2014 году предприятиям и организациям радиоэлектронной промышленности удалось удержать положительные тенденции в развитии промышленного производства и научно-технической деятельности. Вырос объем производства промышленной продукции, увеличилось производство средств связи и радиоэлектронной промышленности [6] (рисунок 9).

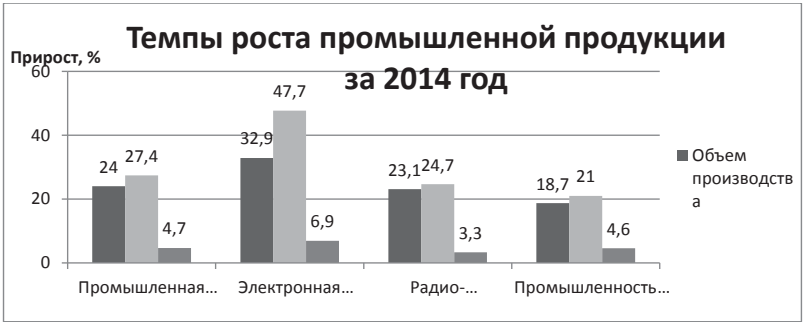


Рисунок 9 – Темпы роста промышленной продукции за 2014 год

Увеличилась производительность труда и среднегодовая численность работников РЭП. Средний возраст работников предприятий и организаций РЭП в 2014 году составил 48 лет. Улучшилось социально-экономическое положение и средняя заработная плата работников.

Таким образом, на фоне положительных изменений, сохраняется главное отрицательное – отсутствие четкой системы государственно-частного партнерства; концентрация электронной отрасли в руках государства, перетекание заказов в военную область и спад гражданской, как следствие, потеря интереса частных компаний к бизнесу в отрасли, что существенным образом отражается и на радиоэлектронной составляющей информационной безопасности [1-9].

Тенденции развития современной электронной промышленности таковы, что: современный рынок электроники является глобальным и высоко конкурентным, что предъявляет весьма серьезные требования и условия к эффективности и качеству производства.

Основываясь на примерах других государств, можно смело говорить о том, что при грамотном проведении необходимых поэтапных преобразований можно добиться значительного скачка в развитии электронной отрасли. Для этого, в свою очередь, необходимо наличие четкой, скоординированной программы действий, позволяющей в результате осуществить переход на качественно новый этап.

Литература

1. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
2. The World Bank (Всемирный Банк), – Каталог данных, – Электронный ресурс. Режим доступа: http://datacatalog.worldbank.org/ (дата обращения 05.12.2015).
3. Валерий Кодачигов, – Милитаризация чипов, – ежедневная деловая газета «Ведомости», №3796, 24.03.2015. Электронный ресурс. Режим доступа:http://www.vedomosti.ru/newspaper/articles (дата обращения 27.12.2015).
4. Концерн «Радиоэлектронные технологии». Официальный сайт. Электронный ресурс. Режим доступа: http://kret.com/news/3235/ (дата обращения 27.12.2015).
5. Корпорация «Ростехнологии». Официальный сайт. Электронный ресурс. Режим доступа: http://rostec.ru/about/holdings/346 (дата обращения 27.12.2015).
6. Министерство промышленности и торговли Российской Федерации. Официальный сайт. Электронный ресурс. Режим доступа: http://minpromtorg.gov.ru/activities/industry/otrasli/radio/#collapseOne (дата обращения 27.12.15).
7. Отраслевой деловой ежегодник – «Живая электроника России – 2015». Электронный ресурс. Режим доступа:

http://www.russianelectronics.ru/skachivanie/72418/1/ (дата обращения 27.12.2015).
8. Статья: Контрактное производство электроники в России в 2015 году. Проблемы, перспективы и импортозамещение. Электронный ресурс. Режим доступа: http://www.ixbt.com/editorial/ruselectr2015-overview.shtml (дата обращения 27.12.2015).
9. Стратегия развития электронной промышленности России на период до 2025 года от 07.08.2007г. Электронный ресурс. Режим доступа: http://www.gosbook.ru/system/files/documents/2011/07/12 (дата обращения 27.12.2015).

ТЕХНОЛОГИЯ ОРГАНИЗАЦИИ ПРОТИВОДЕЙСТВИЯ ОТМЫВАНИЮ ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА

Кручинина Светлана Александровна, студентка 3 курса кафедры Информационной безопасности
Научный руководитель: **Сухотерин Александр Иванович,** к.воен.н., доцент кафедры Информационной безопасности

Организация противодействия отмыванию доходов, полученных преступным путем и финансирование терроризма является важной проблемой современности. На данный момент существует широкая сеть организаций, как в России, так и в мире в целом, специализирующихся на выработке эффективных решений по данному вопросу. Для предотвращения таких преступлений необходимо иметь отлаженную систему отслеживания финансовых операций и четкую организацию взаимодействие между всеми заинтересованными сторонами. Предлагаемый алгоритм действий может существенно повысить раскрываемость подобного рода преступлений.

Система противодействия, отмывание доходов, финансирование терроризма.

TECHNOLOGY OF THE ORGANIZATION OF COUNTERACTION MONEY LAUNDERING OF CRIMINAL PROCEEDS AND FINANCING OF TERRORISM

Kruchinina Svetlana, 3d year student of the Department of information security

Scientific adviser: **Sukhoterin Alexander,** Candidate of Military Sciences, Associate Professor of the Department of information security

The organization of counteraction money laundering of criminal proceeds and financing of terrorism is an important issue of our time. At the moment, there is a wide network of organizations, both in Russia and in the world as a whole, specializing in the development of effective solutions to the issue. To prevent such crimes need to have a well-defined system to track financial transactions and the smooth organization of interaction between all stakeholders. The proposed algorithm of actions can greatly increase the detection rate of the crimes.

Counteraction system, money laundering, financing of terrorism.

Легализация (отмывание) доходов, полученных преступным путем, – придание правомерного вида владению, пользованию или распоряжению денежными средствами или иным имуществом, полученными в результате совершения преступления [1].

Отмывание доходов и финансирование терроризма представляют собой финансовые преступления, которые являются одним из дестабилизирующих факторов как для экономики отдельно взятой страны, так и мировой экономики в целом. В последнее время данная проблема все чаще становится предметом обсуждения на многих международных встречах, связанных с развитием современной экономики.

По оценкам экспертов, сумма ежегодно легализуемых денежных средств составляет от 1000 млрд долл. до 1750 млрд долл. (приблизительно 50% всех криминальных средств) [2].

Отмывание доходов (далее ОД) – деятельность, занимающая по своим размерам третье место в мире (рисунок 1).

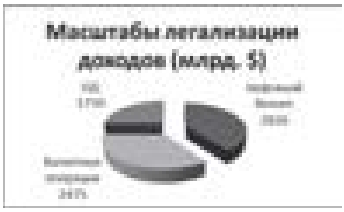


Рисунок 1 – Масштабы легализации доходов

Стоит отметить, что в эффективной системе противодействия отмыванию доходов и финансированию терроризма (далее ПОД/ФТ) заинтересованы прежде всего кредитные организации, так как они занимают центральное место в мировой финансовой системе и являются наиболее универсальной категорией финансовых учреждений, осуществляющей практически все виды финансовой деятельности.

Наглядным подтверждением данного тезиса является статистика Федеральной службы по финансовому мониторингу (Росфинмониторинг, или ФСФМ). Всего в 2014 году было получено более 11 миллионов сообщений о сомнительных операциях на сумму порядка 160 триллионов рублей (на 59% больше предыдущего периода). В том числе: от кредитных организаций – более 11 миллионов; от некредитных организаций – более миллиона (рисунок 2) [1-,9].

Рисунок 2 – Количество сообщений о сомнительных операциях в 2014 году

В связи с этим, создание эффективной системы ПОД/ФТ является актуальной проблемой современности.

Говоря об ОД, стоит отметить, что главная цель такой деятельности – сокрытие, маскировка их незаконного происхождения, что в свою очередь дает владельцу возможность использовать их, не вызывая подозрений у правоохранительных органов.

Процесс ОД – это, как правило, многоэтапный процесс, который независимо от используемой схемы, включает три основных этапа: размещение, рассредоточение и интеграцию (рисунок 3).

Первым этапом является размещение, в течение которого осуществляется видоизменение адреса или начальной формы денег. Стоит отметить, что правоохранительным органам легче всего выявить процесс ОД именно на этом этапе, в связи с чем, основные силы концентрируются именно на нем.

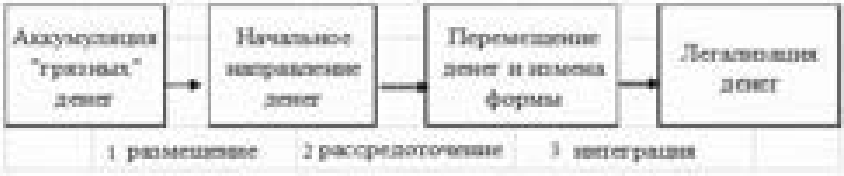


Рисунок 3 – Механизм «отмывания» денежных средств

Второй этап – рассредоточение – сокрытие следов преступления путем проведения множества финансовых операций, происходит отделение нелегальных доходов от их источника [1-9].

Третий (заключительный) этап – интеграция, здесь владелец преступных доходов получает возможность распоряжаться ими вполне легально; доходы, полученные преступным путем, приобретают вполне легальное происхождение.

Таким образом, суть процесса ОД сводится к трем ключевым этапам, которые направлены на придание преступным доходам легальных источников происхождения, с целью дальнейшего распоряжения ими в реальном секторе экономики.

Существует ряд международных организаций, деятельность которых направлена на ПОД/ФТ, главными из которых являются ООН и Интерпол. Данные организации для решения задачи по ПОД/ФТ разрабатывают комплекс специальных мероприятий (процедуры, экспертизы) с целью выявления как отдельных нарушений, так и признаков реализации указанной деятельности на постоянной основе .

Что касается отдельных стран, то Российская Федерация обладает достаточно развитой сетью организаций, занимающихся ПОД/ФТ (рисунок 4) [1-9].

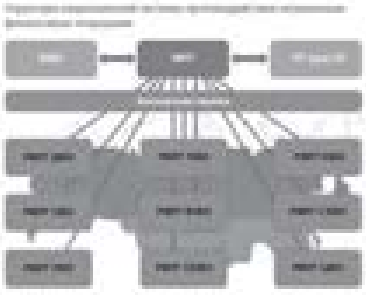


Рисунок 4 – Структура национальной системы противодействия незаконным финансовым операциям

Одной из ключевых задач в данной сфере остается повышение эффективного взаимодействия, координации и принимаемых мер всеми участниками национальной «антиотмывочной» системы.

Благодаря совместным усилиям участников национальной «антиотмывочной» системы в 2014 году удалось достигнуть заметных результатов (рисунок 5) [3].

Рисунок 5 – Национальная «антиотмывочная» система РФ

Таким образом, проблема ПОД/ФТ волнует все страны мира. Убытки от незаконной деятельности, связанной с ОД, наносят огромный ущерб мировой экономике. Данная тема является предметом постоянных обсуждений как для россиийской банковской системы, так и для мировой системы в целом. Для выработки эффективных решений существующих задач, связанных с пресечением деятельности по ОД, необходимо осуществлять как внутренний контроль (в пределах отдельно взятого государства), так и контроль (сотрудничество) на международном уровне.

В банковской практике под внутренним контролем в целях ПОД/ФТ понимается деятельность организаций, осуществляющих операции с денежными средствами или иным имуществом, по выявлению операций, подлежащих обязательному контролю, и иных операций, связанных с ОД, полученных преступным путем, и финансированием терроризма.

К операциям, подлежащим обязательному контролю, относятся [1, 2, 8, 9]:

1) Операции с денежными средствами или иным имуществом, если сумма, на которую они совершаются, равна или превышает 600 тыс. руб. либо равна сумме в иностранной валюте, эквивалентной 600 тыс. руб., или превышает ее, а по своему характеру данные операции относятся к одному из следующих видов операций:

- операции с денежными средствами в наличной форме;
- операции по банковским счетам (вкладам);
- сделки с движимым и недвижимым имуществом.

2) Кроме того, операция с денежными средствами или иным имуществом подлежит обязательному контролю в случае, если хотя бы одной из сторон является организация или физическое лицо, в отношении которых имеются полученные сведения об их причастности к экстремистской деятельности или терроризму, либо юридическое лицо, находящееся в собственности или под контролем таких организации или лица, либо физическое или юридическое лицо, действующее от имени или по указанию таких организации или лица.

При осуществлении банковской деятельности, также могут фиксироваться сомнительные операции и необычные сделки – операции, носящие запутанный (необычный) характер, не имеющие явного экономического смысла или цели. Как правило, цель таких сделок –уклонение от уплаты налогов, ОД или финансирование терроризма.

Для обнаружения необычной или подозрительной деятельности необходима организация постоянного внутреннего контроля – мониторинга, охватывающего всю систему финансовых операций в целом, а также соблюдение принципа «знай своего клиента», а именно, анализ контактов клиента, информации из независимых источников (например, из СМИ или сети Интернет), собственной информации об окружении клиента (рисунок 6) [1, 2, 8, 9].

Рисунок 6 – Организация взаимодействия в рамках ПОД/ФТ

При фиксации сомнительных операций и отсутствии рациональных объяснений им, могут быть приняты следующие решения:

– продолжить работу с клиентом, осуществляя повышенный контроль;

– информировать уполномоченные органы о зафиксированном случае.

Оповещение уполномоченных оргнизаций осуществляется службой контроля, кроме того, об инциденте могут быть проинформированы старшие должностные лица банка (например, руководитель подразделения, совет директоров).

Для организации эффективного контроля предлагается следующий алгоритм действий, который может существенно повысить раскрываемость подобного рода преступлений (рисунок 7) [1, 2, 8, 9].

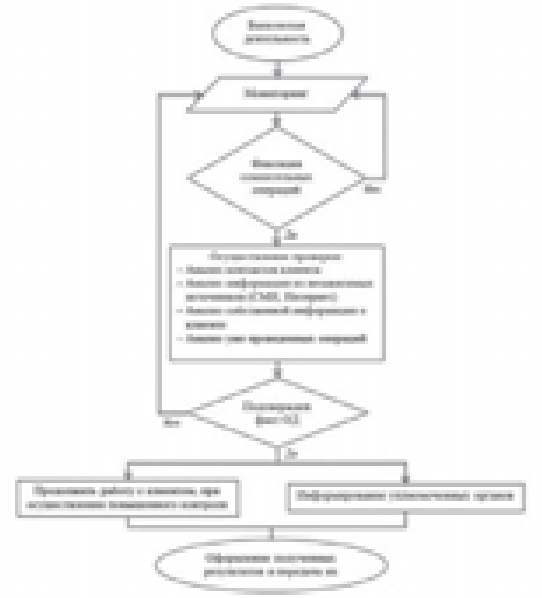


Рисунок 7 – Схема работы системы мониторинга (обнаружения мошенничества)

Подводя итоги, хотелось бы отметить, что ПОД/ФТ – проблема, волнующая все мировые державы, так как убытки от такой деятельности наносят огромный ущерб мировой экономике. В эффективной системе ПОД/ФТ заинтересованы, прежде всего, кредитные организации, так как большое количество сомнительных финансовых операций совершается именно через эти структуры, в

связи с этим именно банки обладают наиболее широким спектром возможностей противодействия отмыванию преступных доходов.

Литература

1. Федеральный закон от 07.08.2001 N 115-ФЗ (ред. от 29.06.2015) "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" (с изм. и доп., вступ. в силу с 30.10.2015)
2. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Некоторые перспективы применения систем контроля и управления доступом в региональных ВУЗАХ. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
3. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Развитие сотрудничества российских и зарубежных ВУЗОВ по защите информационного ресурса. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
4. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
5. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский

Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
6. Соляной В.Н., Сухотерин А.И Выработка коммуникативной компетенции при подготовке профессионалов по информационной безопасности с использованием технологии модерации. «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7
7. Соляной В.Н., Сухотерин А.И, Антоненко В.И. Проблемно-ориентированная подготовка специалистов по информационной безопасности с использованием имитационного метода (мозговой штурм). «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7.
8. Финансовый мониторинг: управление рисками отмывания денег в банках / П.В. Ревенков, А.Б. Дудка, А.Н. Воронин, М.В. Каратаев. – М.: КНОРУС : ЦИПСиР, 2012. – 280 с.
9. Публичный отчет о работе федеральной службы по финансовому мониторингу в 2014 году. Электронный ресурс. Режим доступа:
http://fedsfm.ru/content/files/activity/annualreports/посл.вер.%20отчет%202014.pdf (дата обращения06.12.2015).

МЕРЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ИНФОРМАЦИОННОЙ СИСТЕМЕ, ОТ НСД ПРИ ПРИМЕНЕНИИ БЕСПРОВОДНЫХ СЕТЕЙ

Кузнецова Алина Владимировна, студентка 4 курса кафедры Информационной безопасности
Научный руководитель: **Журавлев Сергей Иванович**, к.т.н., доцент кафедры Информационной безопасности

Использование компьютеров и автоматизированных технологий приводит к появлению ряда проблем для руководства организацией. Компьютеры, часто объединенные в сети, могут предоставлять доступ к колоссальному количеству самых разнообразных данных. Поэтому люди беспокоятся о безопасности

информации и наличии рисков, связанных с автоматизацией и предоставлением гораздо большего доступа к конфиденциальным, персональным или другим критическим данным. Электронные средства хранения даже более уязвимы, чем бумажные: размещаемые на них данные можно и уничтожить, и скопировать, и незаметно видоизменить.

Беспроводные сети, несанкционированный доступ, меры защиты.

MEASURES TO PROTECT THE INFORMATION CONTAINED IN THE INFORMATION SYSTEM FROM UNAUTHORIZED ACCESS WHEN USING WIRELESS NETWORKS

Kuznetsova Alina, 4th year student of the Department of information security
Scientific adviser: **Zhuravlev Sergey,** Candidate of Technical Sciences, Associate Professor of the Department of information security

The use of computers and automated technologies causes several problems for the management of the organization. Computers, often networked, can provide access to enormous amount of diverse data. So people are worried about information security and availability risks associated with automation and the provision of much greater access to confidential, personal or other critical data. Electronic means of storing even more vulnerable than paper: hosted data possible and to destroy, and to copy, modify and quietly.

Wireless networks, unauthorized access, security measures.

Беспроводные сети передачи данных (БСПД) могут использоваться для доступа к информационным ресурсам различных категорий, например, к информационным ресурсам сети Интернет, общедоступным и/или конфиденциальным информационным ресурсам организации. В зависимости от варианта использования БСПД, условно можно выделить 3 основных решения по обеспечению безопасности информации БСПД: решение по открытому доступу, решение по базовой безопасности и решение по повышенной безопасности (см. таблицу 1). Для реализации каждого из решений по обеспечению безопасности информации БСПД требуется реализация специфичного комплекса мер по защите информации [6].

Таблица 1 – Классификация решений по обеспечению безопасности информации БСПД

№ п/п	Классификационные признаки	Решение по обеспечению безопасности информации БСПД		
		Открытый доступ	Базовая безопасность	Повышенная безопасность
1.	**Тип БСПД**	1	2	3
2.	**Возможность выхода в сеть Интернет с использованием БСПД**	Да	Да	Да
3.	**Подключение к проводной сети организации**	Нет	Да	Да
4.	**Категория безопасности информации, обрабатываемой в проводной сети**	–	Общедоступная информация	Информация ограниченного доступа
5.	**Защищаемые характеристики безопасности информации, обрабатываемой в проводной сети**	–	Целостность; Доступность	Конфиденциальность; Целостность; Доступность
6.	**Требование по предоставлению удаленного доступа (в т.ч. беспроводного) к ресурсам организации**	–	Требуется	Требуется
7.	**Типы используемых АУ (личное/служебное)**	Личное АУ	Личное АУ –для доступа к сети Интернет; Служебное АУ – для доступа к сети Интернет и ресурсам организации	Личное АУ – для доступа к сети Интернет; Служебное АУ – для доступа к ресурсам организации

Для блокирования установленных угроз НСД к информации, содержащейся в информационной системе, при применении БСПД и способов реализации указанных угроз необходим набор организационных и технических мер по защите информации, дифференцированный в зависимости от варианта использования БСПД (см. таблицу 2).

Технические меры защиты информации от НСД к информации при применении БСПД могут быть реализованы как за счет использования механизмов, встроенных в оборудование БСПД, так и за счет использования механизмов, реализуемых наложенными средствами защиты информации.

В таблице 3 указаны специфичные меры по защите информации, содержащейся в информационной системе, от НСД при применении БСПД. В таблице не указываются общепринятые меры по защите информации, принимаемые при построении защищенных сетей (например, меры по обеспечению физической безопасности оборудования и каналов связи; меры по резервному копированию служебной и технологической информации, резервированию оборудования; и др.), а также меры по защите информации от утечек по техническим каналам, образованным оборудованием БСПД [1].

Предлагаемые меры по защите информации объединены в следующие группы:

– меры, реализуемые в отношении аппаратной и программной платформы оборудования БСПД;

– меры, реализуемые на объекте размещения оборудования БСПД;

– меры, реализуемые для обеспечения «подконтрольности» БСПД;

– меры по созданию элементов системы защиты от НСД с использованием наложенных средств защиты информации;

– меры по созданию элементов системы защиты от НСД с использованием встроенных в оборудование БСПД механизмов защиты информации от НСД;

– меры по защите подключений БСПД к внешним сетям [5].

Таблица 2 – Меры по защите информации, содержащейся в информационной системе, от НСД при применении БСПД

№ п/п	Меры по защите информации, содержащейся в информационной системе, от НСД при применении БСПД	Возможная реализация мер по защите информации	Решение по обеспечению безопасности информации		
			Открытый доступ	Базовая	Повышенная безопасность
1	**Меры, реализуемые в отношении аппаратной и программной платформы оборудования БСПД**				
	Использование оборудования БСПД, не имеющего программных и/или аппаратных закладок (электронных устройств негласного получения	Специальные проверки и специальные исследования оборудования БСПД на предмет выявления электронных	–	–	+/–

	информации, «жучков», «бэкдоров» и др.)	устройств негласного получения информации			
	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов, соответствующих требованиям по обеспечению информационной безопасности	Использование лицензионно чистого программного обеспечения и (или) его компонентов	+	+	+
		Использование программного обеспечения, соответствующего требованиям по обеспечению информационной безопасности (например, сертифицированной операционной системы семейства Microsoft Windows)	–	+/–	+
2	**Меры, реализуемые на объекте размещения оборудования БСПД**				
	Регламентация, ограничение и контроль использования технологий беспроводного доступа и беспроводных устройств [5]. Предоставление беспроводного Wi-Fi доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей [2]. Разграничение доступа с АУ различных видов (личных и служебных) к открытым и защищаемым ресурсам	Разработка и реализация регламента использования оборудования беспроводной передачи данных на объекте, устанавливающего: – виды беспроводного доступа, разрешенные в системе с использованием беспроводных устройств; – круг должностных лиц, которым необходим беспроводной Wi-Fi; – виды АУ, с которых разрешается выполнять беспроводной Wi-Fi доступ; – организационные меры по контролю за использованием в информационной системе технологий беспроводного Wi-Fi доступа и беспроводных Wi-Fi устройств; – правила и режимы использования беспроводных Wi-Fi устройств	–	+/–	+
		Выполнение доступа к ресурсам организации, распложенным в проводной сети организации, со служебных абонентских устройств		+	+
		Выполнение доступа к ресурсам организации, распложенным в проводной сети организации, с личных абонентских устройств		+/–	–
3	**Меры, реализуемые для обеспечения «подконтрольности» БСПД**				

	Мониторинг и контроль применения технологий беспроводного Wi-Fi доступа и беспроводных Wi-Fi устройств на предмет выявления их несанкционированного использования. Применение программно-технических средств для обнаружения, определения местоположения и блокирования несанкционировано используемых беспроводных устройств и беспроводных подключений по технологии Wi-Fi	Реализация системы мониторинга и контроля применения технологий беспроводного Wi-Fi доступа и беспроводных Wi-Fi устройств, обеспечивающей обнаружение, определение местоположения и блокирование несанкционировано используемых беспроводных устройств и беспроводных подключений по технологии Wi-Fi (например, системы, построенной с использованием программно-аппаратного комплекса AirMagnet Enterprise, либо с использованием технологии Cisco ClearAir)	–	+/–	+
	Выделение подсистемы сетевой коммутации БСПД в отдельный физический или логический сетевой сегмент	Логическое или физическое выделение на отдельном коммутационном оборудовании подсистемы сетевой коммутации БСПД	+	+	+
	Максимально возможная локализация зоны покрытия БСПД	Использование направленных антенн точек доступа. Использование средств и методов, существенно затрудняющих или блокирующих распространение беспроводного Wi-Fi сигнала в определенном направлении (например, средств экранирования или электромагнитного зашумления). Реализация ограничения на подключение к БСПД на низких скоростях	+/–	+/–	+
	Ограничение физической доступности БСПД	Реализация режима использования БСПД по заданному расписанию (например, исключительно в рабочие часы)	+/–	+/–	+/–
4	**Меры по созданию элементов системы защиты от НСД с использованием наложенных средств защиты информации**				
	Реализация на рабочем месте администратора центра управления БСПД мер по антивирусной защите	Установка и настройка на рабочем месте администратора центра управления БСПД средств антивирусной защиты (например, антивирусного программного обеспечения «Антивирус Касперского»)	+	+	+
	Реализация на рабочем месте администратора центра управления	Установка и настройка на рабочем месте администратора	–	+/–	+

	БСПД мер по защите информации от НСД	центра управления БСПД средств защиты информации от НСД (например, SecretNet, аппаратно-программного модуля доверенной загрузки «Соболь»)			
	Реализация на служебном АУ мер по защите информации от НСД, равносильных принятым в проводной сети организации и совместимых с ними	Установка и настройка на служебном АУ средств защиты информации от НСД, совместимых с используемыми в проводной сети организации и позволяющих реализовать равнопрочную систему защиты информации (например, сертифицированной операционной системы семейства Microsoft Windows, программного модуля доверенной загрузки, антивирусного программного обеспечения «Антивирус Касперского»)		+	+
	Обеспечение централизованной идентификации и аутентификации пользователей БСПД	Использование средств централизованной идентификации и аутентификации пользователей БСПД (например, Radius-сервера)	+/–	+/–	+
	Выполнение очистки (удаления) информации на АУ после завершения сеанса удаленного доступа к ресурсам проводной сети организации или принятие иных мер, исключающих несанкционированный доступ к хранимой защищаемой информации	Использование средств очистки остаточной информации по завершению сеанса удаленного доступа к ресурсам проводной сети организации (например, SecretNet, СГУ-1) или использование средств шифрования информации, хранимой на АУ (например, SecretDisk)		–	+
	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при доступе с АУ к ресурсам проводной сети организации	Использование на АУ клиентского программного обеспечения для шифрования (например, ViPNet Client или «Континент АП»). Использование на границе проводной сети организации шлюза контроля доступа для расшифрования получаемой от АУ информации (например, ViPNet Coordinator или АПКШ «Континент»)		+/–	+
5	**Меры по созданию элементов системы защиты от НСД с использованием встроенных в оборудование БСПД механизмов защиты информации от НСД**				
	Обеспечение сокрытия БСПД от нарушителя	Сокрытие идентификатора БСПД	+/–	+	+

	Обеспечение стойких методов (технологий) идентификации, аутентификации и шифрования беспроводных WI-Fi подключений	Реализация идентификации АУ по MAC-адресам и/или идентификаторам IMEI/IMSI	–	+/–	+
		Использование строгих методов идентификации, аутентификации и шифрования (например, технологии WPA)	+	+	+
	Применение уникальных имени пользователя и пароля для подключения к БСПД	Использование уникальных имени пользователя и пароля для подключения к БСПД (например, использование технологии WPA-Enterprise совместно с Radius-сервером)	–	+/–	+
	Централизованное управление БСПД	Реализация центра управления БСПД	+/–	+/–	+/–
6	**Меры по защите подключений БСПД к внешним сетям**				
	Обеспечение обнаружения (предотвращения) вторжений (компьютерных атак) на границе между подсистемой сетевой коммутации БСПД и внешней сетью (например, сетью Интернет)	Использование системы обнаружения и/или предотвращения вторжений (например, системы обнаружения атак «Форпост» или «Аргус», системы обнаружения атак ViPNet IDS)	–	+	+
	Управление (контроль) входящими и исходящими из БСПД информационными потоками, реализуемое на физической и (или) логической границе БСПД с внешними сетями, подключаемыми по проводным каналам связи. Обеспечение взаимодействия БСПД с внешними сетями только через сетевые интерфейсы, которые обеспечивают управление (контроль) информационными потоками с использованием средств защиты информации, установленных на физическом и (или) логическом периметре БСПД	Использование средств межсетевого экранирования на физической и (или) логической границе БСПД с внешними сетями (например, Cisco PIX Firewall, средств межсетевого экранирования, встроенных в ViPNet Coordinator или АПКШ «Континент»)		+	+

Обозначения, используемые в таблице 3:

«+» – мера по защите информации, указанная в строке таблице, рекомендована к использованию для реализации решения по обеспечению безопасности информации, указанного в столбце таблице;

«+/–» – мера по защите информации, указанная в строке таблице, может не использоваться для реализации решения по обеспечению безопасности информации, указанного в столбце таблице (в зависимости от выявленных угроз безопасности

информации и/или предъявляемых требований по обеспечению безопасности информации);

«–» – мера по защите информации, указанная в строке таблице, не используется для реализации решения по обеспечению безопасности информации, указанного в столбце таблице.

Отсутствие обозначений в столбце говорит о неприменимости меры по защите информации для реализации решения по обеспечению безопасности информации.

Таблица 3 – Таблица соответствия способов реализации угроз и мер, направленных на их блокирование

№ п/п	Название группы способов реализации угроз НСД к информации	Название группы мер по защите информации
1.	Способы, реализация которых зависит от доверенности используемой аппаратной и программной платформы оборудования БСПД	Меры, реализуемые в отношении аппаратной и программной платформы оборудования БСПД
2.	Способы, реализация которых зависит от применяемых на объекте размещения оборудования БСПД организационных мер по защите информации	Меры, реализуемые на объекте размещения оборудования БСПД
3.	Способы, реализация которых зависит от «подконтрольности» БСПД	Меры, реализуемые для обеспечения «подконтрольности» БСПД
4.	Способы, реализация которых зависит от установленных на оборудование БСПД средств защиты информации от НСД и корректности их настройки	Меры по созданию элементов системы защиты от НСД с использованием наложенных средств защиты информации
5.	Способы, реализация которых зависит от используемых встроенных в оборудование БСПД механизмов защиты информации от НСД и корректности их настройки	Меры по созданию элементов системы защиты от НСД с использованием встроенных в оборудование БСПД механизмов защиты информации от НСД
6.	Способы, реализация которых зависит от наличия подключения БСПД к внешним сетям (например, к сети Интернет)	Меры по защите подключений БСПД к внешним сетям

Меры по защиты информации, предлагаемые для реализации различных решений по обеспечению информационной безопасности, являются базовыми и могут адаптироваться, уточняться и/или дополняться с учетом используемых в конкретной системе информационных технологий, по результатам выполнения анализа рисков и разработки модели угроз безопасности информации, а также с учетом требований по защите информации, установленных нормативными правовыми актами в области защиты информации, либо предъявляемых заказчиком разработки системы защиты информации. При невозможности реализации отдельных мер по

защите информации могут использоваться иные (компенсирующие) меры по защите информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации и способов их реализации [2, 3, 5].

Каждая из представленных мер по защиты информации обеспечивает блокирование одной или совокупности угроз безопасности информации (способов реализации угроз безопасности информации), установленных в настоящем разделе. Комплекс общепринятых и предложенных специфичных мер по защите информации, содержащейся в информационной системе, от НСД при применении беспроводных сетей передачи данных обеспечивают блокирование выявленных угроз безопасности информации и способов их реализации [4, 3].

Литература

1. Белый В.М., Белый Р.В. Эффективность информационных систем и информационных технологий: учебник – Королёв МО; ФТА, 2013 – 396 с.
2. Гришина Н. В. Организация комплексной системы защиты информации. – М.: Гелиос АРВ, 2007. – 256 с.
3. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты: учеб. пособие для ВУЗов – М.: ТИД Диа Софт,2002 г. – 688 с.
4. Журавлев С.И., Мирсаитов Р.С. Один из подходов статистического анализа защищенного трафика ведомственных IP-сетей. Статья в журнале «Двойные технологии» № 1, 2015, с. 34-39.
5. Курило А.П. Основы управления информационной безопасностью - Горячая линия-Телеком,-М.: 2013
6. Северин В.А. - Комплексная защита информация на предприятия для вузов – Городец,-М.: 2008

СОВЕРШЕНСТВОВАНИЕ ЗАЩИТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ НА ОСНОВЕ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ ЦВЗ

Кузнецова Алина Владимировна, студентка 4 курса кафедры Информационной безопасности
Научный руководитель: **Сухотерин Александр Иванович,** к. воен.н., доцент кафедры Информационной безопасности

В любом правовом государстве все правомочия физических и юридических лиц должны защищаться должным образом. Гарантия неприкосновенности интеллектуальной собственности выступает главным фактором успешного развития той или иной сферы культурной и политической деятельности любой страны. Для субъектов отраслевого права предусмотрена защита, и обладатель интеллектуального права имеет набор прав и обязанностей, прямо предусмотренных законодательством РФ.

Интеллектуальная собственность, патентное право, цифровые водяные знаки, субъекты и объекты.

IMPROVING THE PROTECTION OF INTELLECTUAL PROPERTY THROUGH THE USE OF DIGITAL WATERMARKING TECHNOLOGY

Kuznetsova Alina, 4rd year student of the Department of information security
Scientific adviser: **Sukhoterin Alexander,** Candidate of Military Sciences, docent of the Department of information security

In any state of law, all the powers of natural and legal persons should be protected properly. The guarantee of the inviolability of intellectual property is a key factor in the successful development of any sphere of cultural and political activity in any country. For the subjects of industry law, provides protection, and intellectual property rights holder has a set of rights and duties expressly provided for by the legislation of the Russian Federation.

Intellectual property, patent law, digital watermarks, subjects and objects.

Проблема защиты авторских прав приобрела особую актуальность с развитием цифровых технологий и Интернета.

Несмотря на постоянное совершенствование законодательства, в том числе международного, в сфере авторского права, а также непрерывное совершенствование и усложнение технических и программных средств, направленных на предотвращение нарушений в этой области, пиратское использование интеллектуальной собственности стало массовым явлением, ущерб от которого в глобальном масштабе превышает многие миллиарды долларов. Крайне актуальной задача защиты авторских прав является для тех, чья работа связана со СМИ, как печатными, так и электронными, а также рекламной деятельностью. Как только текст, фотография или видеозапись представлены публично, автор или правообладатель практически теряет контроль над возможным несанкционированным использованием материала. Для всех очевидна острота этой проблемы, когда речь идет о размещении тех или иных работ в Интернете, однако на практике очень часто грубые нарушения авторского права имеют место и тогда, когда представленный в виде цифрового файла материал предоставляется, например, в издательство или напрямую в типографию. В случае, когда помимо законной публикации появляются и несанкционированные, естественно, без заключения договора с автором или правообладателем, без выплаты соответствующего вознаграждения за использование работы, а зачастую, даже без указания авторства, у законного владельца прав на пиратски использованный материал остается, практически, только один путь – путь судебного разбирательства.

Первостепенным способом защиты интеллектуальной собственности в России является законодательство. В различных федеральных законах, кодексах и других нормативно-правовых актах прописаны: как защищать, что защищать и какой наказание за неправомочное использование запатентованных изобретений. Но со стороны, например, технической защиты программ ЭВМ, баз данных, композиций и всего того, что существует в электронном виде, существует множество упущений, благодаря чему, многие запатентованные объекты попадают в сеть и распространяются там путем «пиратства».

Согласно п. 1 ст. 1225 ГК РФ интеллектуальной собственностью являются охраняемые правом РИД и приравненные к нам средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий, такие как:

1) произведения науки, литературы и искусства;
2) программ ЭВМ;
3) базы данных;
4) изобретения;
5) полезные модели;
6) промышленные образцы;
7) секреты производства и др. [2].

Специфика угроз перечисленным объектам информационной безопасности состоит в их многообразии, сложности идентификации, поскольку, как правило, они носят уникальный или индивидуальный характер». При классификации угроз в этой области необходимо уделять особое внимание изучению возможности промышленного шпионажа специальных служб и криминальных структур.

Вследствие этой специфики объекты информационной безопасности в области науки, техники и технологии трудно защитимы. Должна быть организована система оценки возможных последствий воздействия угроз на указанные объекты, включающая общественные научные советы и институт независимых экспертиз, вырабатывающие рекомендации для каждого конкретного случая распространения или использования научной, технической и технологической продукции с целью предотвращения незаконного присвоения или использования научного и интеллектуального потенциала.

Реальный путь противодействия угрозам со стороны государства заключается в постоянном совершенствовании законодательства в этой области и механизмов его реализации. Многие мероприятия по предотвращению или нейтрализации угроз в этой области, особенно в части, касающейся научных кадров, лежат в сфере социальной и экономической политики государства [5].

Использование цифровой информации в настоящее стало повсеместным. Но наряду с этим в современном информационном обществе, исследования и разработки в области стеганографии становятся все более популярными. Это связано с тем, что существуют проблемы управления цифровыми ресурсами и контроля использования прав собственности на компьютерные файлы [4].

Стеганография — это метод организации связи, который, собственно, скрывает само наличие связи. В отличие от криптографии, где злоумышленник точно может определить, является ли передаваемое сообщение зашифрованным текстом,

методы стеганографии позволяют встраивать кодированные сообщения в безобидные послания так, чтобы невозможно было заподозрить существование встроенного послания [3].

Происходящие в последние годы процессы развития новых, обезличенных средств обмена электронной информацией, таких как международная компьютерная сеть Интернет, изменение самой концепции создания контента, в которой могут теперь участвовать не только автор, но и пользователи, остро поставили вопрос идентификации и защиты прав интеллектуальной собственности. В условиях, когда обладатели авторских прав не могут проследить за использованием своих произведений и получить причитающееся им вознаграждение, они не заинтересованы в предоставлении своих произведений.

Задача установления и охраны авторских прав (защиты интеллектуальной собственности) тесно связана с задачей ограничения доступа. Для этой цели, например, в системах цифрового ТВ и звукового вещания применяют специальные метки (маркеры) авторского материала и скомпонованных программ, так называемые цифровые водяные знаки (Digital Watermark, DW — ЦВЗ). Цифровые методы ограничения доступа, в частности, частая смена ключей, позволяют передать содержание исключительно подписчикам службы. Но при этом все равно остается задача удостовериться, что содержание не было нарушенным.

ЦВЗ — это нестираемый скрытый код (или метка), который незаметным образом вводится в аудиовизуальные сигналы программы и позволяет проверить оригинальность материала или предоставляет средства для транспортировки скрытой информации. Право выделения ЦВЗ и отображения предоставляется только тем, у кого есть ключ для их выделения, контроля и использования с целью идентификации содержания, установления аутентичности (подлинности), обнаружения копий, контроля трафика и т.п.

Цифровые водяные знаки (или метки) делятся на два типа: видимые и невидимые.

Чтобы технология ЦВЗ обеспечивала защиту, они должны отвечать следующим требованиям:

- индивидуальность алгоритма нанесения ЦВЗ;
- невидимость метки для пользователей;
- невозможность извлечения ЦВЗ третьими лицами;
- возможность обнаружения несанкционированного

использования файла, помеченного ЦВЗ;

• устойчивость к изменениям носителя/контейнера (изменение формата, размеров - масштабирование, сжатие, поворот, фильтрация, спецэффекты, монтаж, аналоговые и цифровые преобразования).

Основным недостатком методов, предусматривающих внедрение в цифровых водяных знаков, является их неспособность предотвратить незаконное использование авторских материалов.

Основные отличия цифровых водяных знаков от обычных (бумажных) заключаются в том, что ЦВЗ невидимы (существует всего несколько случаев применения видимых ЦВЗ), а также в том, что задача злоумышленника состоит не в наиболее точной имитации водяного знака, а, напротив, в его полном уничтожении.

Требование невидимости необходимо прежде всего для того, чтобы злоумышленник не смог обнаружить цифровой водяной знак визуально (так как в этом случае его задача существенно упрощается). Лучшим способом борьбы с атаками является распределение ЦВЗ по всему цифровому контейнеру. Если речь идет об изображении (фотографии), основными атаками (методами уничтожения) на ЦВЗ являются: масштабирование, поворот на произвольный угол, вырезание каких-либо участков изображения, конвертирование в другой графический формат, печать и последующее сканирование [2] (смысл в этом имеется, если, конечно, после таких преобразований, картинка похожа на первоначальный вариант). Цифровой водяной знак должен успешно противостоять подобным атакам.

На сегодняшний день существует большое количество систем внедрения ЦВЗ в электронную информацию, некоторые из них уже используются на практике; в каждой из сред есть множество способов строить скрываемую информацию. Менее проработанным является вопрос защиты текстовой информации при помощи внедрения ЦВЗ [6].

Цифровые водяные знаки и отпечатки пальцев всем хороши, кроме одного. Скопируйте бумагу, и водяные знаки пропадут. Скопируйте цифровой файл, и водяные знаки перейдут на копию.

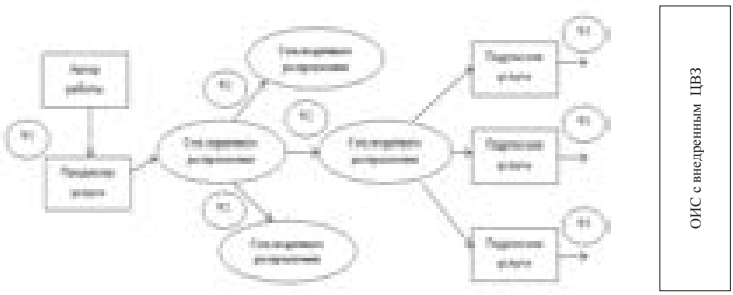
Стегосистемы ЦВЗ, в частности, должны выполнять задачу защиты авторских и имущественных прав на электронные сообщения при различных попытках активного нарушителя искажения или стирания встроенной в них аутентифицирующей информации. Формально говоря, системы ЦВЗ должны обеспечить

аутентификацию отправителей электронных сообщений. Подобная задача может быть возложена на криптографические системы электронной цифровой подписи (ЭЦП) данных, но в отличие от стегосистем ЦВЗ, известные системы ЭЦП не обеспечивают защиту авторства не только цифровых, но и аналоговых сообщений в условиях, когда активный нарушитель вносит искажения в защищаемое сообщение и аутентифицирующую информацию. Иные требования по безопасности предъявляются к стегосистемам, предназначенным для скрытия факта передачи конфиденциальных сообщений от пассивного нарушите- ля. Также имеет свои особенности обеспечение имитостойкости стегосистем к вводу в скрытый канал передачи ложной информации [5].

Маркирование ЦВЗ напоминает процесс присвоения программе в ходе ее производства некоторого ярлыка, который подтверждает права собственности на нее. Без специальных технических средств ЦВЗ является невидимым, никоим образом не нарушающим программу (в худшем случае он просто добавляет небольшой шум к видимому содержанию программы) и не может быть подделан.

Для ввода ЦВЗ в сигнал и для обнаружения его в сигнале требуется специальная кодовая комбинация, несущая информацию о параметрах ввода, — ключ ЦВЗ. Непреднамеренные искажения сигнала вместе с введенным ЦВЗ при обработке и при передаче по каналу или преднамеренные пиратские попытки взлома и подавления ЦВЗ ведут к снижению надежности его обнаружения и выделения. Для осуществления процесса детектирования ЦВЗ ключ должен быть передан на детектор защищенным образом. При детектировании выносится двоичное решение — присутствует или нет ЦВЗ в сигнале. Секретные ключи ЦВЗ могут выполнять роль идентификационного номера владельца информации или ее получателя. Вследствие малого объема информации, помещающейся в ЦВЗ, в нем может лишь быть посыл к записи в базе данных, содержащей подробные сведения о защищаемом контенте.

Ввод и передача ЦВЗ сопровождается всегда степенью заметности (видимости-открытости) его и степенью надежности (устойчивости к различного рода преобразованиям и ложной тревоге). Ввод ЦВЗ может быть осуществлен в различных точках тракта телевещания (направленной телепередачи). Выделяют три характерные точки маркирования (Wl, W2, W3), которые показаны на функциональной схеме сети вещания на рис. 1 [1].



Условные обозначения: $W_{1,...}$ W_3 - точки ввода.

Рисунок 1 - Варианты размещения точек ввода ЦВЗ

ЦВЗ W1 (универсальный указатель базы данных прав собственности) идентифицирует некоторую работу (услугу, программу) в момент ее создания, например, используя маркирование непосредственно в видеокамере. ЦВЗ W1 указывает на запись в базе данных, которая хранит описание этой работы. Универсальная структура W1 — кодовая комбинация длиной 64 бита, разделенная на три поля. В виде конкретного варианта может быть такой. Первое поле длиной 8 бит отводится для идентификации международной организации, которая стандартизирует описание содержания базы данных (255 организаций). Второе поле длиной 15 бит предназначено для идентификации местного агентства, уполномоченного международной организацией распределять указатели W1 (32768 местных агентств). Третье поле длиной 41 бит — это собственно идентификационный номер (каждое местное агентство может идентифицировать 2199 миллиардов выполненных работ).

ЦВЗ W2 служит для защиты в тракте первичного распределения программ. Этот тракт представляет собой систему с одним входом (на него поступает сигнал с введенным ЦВЗ W1) и множеством выходов. На каждом из выходов с целью его идентификации вводится ЦВЗ W2 длиной 64 бита, содержащий идентификационные номера поставщика и получателя программы, а также краткие сведения о вещателе, получающем программу для дальнейшего распределения.

ЦВЗ W3 используется для контроля возможного пиратского копирования программ, получаемых подписчиком, и вводится непосредственно в приемнике-декодере конечного пользователя [1].

В данной работе были выявлены уязвимые места в защите интеллектуальной собственности России в Интернет пространстве:

1. На законодательном уровне - отсутствуют законодательные акты по защите цифровой интеллектуальной собственности;

2. На программно-аппаратном уровне - отсутствуют высокоэффективные механизмы по защите цифровой интеллектуальной собственности.

Предложен наиболее целесообразный способ защиты цифровых объектов интеллектуальной собственности, находящейся в электронном виде – использование цифровых водяных знаков. Данный механизм достаточно простой по реализации и обеспечивает многовариантоность цифровых водяных знаков, что обуславливает его практическую значимость.

Литература

1. Барсуков В.С. Романцов А.П. Компьютерная стеганография: вчера, сегодня, завтра. Технологии ин- формационной безопасности XXI века // Специальная техника. – 1998.

2. Защита интеллектуальной собственности: учебник для бакалавриата и магистратуры / А.К. Жарова; под общ. ред. проф. С.В. Мальцевой. – 2-е изд., перераб. и доп. – М. : Издательство Юрайт, 2015. – 426 с. – Серия: Бакалавр и магистр. Академический курс.

3. Интеллектуальные активы: закрепление прав на интеллектуальную собственность // Журнал «INSIDE» №3 2015 г., Зорина Ю.Г., Павлов В.Ю., Парвулюсов Ю.Ю., Фокин Г.В..

4. Использование стенографических методов для защиты текстовой информации. М.: T-comm Телекоммуникации и транспорт, 2009. С. 42-50.

http://studme.org/1079042219308/etika_i_estetika/zaschita_intellektualnoy_sobstvennosti http://refoteka.ru/r-154584.html#_ Toc129863537

5. Основы практической защиты информации. 4-е изд., доп. Учебное пособие. – М.: СОЛОН-Пресс, 2005. – 384 с.: илл.

6. Соляной В.Н., Сухотерин А.И. Модульно-ориентированный подход формирования базовых дисциплин ФГОС ВО 3+ как основа реализации профессиональной подготовки бакалавров в области информационной безопасности Научно-практический журнал №25, том 2 2015г. Информационное противодействие угрозам терроризма Материалы XIX Пленума учебно-методического объединения по образованию в области информационной безопасности «учебно-методическое обеспечение образовательных программ в области

информационной безопасности» г. таганрог. рост. обл.: изд-во южн.фед.унив, 2015.-332 с. issn 2219-8792
7. Соляной В.Н., Сухотерин А.И. Становление направления «Радиоэлектронная безопасность информационных объектов» в системе дополнительного профессионального по информационной безопасности. Научно-практический журнал №25, том 2 2015г. Информационное противодействие угрозам терроризма Материалы XIX Пленума учебно-методического объединения по образованию в области информационной безопасности «учебно-методическое обеспечение образовательных программ в области информационной безопасности» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН.ФЕД.УНИВ, 2015.-332 с. ISSN 2219-8792
8. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Некоторые перспективы применения систем контроля и управления доступом в региональных ВУЗАХ. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
9. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Развитие сотрудничества российских и зарубежных ВУЗОВ по защите информационного ресурса. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.

СОВЕРШЕНСТВОВАНИЕ УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ФИНАНСОВО – КРЕДИТНОЙ СФЕРЕ

Кузнецова Алина Владимировна, студентка 3 курса кафедры Информационной безопасности, **Суржиков Дмитрий Игоревич,** магистрант 2 курса кафедры Информационной безопасности
Научный руководитель: **Сухотерин Александр Иванович,** к.воен.н., доцент кафедры Информационной безопасности

В данной статье раскрывается понятие инцидента, определенны основные проблемы по реагирования на инциденты в финансово-кредитной сфере. Проанализирован внутренний контроль за инцидентами в финансовых структурах. Так же разработана система оповещения служб информационной безопасности банков.

Инцидент, менеджмент информационной безопасности.

IMPROVING THE MANAGEMENT OF INFORMATION SECURITY INCIDENTS IN THE FINANCIAL - CREDIT SPHERE

Kuznetsova Alina, 3rd year student of the Department of information security, **Surgikov Dmitry,** 2nd year undergraduate of the Department of information security
Scientific adviser: **Sukhoterin Alexander,** Candidate of Military Sciences, Associate Professor of the Department of information security

In this article we give a notion of the incident, define the major problems in responding to incidents in the sphere of Credit and Finance. The internal control over incidents in financial structures was analyzed. Also a system of notification of information security services of banks was developed.

Incident, management of information security.

Построение системы обеспечения ИБ в банках в большинстве случаев реализуется на основе требований международных или отраслевых стандартов в области обеспечения ИБ, с использованием процессно-ориентированного подхода, с учётом специфики банка. Прежде всего – количества и разнообразия информационных систем (ИС) и рабочих мест, решаемых задач и типов обрабатываемых

данных, требований по уровням защищённости, территориальной распределённости и т.п.

В большинстве стандартов в области обеспечения ИБ выделяются следующие основные направления деятельности по обеспечению ИБ:

- составление модели угроз и нарушителей ИБ;
- оценка рисков нарушений ИБ;
- внедрение и совершенствование защитных мер;
- создание службы ИБ;
- менеджмент ИБ;
- менеджмент инцидентов ИБ;
- защита персональных данных и другие.

В настоящее время значительное внимание уделяется вопросам менеджмента инцидентов ИБ, что свидетельствует о соответствующем уровне зрелости банка и обусловлено рядом факторов. Прежде всего, участившимися случаями хищений в системах дистанционного банковского обслуживания (ДБО), внутренними мошенничествами в платёжных системах, случаями инсайдерства (особенно при переходе на работу в другую организацию), предпосылками к утечкам конфиденциальной информации, сбоями в работе ИС и другими нарушениями ИБ [7].

Рисунок 1 - Построение управления инцидентами

Обнаружение инцидента всегда сопряжено со стрессом. Сотрудники осознают возможные негативные последствия и должны четко знать все необходимые действия шаг за шагом ведущие к устранению инцидента (рисунок 2).

В подобном ситуации, при отсутствии четких инструкций и должного уровня обучения, процесс реагирования на инциденты

превращается в случайные попытки выявления и устранения инцидентов. Зачастую функции, которые чётко должен выполнять один человек, «размазываются» между несколькими сотрудниками, которые в результате действуют параллельно и лишь теряют драгоценное время [6].

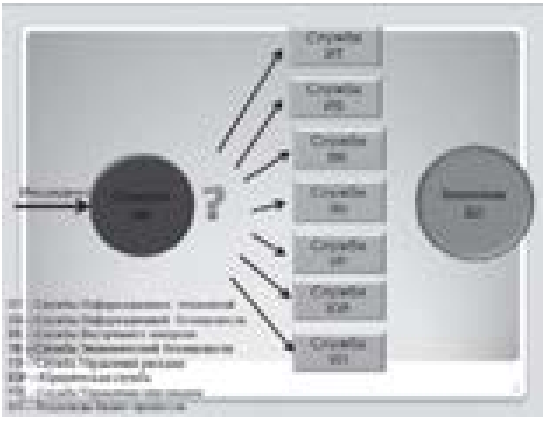


Рисунок 2 – Службы, ответственные при инциденте

Для слаженной работы всех необходимых подразделении необходимо выстроить формализовать и документировать все процессы (рисунок 3) [2].

Рисунок 3 - Этапы устранения инцидентов

Управление инцидентами – сложный процесс, требующий от участков слаженной и точной работы. Именно для того, чтобы любой инцидент не превращался в «ночной кошмар», следует четко придерживаться определенных формальных алгоритмов работы.

Поскольку успешное функционирование процесса в 90% зависит от персонала, особое внимание следует уделять вопросам тестирования планов реагирования на инциденты и восстановления. В любой нештатной ситуации следует придерживаться в порядке приоритета следующих принципов:

1) Безопасность сотрудников и посетителей.
2) Сдерживание инцидента и минимизация ущерба.
3) Безопасность активов организации.
4) Безопасность информационных ресурсов.
5) Восстановление в соответствии с требованиями бизнеса.
6) Расследование инцидента.
7) Принятие мер по недопущению повторения инцидента.

В ходе исследования были выявлены 7 шагов, которые позволяют эффективно построить процедуру управления инцидентами.

Эти семь очевидных шагов – семь важных правил, которые нужно соблюдать, чтобы эффективно построить процессы управления инцидентами информационной безопасности [7].

Предложения по дальнейшему совершенствованию управления инцидентами информационной безопасности в финансово – кредитной сфере

В большинстве случаев, банки работают в одиночку, когда их настигает мошенник, и нет помощи «извне», проще говоря, другие банки не участвуют в устранение инцидента и минимизировании затрат. Это способствовало бы более быстрому реагированию, и было бы экономически целесообразно. Создание базы данных, которая будет доступна специальной структуре «Служба безопасности банков» (СББ), в которой будет информация о всех инцидентах во всех банках России.

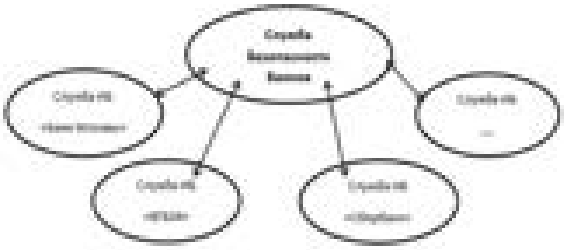


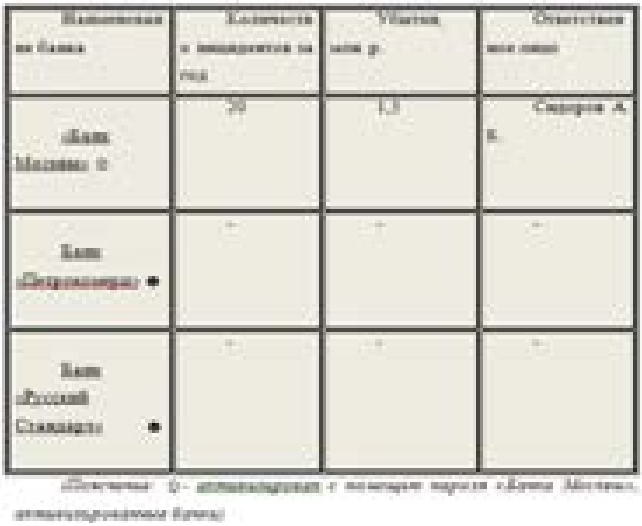
Рисунок 4 - Схема связи Службы безопасности банков с банками

С этой службой будет иметь связь подразделение «Информационной безопасности банка», каждого в частности.

Каждый банк будет иметь доступ к базе данных своих инцидентов, но не других банков, это прерогатива СББ (рисунок 4).

Каждый банк, будет иметь свой логин и пароль для входа в базу данных. После входа в систему, банк будет иметь доступ только к своей базе, где хранятся инциденты за определенный период (таблица 1).

Таблица 1- Общие сведения о количестве инцидентов за 2013 г.



Дальше служба информационной безопасности банка, если такая имеется, или служба безопасности банка может посмотреть по базе, какие инциденты были в банке (рисунок 5).

Рисунок 5 - Виды инцидентов на примере «Банка Москвы»

После выбора категории происшествия, специалист службы может дополнить информацию об уже имеющемся инциденте, добавить новый инцидент или просто просмотреть информацию (рисунок 6).

Рисунок 6 - Инциденты по датам на примере «Банка Москвы»

На рисунке 7 представлено описание инцидента «Мошенничество» произошедшее 23 марта 2006 г в банке «Банк Москвы».

Рисунок 7 - Описание инцидента на примере «Банка Москвы»

Создание «Службы Безопасности Банков России» - это одна из верхних ступеней, которая поможет искать всех преступников, и даст ощущение гражданам, что их сбережения в безопасности. В России должно быть верховенство права и закона во всех сферах жизнедеятельности общества, в том числе и в киберпространстве.

Создание общей «Базы данных инцидентов» упростит работы служб безопасности, ведь большое количество преступлений совершается одним и тем же злоумышленником, поэтому история о каждом из преступлений, поможет выявить того, кого долго искали несколько банков.

Литература

1. Распоряжение Правительства РФ от 03.11.2011 № 1944-р «О перечне направлений подготовки (специальностей) в образовательных учреждениях высшего профессионального образования, специальностей научных работников, соответствующих приоритетным направлениям модернизации и технологического развития российской экономики» Официальная публикация в СМИ: "Российская газета", № 254, 11.11.2011 "Собрание законодательства РФ", 14.11.2011, № 46, ст. 6584.
2. Безопасность банковской деятельности /Гамза В. А./Ткачук И.Б./ 2-е издание;
3. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В., Скрыль С.В., Голубятников И.В. Технические средства и методы защиты информации. Под ред. А.П.Зайцева и А.А.Шелупанова. М.: Машиностроение, 2009.
4. Манько Н.П., Сухотерин А.И., Антоненко В.И. Взгляды на роль и технологию организации самостоятельной работы, как одного из направлений совершенствования образовательного процесса. «Современные образовательные технологии, используемые в очном, заочном и дополнительном образовании» [Текст] сборник – Королёв МО: Изд-во «Канцлер», ФТА, 2014.
5. Методы оценки несоответствия средств защиты/Марков А. С,/Цирлова В. Л./Барабанов А. В./ Издательство «Радио и связь»;
6. Организация и оптимизация менеджмента инцидентов/ журнал «BISjornal», автор Писаренко Игорь, Банк ВТБ24 (ЗАО) (начальник отдела методологии и контроля Управления информационной безопасности).
7. Построение процесса управления инцидентами / журнал «BISjornal», автор Павел Хижняк – руководитель отдела аудита и консалтинга ЗАО «Практика Безопасности», CISM;
8. Соляной В.Н., Сухотерин А.И., Успенский Ф. А. Новые образовательные технологии в подготовке профессионалов информационной безопасности на базе ГБОУ ВПО МО «Финансово технологическая академия» «Современные образовательные технологии, используемые в очном, заочном и дополнительном образовании» [Текст] сборник – Королёв МО: Изд-во «Канцлер», ФТА, 2014.
9. Соляной В.Н., Сухотерин А.И., Федоров М.А. Выбор и внедрение новых образовательных технологий в (учебный процесс)

подготовку бакалавров (специалистов) и магистров по информационной безопасности. «Современные образовательные технологии, используемые в очном, заочном и дополнительном образовании» [Текст] сборник – Королёв МО: Изд-во «Канцлер», ФТА, 2014.
10. Соляной В.Н., Сухотерин А.И.. Взаимодействие человека, техники и природы: проблема информационной безопасности. Научный журнал (КИУЭС) Вопросы региональной экономики. УДК 007.51 №5 (05) г. Королёв. ФТА. 2010г.
11. «Технологический университет делится опытом информационной безопасности». Газета «Подмосковье» от 13 марта 2015 года. Пятница. №43 (3468).

АНАЛИЗ УЯЗВИМОСТЕЙ МОБИЛЬНЫХ ПЛАТЕЖНЫХ ПРИЛОЖЕНИЙ

Маслова Ольга Сергеевна, студентка 1 курса кафедры Информационной безопасности
Научный руководитель: **Соляной Владимир Николаевич,** к.воен.н., доцент, заведующий кафедрой Информационной безопасности

В настоящее время значительно возросло участие мобильных устройств в повседневной жизни: если раньше телефон рассматривался исключительно с точки зрения средства связи, то на сегодняшний день смартфон может выполнять множество других функций. В частности, платежные приложения, которые постепенно появляются на наших мобильных устройствах (смартфонах, планшетах и т.д.). Мобильные устройства пока еще недостаточно изучены, и каждая мобильная ОС (Android, iOS, Windows Phone, Symbian, BlackBerry и т.п.) имеет свою специфику, поэтому в каждой из них можно обнаружить большое количество, как новых уязвимостей, так и хорошо известных.

Мобильных платежи, анализ уязвимостей, безопасность.

VULNERABILITY ANALYSIS OF MOBILE PAYMENT APPLICATIONS

Maslova Olga, 1st year student of the Department of information security
Scientific adviser: **Solyanoy Vladimir,** Candidate of Military Sciences, Associate Professor of the Department of information security

At the present time it has increased significantly the participation of mobile devices in everyday life: if before the phone was considered solely in terms of communications, the smart phone today can perform many other functions. In particular, payment applications, which gradually appear on our mobile devices (smartphones, tablets, etc.). Mobile devices are still not well understood, and each mobile OS (Android, iOS, Windows Phone, Symbian, BlackBerry, etc.) has its own peculiarities, so each of them can be found a large number of both new vulnerabilities, and is well known .

Mobile payments, vulnerability analysis, security.

С ростом популярности разработки мобильных приложений, повышается их капиталоёмкость, а вместе с этим и желание злоумышленников перевести эти капиталы на свои счета. Многие современные мобильные программы предполагают внутренние покупки, а также отправку SMS на платные номера, именно эти лазейки могут использовать хакеры. Механизмов взлома и вытаскивания денег из мобильных устройств чрезвычайно много, каждый год появляются новые алгоритмы, но вместе с тем растёт и сила противодействия, способная своевременно бороться с угрозами.

Оплата за товары и услуги с помощью мобильных устройств уже перестала быть экзотикой, а мобильные платежи, являющиеся ключевой составляющей мобильных финансовых услуг, набирают обороты во всем мире. Но вместе с тем растет риск быть обманутыми злоумышленниками и потерять денежные средства при использовании системы мобильных платежей.

Актуальность данной темы заключается в том, что различные компании предлагают своим пользователям, для удобства, всегда иметь возможность для оплаты товаров и услуг посредством своего мобильного телефона, но так как процесс оплаты упрощён, существуют множество угроз и уязвимостей системы мобильных платежей.

Мобильные платежи - альтернативный метод оплаты, в котором в качестве средства совершения платежа (платежной карты, чека, наличных) выступает мобильное устройство.

Под мобильными платежами понимают самые разные виды платежных решений. В целом, к мобильным платежам можно отнести электронные платежи с использованием мобильных устройств для получения и передачи информации и для совершения денежных

транзакций. Другими словами, это все те способы, которые позволяют осуществлять оплату за товары и услуги, и перевод денежных средств с помощью мобильных устройств.

С мобильными приложениями оплата проходит в разы быстрее, что удобно и предпринимателям, и их клиентам. Теперь нет необходимости выписывать чеки и отправлять их по почте, не надо отправлять счета клиентам и тратить деньги на конверты и услуги почты. Потому что в нашу жизнь пришел смартфон!

Подключившись к интернету, пользователи могут посещать веб-сайты и использовать онлайн приложения к телефону с целью приобретения товаров или услуг. Стоимость покупки можно включить в счет, выставляемый мобильным оператором, или оплатить, зарегистрировавшись в международной платежной системе.

Система мобильных платежей позволяет пользователям осуществлять прием платежей с использованием мобильных телефонов клиентов. Удобство и гибкие условия оплаты способствуют неизменному росту числа пользователей мобильных платежей во всем мире.

Стандарт PA-DSS (Payment Application Data Security Standard) является, с одной стороны, развитием предписания Visa PABP (Payment Application Best Practices), а с другой стороны, адаптацией требований стандарта PCI DSS к приложениям. Требования стандарта PA-DSS распространяются на приложения, обрабатывающие данные о держателях карт на этапе авторизации транзакции. При этом есть исключение – требования PA-DSS не распространяются на приложения собственной разработки и приложения, разработанные на заказ для одного единственного потребителя. Все платежные приложения, выпускающиеся на рынок, должны проходить сертификацию по стандарту PA-DSS, которую могут выполнить только компании, обладающие статусом PA-QSA. Международные платежные системы предписывают торгово-сервисным предприятиям и поставщикам услуг использовать только сертифицированные по стандарту PA-DSS приложения, перечень которых опубликован и регулярно обновляется Советом PCI SSC.

Учитывая важность требований безопасности к платежным приложениям с одной стороны, и совместимость этих приложений с требованиями стандарта PCI DSS с другой стороны, советом PCI SSC был разработан стандарт PA-DSS. Стандарт призван обеспечить

безопасность приложений и совместимость с требованиями PCI-DSS и перенести ответственность за это на производителей программного обеспечения, у которых до этого момента руки были развязаны.

Преимущества использования, сертифицированных по PA-DSS приложений компаниями, попадающим под действие стандарта PCI DSS очевидны. Во-первых, они так же получают возможность оставаться на рынке после начала даты действия стандарта, во-вторых, компания уменьшает количество необходимых для выполнения требований PCI DSS, перенося их на разработчика приложений и сокращая расходы на соответствие PCI DSS, в-третьих, компания получает руководство по безопасному внедрению (Implementation Guide), которое также помогает привести систему в соответствие стандарту PCI DSS и, наконец, в-четвертых, что наиболее важно – они получают безопасное приложение, тем самым существенно уменьшая риск компрометации данных.

Причем следует отметить, что эта безопасность не формальна. За ней стоит реальный аудит безопасности с применением общепризнанных методик, таких как OWASP и WASC на наличие программных уязвимостей.

Можно выделить следующие проблемы безопасности [1-11]:

- активные атаки — злоумышленник исполняет роль сетевого элемента;
- небезопасная передача ключевой информации: аутентификационные данные передаются в явном виде внутри и между сетями;
- односторонняя аутентификация: обеспечивается только аутентификация пользователя для сети, нет средств аутентификации сети для пользователя;
- слабые алгоритмы шифрования. Длина ключа слишком мала, в то время как скорости вычислений растут.

Аудит на наличие программных уязвимостей – это далеко не только статический анализ кода стандартными утилитами на наличие типовых строк, таких как strcpy, указывающих на возможное наличие уязвимости переполнения буфера, и не только blackbox fuzzing с использованием типовых программных средств, это еще и глубокий интеллектуальный анализ бизнес-логики приложения и поиск соответствующих уязвимостей в процессе реальной работы приложения. Как следует из опыта DSecRG по анализу защищенности бизнес-приложений, значительная доля уязвимостей

относится именно к классу логических ошибок, которые не обнаруживаются стандартными утилитами, что также подтверждается известными западными компаниями в их отчетах.

В списке TOP 10 уязвимостей, составленном компанией Cenzic (производитель сканера для поиска уязвимостей в WEB-приложениях), на 2 месте (22% уязвимостей) находятся логические уязвимости, связанные с контролем доступа, а в аналогичном списке компании Trustwave логические ошибки занимают второе место, а третье и четвертое принадлежит ошибкам авторизации и аутентификации. Для поиска ошибок такого класса в отличие от переполнений буфера и различных инъекций кода, не существует программных средств, полностью автоматизирующих данный процесс, поэтому уповать можно только на опыт конкретного эксперта в области анализа защищенности приложений.

Клиентское ПО для ОС Android (рис.1) более уязвимо по сравнению с приложениями для iOS. В частности, критически опасные уязвимости содержатся в 70% приложений для Android и в 50% приложений для iOS.

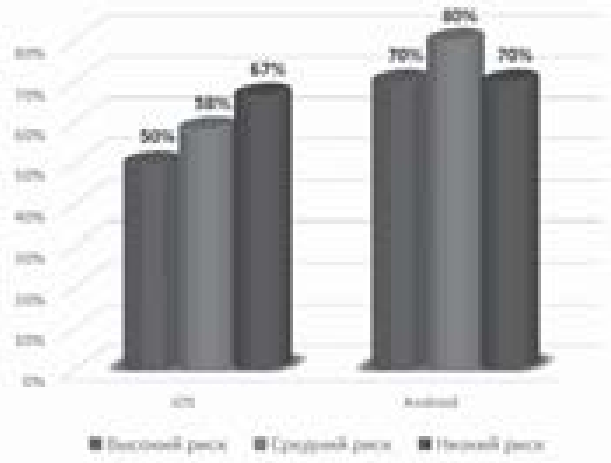


Рисунок 1 – Доли клиентских мобильных программ, подверженных уязвимостям

Наиболее часто в мобильных системах встречались уязвимости, связанные с небезопасной передачей данных (73%), далее идут недостаточная защита сессий (55%) и небезопасное хранение данных в мобильном приложении (41%) (рис. 2).

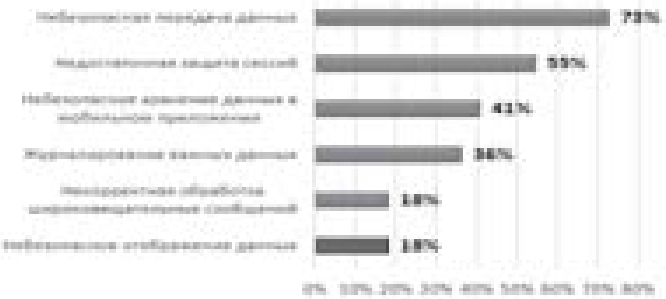


Рисунок 2–Наиболее распространенные уязвимости клиентского ПО мобильных систем

Хотя наиболее распространенные уязвимости мобильных систем имеют среднюю или низкую степень риска, в ряде случаев совокупность выявленных недостатков позволяла реализовать серьезные угрозы безопасности. Например, одно из исследованных приложений отправляло широковещательное сообщение, содержащее полученное от банка SMS-сообщение (с одноразовым паролем для проведения транзакции), которое могло быть перехвачено сторонним приложением. Кроме того, данное мобильное приложение осуществляло журналирование важных данных, таких как учетная запись пользователя, вследствие чего при успешном заражении устройства пользователя вредоносным кодом атакующий мог получить полный доступ к аутентификационным данным и проводить транзакции от лица пользователя мобильного приложения.

Компания «Инфосистемы Джет» представила собственную аналитику по уязвимостям мобильных банковских приложений (рис.3), действующих под управлением iOS, Android и Windows Phone: 98% исследованных приложений имеют уязвимости и более 40% из них обладают критичными уязвимостями.

Отчет основан на данных, полученных экспертами компании в ходе обследования 58 банковских приложений. Был проведен статический и динамический анализ исходного кода приложений. Эксперты компании «Инфосистемы Джет» оценили уровень безопасности межсетевого взаимодействия между мобильным приложением и web-сервисом и настройки защищенного соединения web-сервиса.

Выявленные по результатам тестирования уязвимости проранжированы по степени их критичности. Операционные системы

Оценены с точки зрения распределения между ними числа уязвимых приложений. Кроме того, составлен рейтинг обнаруженных уязвимостей. В данной статье рассмотрен список уязвимостей, которые могут нанести ущерб безопасности, созданным приложениям. Соответственно, данный список дает возможность при реализации системы мобильных платежей предотвратить несанкционированный доступ к конфиденциальной информации посредством устранения перечисленных уязвимостей. Для этого необходимо осуществлять аудит кода, анализ защищенности приложения, тестирование на проникновение.

Рисунок 3–Уязвимости мобильных банковских приложений

Подводя итоги анализа, следует отметить необходимость создания комплекса мероприятий по разработке мер для защиты и устранения уязвимости при использовании незащищенных протоколов передачи информации.

Литература

1. Белов Е.Б, Лось В.П. и др., Основы информационной безопасности. М.: Горячая линия - Телеком, 2006. — 544 с.

2. Соляной В.Н., Сухотерин А.И Выработка коммуникативной компетенции при подготовке профессионалов по информационной безопасности с использованием технологии модерации. «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7
3. Соляной В.Н., Сухотерин А.И, Антоненко В.И. Проблемно-ориентированная подготовка специалистов по информационной безопасности с использованием имитационного метода (мозговой штурм). «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7.
4. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
5. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
6. Фомичев В.М., Малюк А.А., Горбатов В.С., Королёв В.И., Дураковский А.П., Кондратьева Т.А., Введение в информационную безопасность. М.: Горячая линя - Телеком, 2011. — 288 с.
7. Безопасность приложений. Аналитический отчёт IBM X-Force// Режим доступа: www.ibm.com/software/products/ru/category/application-security

8. Анализ защищенности мобильных приложений (клиентская часть). Аналитический отчёт компании Digital Security// Режим доступа: www.dsec.ru/services/security-analysis/mobile-applications
9. Миноженко Александр. Безопасность мобильных банковских приложений//Режим доступа: www.itsec.ru/articles2/25kadr/bezopasnost-mobilnyh-bankovskih-prilozheniy.
10. Главные уязвимости онлайн-банков: авторизация, аутентификация и Android // Режим доступа: www.pcidss.ru/articles/226.html
11. 98% мобильных банковских приложений имеют уязвимости//Режим доступа: www.plusworld.ru/daily/98-mobilnih-bankovskih-prilojeniy-imeut-uyazvimosti/

ОБМАННЫЕ СИСТЕМЫ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ В КОМПЬЮТЕРНЫХ СЕТЯХ

Молошенко Павел Максимович, студент 1 курса кафедры Информационной безопасности
Научный руководитель: **Соляной Владимир Николаевич**, к.воен.н., доцент, заведующий кафедрой Информационной безопасности

Одними из перспективных механизмов, дополняющих существующие механизмы защиты информационных ресурсов в компьютерных сетях, являются механизмы введения в заблуждение (обмана) нарушителей информационной безопасности. Эти механизмы предназначены для повышения защищенности целевых информационных систем за счет привлечения злоумышленников к ложным информационным целям, введения в заблуждение, идентификации их действий и разоблачения. Механизмы введения в заблуждение нарушителей реализуются посредством разработки и использования обманных систем (ОбС) или компонентов, называемых также ложными информационными системами, имитаторами информационных систем или ловушками.

Информационная безопасность, обманные системы, создание систем, ложные системы.

DECEPTION SYSTEMS FOR PROTECTION OF INFORMATION RESOURCES IN COMPUTER NETWORKS

Malashenko Pavel, 1st year student of the Department of information security
Scientific adviser: **Solaynoy Vladimir**, Candidate of Military Sciences, Associate Professor, Head of the Department of information security

Ones of the perspective mechanisms supplementing existing mechanisms of information resources protection in computer networks are malefactors' deception mechanisms. These mechanisms are intended for increasing the security of target information systems on the base of attraction of malefactors to false information goals, deceptions, identification of their actions and disclosure. Malefactors' deception mechanisms are realized by means of development and usage of deception systems (DS) or components named also false information systems, simulators of information systems, traps or honeypots.

Information security, deception systems, building systems, false system.

В настоящее время все более актуальной становится задача защиты информационных ресурсов компьютерных сетей от атак со стороны внешних и внутренних нарушителей. Для решения данной задачи необходимо не только предупреждать, блокировать, обнаруживать и реагировать на действия нарушителей, но и отвлекать их от основных целей, заманивая на ложные информационные объекты, производить сбор информации о приемах, тактике и мотивации злоумышленников, осуществлять их идентификацию и разоблачение.

Для выполнения этих подзадач могут быть использованы обманные системы (ОбС), называемые также ложными информационными системами, имитаторами информационных систем или системами-ловушками.

Основными функциями таких систем являются привлечение и удержание внимания злоумышленников на ложных информационных целях, введение злоумышленников в заблуждение, обнаружение и фиксация действий нарушителей, их контроль, а также сбор и агрегация данных о действиях нарушителей из различных источников. ОбС представляют собой программно-аппаратные средства обеспечения информационной безопасности, реализующие функции сокрытия и камуфляжа защищаемых информационных

ресурсов, а также дезинформации нарушителей. С помощью фиксации и сбора данных, межсетевого экранирования, обнаружения вторжений и обмана нарушителей (на основе имитации ложных целей, уязвимых для нападения), а также других механизмов эти системы позволяют в реальном времени выявлять атаки, направлять их по ложному следу, ограничивать их распространение, идентифицировать нарушителей, исследовать их действия и определять намерения.

В статье определены место и роль механизма введения в заблуждение нарушителя, рассмотрено состояние исследований в данной области, представлен подход к построению ОбС, охарактеризованы функции и структура перспективной ОбС, дано представление о реализуемых схемах функционирования ОбС.

Рассмотрим последовательность фаз реализации атаки на компьютерную сеть, отражаемых через жизненный цикл инцидента безопасности, и механизмы защиты информации, необходимые для реализации на каждой фазе выполнения атаки. Данные механизмы защиты и фазы жизненного цикла инцидента безопасности представлены на рис. 1. Основными фазами жизненного цикла любого инцидента безопасности являются: (1) предупреждение угрозы безопасности, (2) реализация угрозы и возникновение инцидента, (3) нанесение ущерба и (4) восстановление ресурсов защищаемой системы после нанесения ущерба.

Рисунок 1 - Цикл инцидента безопасности

Основными видами угроз являются угрозы конфиденциальности, целостности и доступности. Угрозы конфиденциальности направлены на разглашение информации, т.е. в результате реализации этих угроз информация становится известной лицу, которое не должно иметь к ней доступа. Для обозначения этого явления используется термин “несанкционированный доступ” (НСД), под которым понимается доступ к информации, нарушающий установленные правила разграничения доступа. Угрозы целостности

представляют собой любое искажение или изменение неуполномоченным на это действие лицом хранящейся в вычислительной системе или передаваемой информации. Целостность информации может быть нарушена как злоумышленником, так и в результате объективных (неумышленных) воздействий со стороны среды эксплуатации системы. Можно выделить следующие группы механизмов защиты, реализуемых на различных фазах жизненного цикла инцидента безопасности (рис.1.): (1) предупреждение, (2) ослабление, (3) введение в заблуждение (обман) нарушителя, (4) обнаружение, (5) реагирование, (6) нейтрализация и устранение последствий и (7) оценивание инцидента и принятых мер.

По своему назначению выделим два класса информационных систем (ИС): целевые ИС, предназначенные для автоматизации необходимых функций организации, и ложные ИС (ОбС), служащие для имитации целевых ИС с целью введения в заблуждение (обмана) нарушителей и отвлечения их внимания от информационных ресурсов целевых ИС. ОбС предназначены для:

- ограничение атак на целевые системы за счет отпугивания нарушителя и “принятия огня на себя”
- скрытное обнаружение (отслеживание) и исследование (оперативный анализ) атак и неавторизованной активности
- мониторинг случаев несанкционированного доступа к системе и ее использования не по назначению;
- реагирование на действия нарушителя с целью введения его в заблуждение.

ОбС могут обеспечить повышение безопасности ИС напрямую или косвенно. Непосредственное влияние ОбС на защищенность проявляется в усилении общей архитектуры защиты и конкретных механизмов защиты за счет перенесения внимания нарушителей с компонентов целевой системы на компоненты ложной, задействования межсетевого экранирования, обнаружения вторжений, реализации более эффективных механизмов реагирования на действия нарушителя и др. Косвенное влияние проявляется в раскрытии стратегий, средств и действий нарушителей для последующего усиления защитных механизмов. ОбС должны строиться таким образом, чтобы атака на них была наиболее привлекательна по тем или иным причинам для злоумышленника (наименее защищенная часть системы или кажущаяся

привлекательность по информативности). По назначению выделяют два основных типа ОбС — "производственные" и исследовательские. Производственные ОбС применяются для защиты ресурсов отдельных компьютеров и компьютерных сетей, в том числе снижения риска их компрометации. Как правило, данные ОбС легче реализовать, так как они обладают меньшей функциональностью, чем исследовательские ОбС. Исследовательские ОбС применяются для изучения действий нарушителей, используемых ими стратегий и средств с целью построения более эффективных механизмов защиты. ОбС данного типа характеризуются гораздо более высоким уровнем взаимодействия с нарушителем, чем производственные. Это позволяет получать больше информации о нарушителях. Однако более высокая функциональность приводит к большим затратам на их сопровождение и к большему риску их компрометации и использования против других систем. Фактически ОбС данного типа могут существенно снизить защищенность АС, в которых они развернуты. Следует отметить, что различие между производственными и исследовательскими ОбС не является принципиальным. По уровню взаимодействия с нарушителем различают следующие типы ОбС (табл. 1.).

Таблица 1 - Характеристика ОбС по уровню взаимодействия

Уровень взаимодействия	Трудоемкость установки и конфигурирования	Трудоемкость развертывания и поддержки	Возможности по сбору информации	Уровень риска
Низкий	Низкая	Низкая	Ограниченные	Низкий
Средний	Средняя	Средняя	Ограниченные	Средний
Высокий	Высокая	Высокая	Значительные	Высокий

ОбС базируются на сборе данных небольшого объема, так как они ориентированы на фиксацию только действий нарушителей и любое взаимодействие с ОбС, вероятнее всего, вызвано неправомочными или злонамеренными действиями. ОбС требуют минимальных ресурсов, так как они используют данные, характеризующие только неправомочные или злонамеренные действия; все типы ОбС основываются на простой стратегии — если кто-то взаимодействует с ОбС, отслеживай его действия и реагируй на них. Понятно, что чем проще компонент защиты, тем менее вероятны ошибки функционирования и сбои в работе.

ОбС позволяют непрерывно демонстрировать руководству организаций свою значимость, а также подтверждать роль других механизмов защиты. Всякий раз, когда на компоненты ОбС

осуществляется атака, администраторы безопасности и руководство будут проинформированы об этом.

В качестве основных недостатков использования ОбС отметим следующие:

- ОбС имеют ограниченную область применения, так как могут отслеживать только деятельность, которая непосредственно направлена на них;
- ОбС не могут обнаруживать и реагировать на деятельность против других систем, если нарушитель не взаимодействует с ОбС;
- наличие у ОбС “демаскирующих признаков”, т.е. отличительных характеристик и поведения, обнаруживаемых нарушителем по ответной реакции ОбС на его действия.

Наличие данного недостатка может привести к тому, что нарушитель, в свою очередь, попытается обмануть систему защиты для реализации своей цели. Например, если нарушитель идентифицировал использование ОбС, он может атаковать ее от имени реального компьютера целевой системы. ОбС обнаружит эту атаку и ошибочно оповестит администратора о том, что целевая система была использована злоумышленником, порождая цепочку разбирательств, ведущих по ложному следу, а в это время нарушитель сможет сосредоточиться на реальных целях.

Однако, в силу представленных выше причин, представляется, что в большинстве случаев более разумно, чтобы ОбС действовали скрытно и не были обнаружены.

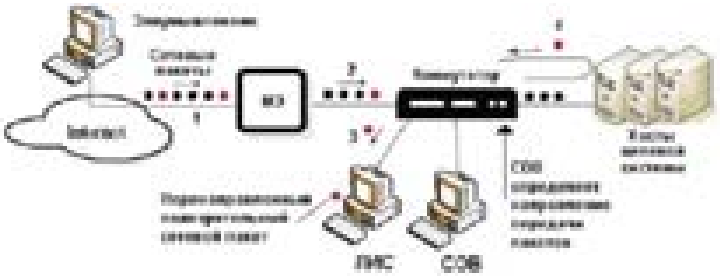
В настоящее время исследования в области построения ОбС — одно из наиболее бурно развивающихся направлений в защите информации. Исследования в области ОбС были инициированы с начала 1990-х годов. Одной из первых работ по использованию механизмов обмана для защиты информационных систем была работа Била Чеквика (Bill Cheswick) .В ней раскрывались сценарии трассировки в реальном времени действий нарушителя на основе механизмов введения нарушителя в заблуждение. С этого момента началось детальное и тщательное изучение данного метода защиты информации.

В наше время наиболее продвинутым интернациональным проектом в области создания ОбС является Honeynet Project. Honeynet Project — это научная организация, занимающаяся исследованиями в области защиты информации и

специализирующаяся на изучении инструментария, используемого злоумышленниками, их тактики и мотивов.

В состав организации входят специалисты по вопросам безопасности из разных стран, которые на добровольной основе предоставляют свои ресурсы для развертывания и изучения сетей-приманок, основное назначение которых — стать объектом атаки хакеров.

В настоящее время существует множество коммерческих и свободно распространяемых ОбС. Они различаются уровнем имитации реальных систем, количеством поддерживаемых протоколов, конструкцией, условиями распространения и т.п. Часть ОбС могут эмулировать только некоторые сервисы или уязвимости, причем на том компьютере, на котором они запущены. Примерами таких систем являются Decoy-режим RealSecure Server Sensor, WinDog-DTK или система The Deception Toolkit (DTK). Более развитые системы эмулируют не отдельные сервисы, а сразу целые компьютеры и даже сегменты, содержащие виртуальные узлы, функционирующие под управлением разных ОС. Примеры таких систем — CyberCop Sting или Honeyd.



Условные обозначения:
1 - сетевые пакеты;
2 - межсетевой экран;
3 - компоненты обманной системы;
4 – хосты целевой системы

Рисунок 2 - Место компонентов обманной системы в компьютерной сети

В настоящем разделе сформулированы теоретические положения по созданию перспективной производственной ОбС, прототип которой разрабатывается в лаборатории интеллектуальных систем СПИИРАН. Место компонентов данной ОбС в компьютерной сети представлено на рис. 2. Предполагается, что поступающие из сети Интернет сетевые пакеты (1) вначале проходят предварительную

фильтрацию посредством межсетевого экрана (МЭ) (2), затем анализируются на предмет наличия атак системой обнаружения вторжений (СОВ), если пакет отнесен СОВ к категории подозрительных или обнаружена явная атака, он перенаправляется на компоненты ОбС (3).

Если СОВ не удалось обнаружить атаку на сетевом уровне, но злоумышленные действия были выявлены СОВ после их реализации на хостах целевой системы (4), осуществляется перенаправление последующих пакетов злоумышленника на компоненты ОбС.

В качестве основных функций, которые должны быть реализованы в перспективной ОбС, на основании анализа исследований в указанной области выделим следующие:

- захват данных (“прослушивание” сетевого трафика и фиксация данных для последующего анализа);
- сбор и объединение данных от различных программных и аппаратных компонентов компьютерной сети, в частности, сенсоров, МЭ, СОВ, маршрутизаторов и др.;
- определение “свой-чужой” и переадресация несанкционированных запросов на компоненты ОбС;
- фильтрация событий (для автоматической отбраковки несущественных и фокусировки на значимых событиях);
- обнаружение вторжений (атак);
- выявление источника угроз, трассировка и идентификация нарушителя (определение типа, квалификации и др.);
- распознавание плана (стратегии) действий нарушителя;
- контроль действий нарушителя и реагирование на них, в том числе оповещение администратора о компрометации, блокирование действий нарушителя и др.;
- формирование плана действий компонентов ОбС по имитации целевой информационной системы;
- заманивание и обман нарушителя (привлечение внимания, сокрытие реальной структуры защищаемой системы и ресурсов, камуфляж, дезинформация) за счет эмуляции сетевых сегментов, серверов, рабочихстанций, в том числе передаваемого трафика, и их уязвимостей, автоматическое реагирование на действия нарушителя, в том числе оповещние администратора;
- удаленное администрирование, документирование, ввод сигнатур, профилей и др. (обеспечивает централизованное

управление, основанную на правилах безопасности реакцию системы, подготовку отчетов и анализ тенденций);

- обеспечение интерфейса с администратором безопасности.

Обобщенная функциональная структура перспективной ОбС представлена на рис. 3. выделены базовые компоненты ОбС.

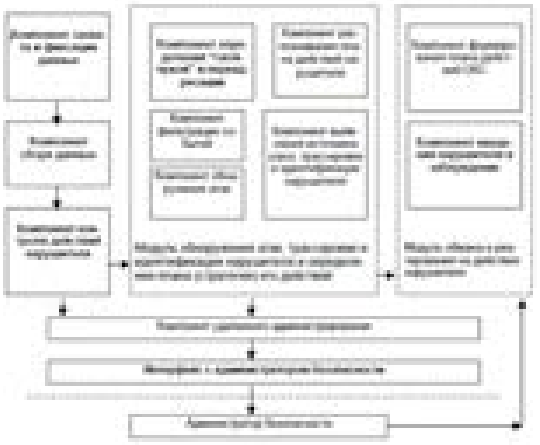


Рисунок 3 - Обобщённая функциональная структура обманной системы

Для реализации прототипа ОбС предложена следующая структура компьютерной сети, представленная на рис. 3.

Основные компоненты сети: (1) граничный хост, (2) персональные компьютеры (ПК) ЛВС, (3) демилитаризованная зона (ДМЗ) с расположенными в ней рабочими серверами, а также (4) подсеть с серверами, играющая роль сети-приманки.

Граничный хост выполняет следующие задачи: обеспечение безопасного доступа ПК ЛВС и рабочих серверов в публичную сеть Internet, блокировка запросов внешних пользователей к ПК ЛВС, ограничение исходящего сетевого трафика из сети-приманки, фильтрация и маршрутизация сетевого трафика, обнаружение вторжений на сетевом уровне, сбор с ПК всей сети данных из журналов регистрации событий.

Предполагается, что на жестких дисках ПК ЛВС никакой важной информации пользователи не хранят, а вся работа производится с данными, расположенными на серверах (например, могут использоваться так называемые “тонкие клиенты”). Любая

попытка произвести соединение из публичной сети Internet с ПК ЛВС блокируется граничным хостом.

В ДМЗ располагаются рабочие сервера, в частности web-сервер, ftp-сервер, mail-сервер (реализующий протоколы POP3 и SMTP) и telnet-сервер. В ДМЗ также развертывается хост-приманка, которая для пользователей представляется в качестве рабочего сервера. Все запросы, приходящие на данный хост, рассматриваются как носящие заведомо злоумышленный характер. Граничный хост должен обеспечивать маршрутизацию сетевых пакетов, идущих на хост-приманку, в сеть-приманку.

На рабочих серверах ряд приложений формируются следующим образом: целевой модуль сервиса вместе с модулем обмана вкладывается в обертку. В режиме санкционированного использования при вызове

сервиса управление передается целевому модулю. При обнаружении несанкционированного обращения управление передается модулю обмана.

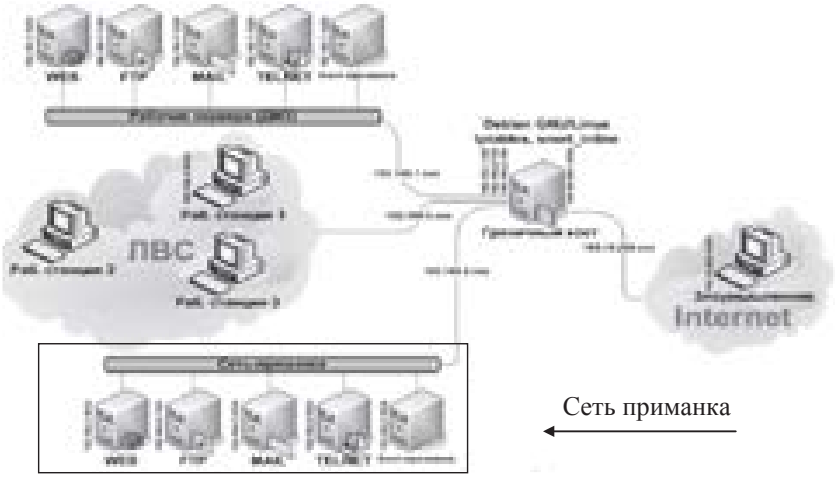


Рисунок 4 - Архитектура компьютерной сети с обманной системой

Серверы сети-приманки имитируют функции рабочих серверов. На этих серверах производится программная эмуляция работы сервисов и приложений web, ftp, mail и telnet. Хосты-приманки могут быть как системами с эмулируемыми сервисами, так и обычными незащищенными системами. Любая попытка произвести с сервера сети-приманки соединение с рабочим сервером или с ПК из ЛВС

должна блокироваться граничным хостом. Для обнаружения изменений в критически важных файлах на всех ПК сети используется система проверки целостности файлов.

ОбС обладает интерфейсом администратора, с использованием которого в реальном времени приводится анализ общего журнала регистрации событий и отражается сетевой трафик, проходящий через граничный хост.

Для реализации экспериментов на ПК, расположенном в публичной сети Internet, эмулируются действия злоумышленника. Каждый ПК, входящий в состав имитируемой компьютерной сети (см. рис. 4), может являться как физическим ПК, так и виртуальным. В последнем случае ПК должен эмулироваться с помощью различных программных средств.

Таблица 2 - Основные функции обманных систем

Функция	Программные средства
1. Замедление и сбивание нарушителя	Программы, эмулирующие работу сервисов (telnet, ftp, telnet и т.п.)
2. Обнаружение и фиксация действий нарушителя	Программные средства обнаружения вторжений и фиксации действий на сетевом уровне: snort_inline, winsbmp, tcpdump. Программные средства фиксации действий на уровне ОС: syslog.reg в качестве сервера (на граничном хосте) для захвата всех сообщений со всех ПК сети; eventlog to syslog для Windows в качестве клиента syslog.reg
3. Контроль действий нарушителя	Программный пакет Iptables на граничном хосте для ограничения исходящего из сети приманки трафика и для реализации функции маршрутизации
4. Сбор и агрегация данных о действиях нарушителей из различных источников	Программные компоненты фильтрации событий (из журналов регистрации событий ОС и из проходящих по сети пакетов), упорядочивания событий по шкале времени и представления данной информации администратору в удобочитаемом виде. Программные компоненты объединения данных (журналы регистрации событий со всех ПК сети объединяются в один общий журнал, расположенный на граничном хосте; сетевые пакеты записываются в текстовый файл программой tcpdump, winsbmp или snort)

В статье охарактеризовано текущее состояние в области исследований ОбС, представлен предлагаемый подход к построению перспективной производственной ОбС, рассмотрены архитектура прототипа этой системы. Рассматриваемый в статье подход основан на программной эмуляции компонентов информационных систем и на выделении трех уровней введения злоумышленников в заблуждение: (1) сегмента сети — производится эмулирование работы целого сегмента сети-приманки, дублирующего сегмент сети с рабочими серверами; (2) хоста — среди рабочих серверов используется хост-приманка; (3) сервисов и приложений — на отдельных серверах применяются программы, эмулирующие работу сервисов и приложений.

Направлениями дальнейших теоретических исследований является раз-работка и совершенствование моделей и алгоритмов

реализации функций ОбС, в частности, по выявлению источника угроз, трассировке и профилированию нарушителя, идентификации плана действий нарушителя, формированию плана действий компонентов ОбС по имитации целевой информационной системы, сокрытию реальной структуры защищаемой системы и дезинформации злоумышленника, а также состав обрабатываемых атак и реализуемых сценариев работы.

Литература

1. Cheswick B. An Evening with Berferd, 1991.
2. Cohen F. A Note On Distributed Coordinated Attacks // Computers and Security, 1996.
3. Cohen F. A Note on the Role of Deception in Information Protection // Computers and Security 1999.
4. Cohen F. Internet Holes - Internet Lightning Rods // Network Security Magazine, July, 1996.
5. Cohen F. Operating System Protection Through Program Evolution // Computers and Security.1992.
6. Cohen F., Lambert D., Preston C., Berry N., Stewart C., Thomas E. A Framework for Deception.
7. Honeynet Definitions, Requirements, and Standards. The Honeynet Project, 2003.
8. Intrusion Detection: Generics and State-of-the-Art. RTO TECHNICAL REPORT, № 49. 2002.
9. Spitzner L. Honeypots: Tracking Hackers. Addison Wesley, 2002.
10. Spitzner L. Know Your Enemy: Honeynets. The Honeynet Project, Jan 2003.
11. Котенко И. В., Степашкин М. В. Прототип ложной информационной системы // XI Российская научно-техническая конференция (по Северо-западному региону) “Методы и технические средства обеспечения безопасности информации”: Тезисы докладов. СПб.: Издательство СПбГПУ, 2003.
12. Лукацкий А. В. Обнаружение атак. СПб.: БХВ-Петербург, 2003.
13. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.

14. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Развитие сотрудничества российских и зарубежных ВУЗОВ по защите информационного ресурса. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» При поддержке Посольства Туркменистана в Российской Федерации. Текст Сборник материалов III Ежегодная международная научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
15. Спитцнер Л. Honeynet Project: ловушка для хакеров // Открытые системы, № 07–08, 2003.
16. Spitzner L. Honeypots: Definitions and Values. May 2003. http://www.trackinghackers.com/papers/honeypots.html

МНОГОУРОВНЕВАЯ ИДЕНТИФИКАЦИЯ БЕСПРОВОДНЫХ СЕТЕЙ

Музяков Егор Сергеевич, студент 4 курса кафедры Информационной безопасности
Научный руководитель: **Соляной Владимир Николаевич**, к.воен.н., доцент, заведующий кафедрой Информационной безопасности

Как правило, процедура развертывания беспроводной сети подразумевает ряд мероприятий, направленных на обеспечение безопасности итоговой инфраструктуры. Однако трудность состоит в том, что лишь иногда "ряд" подразумевает действительно внедрение продуманной политики безопасности, зачастую, к сожалению, для этого не делается вообще ничего.

Конечно же, беспроводные технологии - это действительно очень удобно. И популярность данного вида связи растет радующими глаз темпами. Но, как давно замечено, популярность чего-либо в сфере компьютерных технологий практически стопроцентно вызывает нездоровый интерес различных "криминальных элементов от IT". Тут бы и задуматься о безопасности всерьез - ведь порой и стандартные средства могут оказаться бессильны.

Информационная безопасность, MAC-адреса, WEP-шифрование.

MULTI-LEVEL IDENTIFICATION OF WIRELESS NETWORKS

Muzyakov Egor, 4rd year student of the Department of information security
Scientific adviser: **Solaynoy Vladimir**, Candidate of Military Sciences, Associate Professor, Head of the Department of information security

Typically, the procedure involves the deployment of a wireless network a number of measures aimed at ensuring the safety of the final infrastructure. However, the difficulty lies in the fact that only sometimes "number" refers to the introduction of truly elaborate security policy is often, unfortunately, it does not do anything at all.

Of course, wireless technology - it's really very convenient. And the popularity of this type of communication is growing rapidly aesthetically pleasing. But, as has long been noted, the popularity of anything in the area of computer technology is almost completely unhealthy interest in the various "criminal elements from IT". There would have to think about security seriously - because sometimes the standard tools may be powerless.

Information security, MAC-addresses, WEP-encryption.

Ощущение изначальной уязвимости беспроводных сетей появляется после простейших размышлений. В чем состоит отличие проводной сети от беспроводной? В общем случае проводная сеть, при условии идеальной и бесспорной порядочности ее пользователей, может быть атакована лишь из Интернета - если подключена к Сети. Беспроводная же открыта всем, и помимо вторжений из Интернета ей как минимум угрожает попытка "прощупывания" со стороны коллег из соседнего офиса или с нижнего этажа. А это уже немаловажно - подобные действия способны не только принести удовлетворение от созерцания беспроводной сети, но и найти пути, чтобы в нее проникнуть. Соответственно, если безопасности не уделяется должного внимания, такую сеть вполне можно считать публичной, что неизбежно отразится на ее функционировании не лучшим образом.

Попытки проникновения в корпоративную закрытую сеть могут происходить по нескольким причинам [1-8]. Во-первых, целенаправленный взлом с целью похищения конфиденциальной информации. Чаще всего именно из-за этого необходимо позаботиться о безопасности беспроводного сегмента сети, хотя на

самом деле процент таких взломов достаточно невелик. Гораздо большей популярностью пользуются попытки проникнуть в сеть, чтобы воспользоваться чужим интернет-соединением.

В данном случае также происходит воровство, но не осязаемых конфиденциальных документов, а виртуальное - воровство интернет-трафика. Если злоумышленник пользуется чужим интернет-каналом для сугубо утилитарных целей (электронная почта, веб-серфинг), то ощутимого материального урона он не нанесет, но если локальная сеть организации используется как плацдарм для рассылки спама или последующей масштабной интернет-атаки - последствия могут быть крайне неприятными как со стороны интернет-провайдера, так и со стороны контролирующих органов.

Каковы же наиболее популярные средства защиты беспроводных сетей из тех, что предоставляют производители данного оборудования? Их три:

1. Разграничение доступа, основанное на MAC-аутентификации.
2. Запрет широковещательной передачи идентификатора SSID.
3. 64- и 128-битное WEP-шифрование трафика.

Принято считать, что разграничение доступа, основанное на разделении аппаратных MAC-адресов (рис. 1) беспроводных сетевых адаптеров на "своих" и "чужих", является эффективным средством противодействия атакам. Это действительно так, но лишь при обеспечении дополнительных мер безопасности.

Рисунок 1 - Мас-адрес

Кстати, аутентификация беспроводного клиента по MAC-адресу - исключительно инициатива конкретного производителя,

спецификации беспроводных стандартов 802.11b/g такой меры безопасности не предусматривают. То есть подобный метод аутентификации может либо присутствовать, либо нет, - в зависимости от желания и маркетинговой политики производителя.

Даже если существует возможность "отсеивания" чужих беспроводных клиентов, полностью полагаться на эту меру не стоит - ее взлом занимает считанные минуты и доступен даже начинающему хакеру с неоконченным средним образованием.

Суть взлома такова: при помощи специальной утилиты прослушивается радиообмен точки доступа на канале, по которому происходит обмен информацией с клиентами, и в полученном трафике выделяется список "своих" клиентов. Затем остается лишь программно подменить аппаратный адрес своего беспроводного адаптера на один из списка валидных адресов (в подавляющем большинстве случаев это можно сделать даже стандартными средствами драйвера) - и "чужой" адаптер стал "своим".

SSID - своего рода имя беспроводной сети, знание этого идентификатора является необходимым условием для подключения. Если, скажем, инфраструктура сети компании подразумевает наличие пяти точек доступа, то каждой точке можно либо назначить уникальный идентификатор SSID (причем образуется пять "логических" сетей), либо организовать работу точек в режиме повторения для наиболее полного покрытия одной логической сетью - хотя, конечно, возможны различные вариации. Так или иначе, для подключения к беспроводному сегменту сети этот идентификатор надо знать.

SSID может широко транслироваться в эфир (широковещательная передача) или быть "скрытым" - в таком случае клиенту придется в настройках своего подключения прописать идентификатор вручную. Принято считать, что отключение широковещательной передачи SSID повышает степень безопасности беспроводной сети, впрочем, данное утверждение весьма и весьма спорно.

В действительности же запрещение трансляции SSID (рис. 2) нисколько не способствует увеличению "атакоустойчивости". Такой шаг способен привести лишь к появлению потенциальных проблем у подключаемых клиентов, поскольку конфигурирование сети становится гораздо менее гибким. Отключение широковещательной передачи SSID создает иллюзию надежности: ведь значение этого

идентификатора все равно можно подслушать - оно находится во фреймах Probe Response. В любом случае беспроводная точка доступа - потенциальный источник угрозы, так как опытный пользователь, имеющий в арсенале ноутбук с беспроводным адаптером и необходимый минимум знаний, достаточно короткий срок может стать полноценным участником корпоративной сети со всеми вытекающими последствиями. Естественно, речь идет о преодолении стандартных препятствий, предусмотренных спецификациями стандартов 802.11b/g и инициативой производителя.

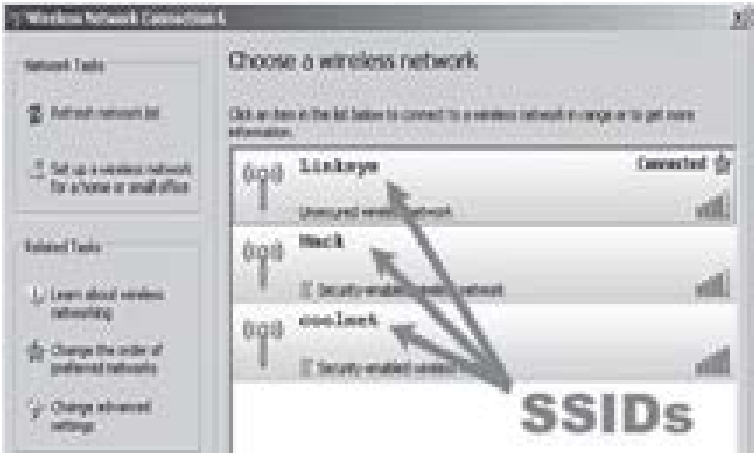


Рисунок 2 - Идентификатор SSID

Одной из наиболее действенных мер по защите беспроводной сети от несанкционированного вторжения принято считать WEP-шифрование трафика. WEP (Wired Equivalence Privacy) представляет собой статический ключ длиной 64 или 128 бит, при помощи которого шифруется вся информация между точкой доступа и беспроводными клиентами в случае Infrastructure-организации сети или между клиентами при Ad-Hoc-организации.

Шифрование базируется на алгоритме RC4. Правда, профессионалы от IT-безопасности не питают к нему особого доверия, поскольку он легко поддается взлому. Да и с WEP-шифрованием все далеко неоднозначно - и при 64-, и при 128-битном ключе имеет место некоторая условность. Дело в том, что эффективная длина ключа в первом случае составляет 40 бит, а во втором - 104 бит. Недостающие до заявленных служебные 24 бит используются для дешифрования информации на принимающей

стороне. Таким образом, числа "64" и "128" хороши лишь для пресс-релизов, а не для реальной безопасности. Кроме того, не будем забывать, что ключи являются статическими - а значит, их нужно периодически менять. Если для беспроводной сети, состоящей из точки доступа и трех клиентов, это не представляет особой проблемы, то для корпоративных сетей с сотнями беспроводных пользователей данное решение явно не подходит. Более того, для обеспечения достаточного уровня безопасности при использовании WEP-шифрования требуется смена 64-битного ключа раз в полчаса, а 128-битного - раз в час.

Однако это трудности, лежащие на поверхности. Какие же методы сегодня предпочитаются при взломе WEP? Прежде всего, анализ "подслушанного" трафика утилитами AirSnort и WEPCrack (поиск в Интернете при помощи www.google.com выдает домашние страницы обоих проектов в первой же строчке). Для того чтобы читатель реально представлял себе степень защиты (или беззащитности) беспроводной сети, приведем следующие цифры: при анализе беспроводного трафика на расшифровку 128-битного ключа (на самом деле он 104-битный) при помощи AirSnort уходит всего 2-4 часа.

На сегодняшний день разумными считаются два средства, дополняющие уже имеющиеся, - стандарты IEEE 802.1x, 802.11i и виртуальная частная сеть VPN.

IEEE 802.1x применяется для авторизации, аутентификации и аккаунтинга пользователей, чтобы проверить возможность предоставления доступа к сети. В случае 802.1x используются уже динамические ключи шифрования, что является несомненным плюсом. 802.1x предназначен для работы со сторонними средствами, такими как сервер.

Сервер - своего рода "проходная", вахтер на которой самостоятельно решает, пустить пользователя в сеть или нет. К чести некоторых производителей беспроводного доступа (например, D-Link и U.S. Robotics), возможность авторизации и аутентификации пользователя на сервере с помощью 802.1x предусмотрена даже в достаточно старых устройствах стандарта 802.11b.

Что следует в данном случае понимать под терминами "авторизация", "аутентификация" и "аккаунтинг"? Аутентификация - процесс определения тождественности пользователя, в наиболее общем виде - посредством имени ("логина") и пароля. Авторизация -

определение сетевых сервисов, доступных конкретному пользователю, и сервисов, к которым доступ запрещен. Наконец, аккаунтинг - журналирование использования сетевых ресурсов и сервисов.

В общем случае алгоритм привязки сервера к беспроводной сети представлен в рис. 3. и имеет следующие характеристики:

1. Сетевой администратор дает команду серверу завести новую учетную карточку пользователя с занесением в нее имени пользователя, под которым он будет проходить аутентификацию, и его пароля.

Рисунок 3 - Алгоритм привязки сервера к беспроводной сети

2. Внесенный в базу сервера пользователь с помощью беспроводной связи подключается к точке доступа, чтобы проверить электронную почту.

3. Точка доступа запрашивает у пользователя его имя и пароль.

4. Точка доступа связывается с сервером и дает запрос на аутентификацию пользователя.

5. Сервер находит валидные имя пользователя и пароль, дает добро на новую сессию и заводит в журнале соответствующую запись о начале новой сессии.

6. Точка доступа предоставляет пользователю возможность работать с теми сервисами, которые ему предписаны (это и есть авторизация).

7. По окончании сессии, которая может быть прервана либо самим пользователем, либо сервером (например, истек "нарезанный" по регламенту промежуток времени работы), сервер делает в журнале запись об окончании сеанса.

Как видим, процедура достаточно строгая, но в тоже время логически верная - хотя и относится лишь к управлению доступом.

В действительности построить хорошо защищенную сеть можно и при помощи уже имеющихся средств - даже несмотря на WEP, SSID broadcasting и MAC-доступ. Хорошо зарекомендовавшее себя решение - Virtual Private Network, виртуальная частная сеть, в которую можно "завернуть" всю беспроводную сеть вместе с ее огрехами в области безопасности. Средства VPN работают на глобальном сетевом уровне, поэтому, видимо, в настоящее время это один из немногих способов обеспечения достойной безопасности.

Развертывание виртуальной частной сети поверх имеющейся беспроводной позволяет решить львиную долю проблем безопасности - на фоне VPN недостатки WEP, SSID и т. д. будут просто несущественны, так как особой практической ценности в данном случае они не имеют.

1) Проанализировав существующие средства защиты беспроводной сети, были выявлены недостатки MAC-адресов, SSID, WEP-шифрования.

2) Существующие недостатки в средствах защиты беспроводной сети, решаются внедрением специального сервера.

3) Для повышенной безопасности беспроводной сети рекомендуется развертывание VPN-виртуальной частной сети.

Литература

1. Ефимов А. К. Методика построения тестов проверки технологической безопасности инструментальных средств автоматизации программирования на основе их функциональных диаграмм / А. К. Ефимов Б. П. Пальчун, Л. М. Ухлинов // Вопросы защиты информации -1995. -№3(30). -С. 52-54.

2. Котенко И.В., Шоров А.В., Нестерук Ф.Г. Анализ биоинсперированных подходов для защиты компьютерных систем и сетей // Труды СПИИРАН - 2011

3. Сальников А. А. Новые факторы и безопасность в киберпространстве / А. А. Сальников Р. А. Шаряпов, В. В. Ященко // Вестник Московского университета. Серия политическая. // – 2010. -№ 2. -С. 71-84; -№ 3. -С. 90-103.
4. Скиба В. Ю. Парадигма проактивной безопасности компьютерных систем / В. Ю. Скиба // Защита информации. Инсайд. // -2009. -№ 5. -С. 2-9; М-6. -С. 2-7.
5. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
6. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Некоторые перспективы применения систем контроля и управления доступом в региональных ВУЗАХ. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
7. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Развитие сотрудничества российских и зарубежных ВУЗОВ по защите информационного ресурса. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
8. Ухлинов Л. М. Обеспечение безопасности информации в центрах управления полетами космических аппаратов. / Л. М. Ухлинов, М. П. Сычев, В. Ю. Скиба, О. Б. Казарип //- М.: Изд-во МГТУ им. Н.Э. Баумана -2000. - 366 с.

РЕКОМЕНДАЦИИ ПО СОЗДАНИЮ МЕХАНИЗМА РАЗРАБОТКИ ПОЛИТИКИ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНТЕРНЕТ-СИСТЕМАХ

Пахомов Дмитрий Анатольевич, Кравчени Максим Сергеевич,
студенты 3 курса кафедры Информационной безопасности
Научный руководитель: **Сухотерин Александр Иванович**, к.воен.н.,
доцент кафедры Информационной безопасности

Благодаря развитию информационного общества, многие процессы постепенно переходят в Интернет-сферу. Предоставление различных услуг требует обработку тех или иных персональных данных пользователей в Интернет-системах. С целью информирования пользователей о том, что происходит с их персональными данными, наше государство обязало операторов размещать Политику в отношении обработки персональных данных, процесс создания которой удалось автоматизировать для определенных категорий операторов.

Персональные данные, политика безопасности, информационная безопасность, организационно-правовые меры.

RECOMMENDATIONS FOR THE PERSONAL DATA SECURITY POLICY CREATION MECHANISM IN THE INTERNET SYSTEMS

Pakhomov Dmitry, Kravcheni Maxim, 3rd year students of the Department of information security
Scientific adviser: **Sukhoterin Alexander,** Candidate of Military Sciences, Associate Professor of the Department of information security

Due to development of information society, many of the processes are moving to the Internet. Providing various services requires the processing of certain users' personal data in the Internet systems. For the purpose of informing users about what happens to their personal data, our government is obliged operators to place the policy of personal data processing, the creation process of which could automate for certain categories of operators.

Personal data, security policy, information security, organizational and legal measures.

Персональные данные пронизывают почти все сферы деятельности общества. Любое действие, как поход в магазин, оплата услуг, заключение договоров может означать передачу персональных данных третьему лицу (оператору персональных данных). Тоже касается и Интернет-систем [2-5].

Для информирования субъектов персональных данных, в случае если сбор и обработка персональных данных производится посредством информационно-телекоммуникационной сети Интернет (далее – сеть Интернет), государство обязало операторов опубликовать в сети Интернет документ, определяющий политику в отношении обработки персональных данных и содержащий сведения о реализуемых требованиях к защите персональных данных (далее – Политика) [1, 2].

Оператором, обрабатывающем персональные данные могут быть и государственные органы, и муниципальные органы, а также юридические и физические лица [1].

Под Интернет-системой в данной работе понимается тот Интернет-ресурс, который ведет сбор и обработку персональных данных посредством сети Интернет.

Необходимость опубликования Политики существует лишь для тех Интернет-систем, которые собирают и обрабатывают те данные, которых необходимо и достаточно для идентификации субъекта персональных данных, например, как показано на рисунке 1 [1, 2].

Рисунок 1 - Перечень данных, при сборе которых необходима Политика на сайте

На рисунке 2 показаны данные, не являющиеся персональными. Для сбора и обработки таких данных у организаторов Интернет-систем отсутствует необходимость формирования Политики [2-5].

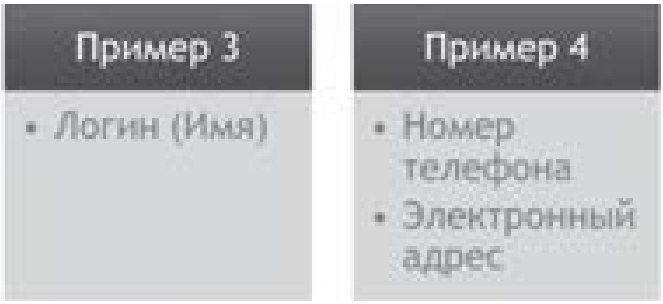


Рисунок 2 - Перечень данных, при сборе которых Политика на сайте необязательна

Необходимо также указать, что вопросы, касающиеся персональных данных, в организациях решаются специально назначенным ответственным. Сама Политика утверждается Руководством организации [1-5].

Следует отметить тот факт, что в малых и средних организациях, проводящих сбор и обработку персональных данных посредством сети Интернет, ввиду различных аспектов вполне может отсутствовать структура или даже специалист по информационной безопасности или защите персональных данных. Также администратором Интернет-системы может быть и физическое лицо. Кроме того, может возникнуть срочная необходимость составления данного документа, например, если владельцем Интернет-системы был получен запрос-требование о размещении Политики в общем доступе от государственных органов, в случае, если государственные органы решили, что собираемые Интернет-системой данные являются персональными [2-5].

Исходя из вышесказанного, формирование Политики – достаточно сложный и трудоемкий процесс для вышеупомянутых категорий операторов персональных данных.

Одним из методов решения вышеуказанной проблемы является автоматизация процесса формирования Политики. С этой целью нами был создан проект «ПДН16». «ПДН16» – программное обеспечение, автоматизирующее процесс создания политики в отношении обработки персональных данных.

Само программное обеспечение (веб-приложение) на данный момент расположено в сети Интернет по адресу: http://pdn16.azurewebsites.net/.

Основными потребителями являются малые и средние организации в таких сферах как интернет-предоставление услуг, здравоохранение, образование, администраторы сайтов (физические лица) и т.п.

Программа способна сформировать до 13 пунктов в том числе:

- Общие положения;
- Перечень нормативных правовых документов;
- Основные определения;
- Цели обработки персональных данных;
- Категории субъектов и перечень персональных данных;
- Принципы обработки персональных данных;
- Условия обработки персональных данных;
- Передача и обработка персональных данных;
- Применяемые меры по обеспечению безопасности персональных данных;
- Права и обязанности Организации;
- Права субъекта персональных данных;
- Порядок рассмотрения обращений субъектов персональных данных;
- Заключительные положения / Ответственность.

Вышеуказанные пункты были сформированы с использованием следующих источников:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Реестр операторов, осуществляющих обработку персональных данных (http://rkn.gov.ru/personal-data/register/);
- Политики Организаций, проверенных Роскомнадзором (http://rkn.gov.ru/plan-and-reports/);
- Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";
- Рекомендации по заполнению формы уведомления об обработке (намерении обработки) персональных данных (утв. 29.01.2016).

Следует отметить, что пункты Политики выбираются на усмотрение пользователя программы, и вовсе необязательно, что формируемая Политика будет содержать все 13 пунктов.

Интерфейс программы условно можно разделить три части. Прежде чем преступить к формированию проекта Политики, пользователю необходимо пройти процедуру регистрации. После прохождения данной процедуры, пользователь попадает в меню создания проекта (рисунок 3).

В этом меню пользователь может создать, выбрать существующий или скачать на своё устройство проект Политики. Сам проект Политики представляет из себя файл формата .doc.

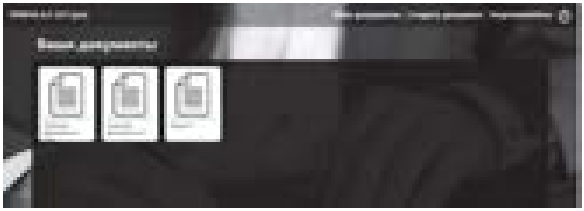


Рисунок 3 - Меню создания проекта Политики

После выбора существующего или создания нового проекта, пользователь попадает в меню формирования проекта, которое подразделяется на два варианта. В первом случае (рисунок 4), пользователю представляется окно ввода текста. При этом у пользователя есть возможность подстановки и редактирования заранее подготовленных шаблонов.

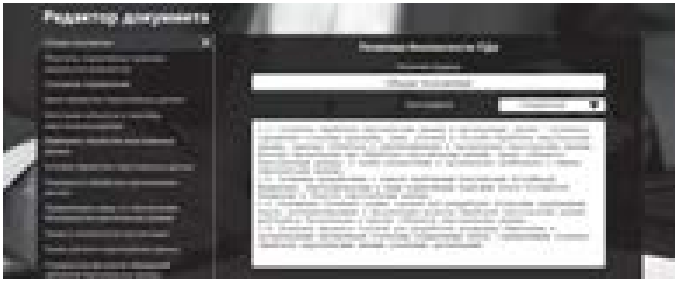


Рисунок 4 - Интерфейс ввода текста с использованием шаблонов

Другой вид интерфейса (рисунок 5, 6) представляет собой меню выборки подготовленных позиций, среди которых пользователь и должен выбрать подходящие для его Интернет-системы параметры. В случае если среди подготовленных не нашлось удовлетворяющих пользователя вариантов, то, благодаря реализованной возможности создания позиций в реальном времени, пользователь сам может дописать недостающую позицию.

Рисунок 5 - Меню выбора позиций, вариант 1

В конце процесса формирования Политики, пользователь имеет возможность скачать файл проекта и редактировать его любым текстовым редактором, работающим с форматом .doc, и оформлять проект по собственному желанию.

В дальнейшем пользователю остается лишь придать проекту Политики юридическую силу и опубликовать Политику на своём сайте. Данные действия от программного обеспечения уже не зависят.

Рисунок 6 - Меню выбора позиций, вариант 2

При создании самого веб-сервиса были использованы следующие технологии:

- HTML;
- CSS;
- JS;
- JQuery;
- C#;
- .net framework 4.6;
- .net core;

- ASP.NET 5;
- ASP.NET MVC 6;
- Identity 3;
- Entity Framework.
- Ajax

Благодаря использованным технологиям, а также возможности систематизации данных в области защиты персональных данных в дальнейшем планируется добавление в функционал программы создания других типов документов (соглашение об обработке, отзыв и т.п.) и создание автоматизированной системы формирования организационно-распорядительной документации в области персональных данных для Интернет-систем.

Литература

1. Соляной В.Н., Сухотерин А.И. Становление направления «Радиоэлектронная безопасность информационных объектов» в системе дополнительного профессионального по информационной безопасности. Научно-практический журнал №25, том 2 2015г. Информационное противодействие угрозам терроризма Материалы XIX Пленума учебно-методического объединения по образованию в области информационной безопасности «учебно-методическое обеспечение образовательных программ в области информационной безопасности» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН.ФЕД.УНИВ, 2015.-332 с. ISSN 2219-8792

2. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Некоторые перспективы применения систем контроля и управления доступом в региональных ВУЗАХ. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.

3. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Развитие сотрудничества российских и зарубежных ВУЗОВ по защите информационного ресурса. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов

III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
4. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
5. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
6. Соляной В.Н., Сухотерин А.И Выработка коммуникативной компетенции при подготовке профессионалов по информационной безопасности с использованием технологии модерации. «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7
7. Соляной В.Н., Сухотерин А.И, Антоненко В.И. Проблемно-ориентированная подготовка специалистов по информационной безопасности с использованием имитационного метода (мозговой штурм). «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7
8. О персональных данных [Текст]: Федеральный закон от 27 июля 2006 года № 152-ФЗ.
9. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. Отчет о деятельности Уполномоченного органа по защите прав субъектов персональных

данных за 2014 год [Электронный ресурс]: Режим доступа: http://rkn.gov.ru/docs/Otchet_ZPD_rus.pdf
10. Корпоративный менеджмент. Защита персональных данных [Электронный ресурс]: Режим доступа: http://www.cfin.ru/management/people/labor_law/private_info.shtml
11. Совит. Особенности создания политик информационной безопасности [Электронный ресурс]: Режим доступа: http://www.sovit.net/articles/methodics/security_policy/
12. Inside. Защита информации. Разработка политик информационной безопасности в организации [Информационно-методическое пособие] ООО «Издательский Дом «Афина».

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 4G-СЕТЕЙ

Руденко Константин Андреевич, Якушев Олег Вячеславович,
студенты 4 курса кафедры Информационной безопасности
Научный руководитель: **Сухотерин Александр Иванович**, к.воен.н., доцент, кафедры Информационной безопасности

Мобильные операторы активно рекламируют и распространяют дешёвую и быструю 4G-связь, однако о её защищённости известно мало. Раньше считалось, что переход на сети 4G повышает устойчивость телефона к атакам. Каждое поколение мобильной связи предполагало повышение безопасности. В 4G сетях, например, безопасность была усилена за счёт аутентификации и защиты ряда сигнатурных протоколов. На основе анализа материалов по исследованиям защищённости 4G-сетей в данной работе были выделены основные угрозы и предложения по их устранению.

Мобильные системы связи, мобильные сети, мобильные услуги, LTE, информационная безопасность.

ENSURING INFORMATION SECURITY 4G-NETWORKS

Rudenko Konstantin, Yakushev Oleg, 4rd year students of the Department of information security
Scientific adviser: **Sukhoterin Alexander,** Candidate of Military Sciences, Associate Professor of the Department of information security

Mobile operators are actively advertise and distribute cheap and fast 4G-communication, but on the security of its little known. Previously it was thought that the transition to 4G network increases the stability of the phone to the attacks. Each generation mobile communications expected to increase security. In 4G networks, for example, security has been strengthened at the expense of a number of authentication and security protocols signature. Based on the analysis of research materials security of 4G-networks in this study were identified the main threats and suggested remedies.

Mobile communication systems, mobile networks, mobile services, LTE, information security.

Оказывается, что LTE-сети выдают информацию о местоположении устройства, хотя даже во времена 2G приватность пользователя была в приоритете. Когда устройство подключается к сети, ему присваивается временный идентификатор (TMSI — Temporary Mobile Subscriber Identity). При обмене сигналами между сетью и устройством учитывается только TMSI, а не IMSI (International Mobile Subscriber Identity) или телефонный номер абонента. Таким образом, потенциальному атакующему будет труднее отследить конкретного пользователя, так как TMSI постоянно меняется при переподключении телефона к новой базовой станции [2].

Несколько лет назад корейские исследователи смогли отследить пользователя в сети 2G путем запросов page request — отправления пустых сообщений или совершения коротких звонков на номер абонента, но такая атака была маловероятна в реальных условиях [1].

Теперь же исследователи обнаружили подобный метод отсылки запросов через мессенджеры соц. сетей. Например, если пользователь Facebook вне списка друзей конкретного человека посылает ему сообщение, Facebook помещает сообщение в папку «Другие», дабы защитить пользователя от спама. Если на LTE-смартфоне установлен мессенджер Facebook, то потенциальный злоумышленник имеет возможность связать идентификатор TMSI с профилем в соц. сети через запрос page request.

Несмотря на «временную» природу идентификатора, TSMI меняется не так часто — например, в городах с большой плотностью населения идентификатор оставался неизменным до трех дней, и для

многих хакеров этого будет более чем достаточно, особенно если они используют «подставные» БС.

Протоколы доступа в сетях LTE используют некоторые алгоритмы отчетности, абсолютно необходимые для функционирования LTE, — например, для обеспечения устранения неисправностей при подключении к сети и переподключении абонента между сетями. Если атакующий получит доступ к одному из таких отчетов, которыми устройство обменивается с сетью, то потенциально сможет выявить местоположение смартфона — в некоторых случаях с точностью GPS-координат.

Также, эксперты обнаружили возможность проведения DDoS-атак по LTE. Например, в ситуации, когда абонент находится в роуминговой зоне, а тарифный план не позволяет пользоваться услугами в роуминге, при попытке подключения к сети смартфон получит сообщение вроде «ROAMING NOT ALLOWED». После этого следующий запрос к сети произойдет при перезагрузке устройства. Этот механизм разработан для того, чтобы сократить количество обращений к сети и сэкономить расход батареи. Таким образом, данная особенность LTE позволяет атакующему обеспечить «отказ в обслуживании» при подключении к 3G или 4G, вынудив устройство подключиться к менее защищенным сетям 2G, открытым для уже известных атак [2, 7-11].

Оборудование, необходимое для осуществления этих атак, состоит из платы USRP и нескольких антенн, снабженных открытым ПО openLTE. Весь пакет обойдется хакеру всего в тысячу евро.

Для устранения выявленных уязвимостей необходим пересмотр сигнатурных протоколов, а также программируемых сетей (SDN). Ряд производителей уже разрабатывают патчи, а также изменения существующих спецификаций LTE (4G-сетей) [5].

Цифровая мобильная связь стандарта GSM используется сейчас во многих критических инфраструктурах, включая промышленные системы управления (SCADA). Другой пример из повседневной жизни, с которым никому не хотелось бы встретиться – это кража денег с банковских счетов. Многие наверняка видели такие маленькие антенны у банкоматов (рис. 1) – здесь тоже GSM [1].

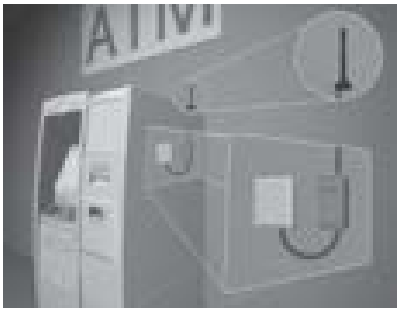


Рисунок 1 – Банковский автомат

Современный модем для беспроводной связи — это компьютер, на который установлена известная операционная система (обычно Linux или Android) и ряд специальных приложений с достаточно широким и возможностями. В этом программном обеспечении и протоколах передачи данных есть уязвимости, которые уже эксплуатировались в последние годы — например, чтобы разлочить модем и отвязать от оператора. Одним из средств защиты от таких взломов стал перенос многих сервисов на Web— однако это дало лишь новые возможности для атак [2].

Для идентификации оборудования нам необходимы документация и поисковая система. В некоторых случаях Google помогает даже больше – можно сразу найти пароль для telnet-доступа (рис. 2).

Рисунок 2 – Поиск информации

Однако для внешних коммуникаций нам нужен не telnet, а http. Подключаем модем к компьютеру и изучаем его, как отдельный сетевой узел с веб-приложениями. Находим возможность атаки через браузер (CSRF, XSS, RCE). Таким способом заставляем модем рассказать о себе разные полезные данные (рис. 3) и (рис. 4) [4].

Рисунок 3 – Полученные данные

Помимо раскрытия данных, на атакованном модеме можно выделить следующие уязвимости:

- Смена настойки DNS (что позволяет перехватывать трафик);
- Смена настройки SMS-центра (перехват SMS или манипулирование ими);
- Смена пароля на портале самообслуживания через SMS (что позволяет увести деньги со счета, подписавшись на сторонний сервис);
- Блокировка модема путём набора неверных PIN- и PUK-кодов;
- Удаленно «обновить» прошивку модема.

Рисунок 4 – Данные оборудования

Можно развить атаку и дальше — добраться до компьютера, к которому подключён USB-модем. Один из вариантов такой атаки: на захваченный модем устанавливается драйвер USB-клавиатуры, после чего компьютер воспринимает модем как устройство ввода. С этой «мнимой клавиатуры» на компьютер передаётся команда перезагрузки с внешнего диска, роль которого играет всё тот же модем. Таким образом, на «материнский» компьютер можно

установить bootkit, позволяющий дистанционно управлять компьютером.

Лучшее, что может сделать пользователь для защиты от подобных атак — не засовывать что попало в свои USB-порты. Понимая при этом, что к выражению «что попало» относятся даже USB-модемы, которые снаружи кажутся всего лишь маленьким и безобидным устройством связи.

Разработчики мобильной технологии LTE все же позаботились о ее защите несколько больше, чем разработчики Интернета. Поэтому можно надеяться, что мобильная сеть будет более надежна и безопасна, чем Всемирная сеть. В LTE используется почти такая же модель безопасности, как и в ранних версиях мобильной связи. Хотя архитектура сети несколько изменилась, общие принципы защиты остались прежними. Если в предыдущих версиях мобильной сети за безопасность отвечал RNC, то теперь его нет, а защита возложена на базовые станции, которые стали более интеллектуальными. Как сообщил Дмитрий Костров, главный эксперт МТС, все функции защиты в LTE объединены стандартом и подразумевают защиту на нескольких уровнях. Предусмотрена защита на уровне доступа к сети, на уровнях сетевого и пользовательского доменов, на уровне приложений и уровне отображения и конфигураций [3].

Каждый из этих уровней предполагает аутентификацию и авторизацию всех устройств, чего нет в Интернете. Хотя каждое устройство в IP-сети имеет свой адрес, а часто еще и уникальный идентификатор MAC, его достаточно легко изменить и подделать. Однако технология LTE предусматривает использование не только IP-адреса, но и системы распространения ключей шифрования для всех устройств, подключенных к сети. В результате для всех взаимодействий в мобильной сети есть возможность безопасного обмена ключевой информацией и установления шифрованного канала связи между ними.

В LTE сохраняются и методы аутентификации пользователей по привязке к карте USIM, как в традиционной мобильной связи: пользователь может заблокировать доступ к телефону по PIN-коду. Василий Сахаров, руководитель отдела информационной безопасности компании «Демос», отмечает, что в LTE от GSM и UMTS наследуются схемы протокола аутентификаиции EAP, в которые добавлены новые алгоритмы, более длинные ключи и расширенная иерархия PKI. Предусмотрены и новые

функциональные возможности для новых сценариев, включающих межмашинное взаимодействие (M2M) и однократную аутентификацию (SSO). Кроме того, предусмотрена защита от несанкционированных соединений поверх мультимедийной IP-сети IMS. Вполне возможно, что используемая в мобильной связи более жесткая система аутентификации позволит навести порядок и в Интернете [5].

Таким образом, для решения проблемы эффективного обеспечения информационной безопасности 4G-сетей, в рамках проведённого исследования, были предложены следующие рекомендации:

- совершенствование протоколов и методов аутентификации пользователей по привязке к карте USIM (получение доступа по PIN-коду);
- использование жесткой системы аутентификации;
- добавление новых алгоритмов в протокол аутентификации и использование расширенной иерархии PKI;
- ограничение доступа к оборудованию передачи данных, скрытие его технических характеристик и установленного программного обеспечения;
- пересмотр, дополнение и модификация сигнатурных протоколов, а также программируемых сетей (SDN);
- использование только проверенных (безопасных) устройств и специального защитного программного обеспечения.

Комплексная реализация данных рекомендаций позволит уменьшить возможную величину возможного как для рядовых пользователей, так и для корпоративных сетей.

Литература

1. 4G ‘inherently less secure’ than 3G. The Telegraph, 2014.
2. Безопасность мобильного интернета изнутри и снаружи. Positive technologies, 2013.
3. Мобильные телефоны и тотальная слежка АНБ: как это работает. Positive technologies, 2014.
4. Соляной В.Н., Сухотерин А.И Выработка коммуникативной компетенции при подготовке профессионалов по информационной безопасности с использованием технологии модерации. «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической

Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7
5. Соляной В.Н., Сухотерин А.И, Антоненко В.И. Проблемно-ориентированная подготовка специалистов по информационной безопасности с использованием имитационного метода (мозговой штурм). «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7.
6. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
7. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Развитие сотрудничества российских и зарубежных ВУЗОВ по защите информационного ресурса. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
8. Статистика уязвимостей корпоративных информационных систем в 2013 г. Positive technologies, 2014.
9. Статистика уязвимостей мобильной связи на основе SS7. Positive technologies, 2014.
10. Уязвимости сетей мобильной связи на основе SS7. Positive technologies, 2014.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЯ В ОПЕРАЦИОННОЙ СИСТЕМЕ WINDOWS 10

Светлов Сергей Юрьевич, студент 1 курса кафедры Информационной безопасности
Научный руководитель: **Соляной Владимир Николаевич**, к.воен.н., доцент, заведующий кафедрой Информационной безопасности

Операционная система Windows 10 от компании Microsoft была выпущена в конце июля 2015 года. Эта версия операционной системы (ОС) стала бесплатной для всех пользователей официальных версий Windows 7, 8, 8.1. Но многие успели заметить, что после обновления до более новой версии Windows ОС стала запрашивать гораздо больше информации о пользователе. Сама компания не отрицает существование "шпионского" функционала в данной ОС. Поэтому большинство пользователей, которым понравился интерфейс новой системы, стали задаваться вопросом: "Как же отключить функции слежения в Windows 10?" На данный момент существует несколько способов сокращения объема информации, которую получает с компьютера, на котором установлена ОС Windows 10, компания Microsoft. Именно о таких способах и пойдет речь в данной статье.

Данные пользователей, НСД, «шпионский» функционал Windows 10.

PROTECTION OF USERS' PERSONAL DATA IN WINDOWS 10 OPERATING SYSTEM

Svetlov Sergey, 1st year student of the Department of information security
Scientific adviser: **Solyanoy Vladimir,** Candidate of Military Sciences, Assistant Professor, Head of the Department of information security

Operating System Windows 10 from Microsoft was released in late July 2015. This version of the operating system (OS) is free for all users of the official version of Windows 7, 8, 8.1. But many have already noticed that after upgrading to a newer version of the Windows operating system was the request much more information about the user. The company itself does not deny the existence of a "spy" functionality in the operating system. Therefore, the majority of users who liked the interface of the new system began to wonder: "How to disable the tracking feature in Windows 10?" At the moment, there are several ways to reduce the amount of

information which is received from a computer that is running the Windows 10, Microsoft has. It is about such methods will be discussed in this article.

User data, unauthorized access, «the spy» Windows 10 functionality.

Перед тем как решить проблему противодействия сбору информации различными способами стоит рассказать, зачем указанный «шпионский» функционал нужен [5]. В настоящее время существует множество различных сервисов, которые улучшают работу программных приложений. Благодаря сбору пользовательской информации приложения могут выдавать нужные данные без дополнительного запроса, например результат матча вашей любимой команды. Такие крупные компании, как “Google” и “Яндекс” давно пользуются такими «облачными» сервисами, собирая базовую информацию о пользователе, чтобы выдавать в поисковике именно то, что он ищет. А реклама Google AdSense показывает объявления на различных сайтах, основываясь на последних результатах поиска. Те же антивирусы собирают информацию, например о скаченных пользователем из интернета файлах. Иногда эти данные отправляются в центральное управление данного антивирусного программного обеспечения (ПО) для выявления новых угроз и поиска способа их устранения [1-8].

Рассмотрим существующие системы контроля в ОС Windows 10: Windows Defender; Advertising ID; строка поиска; телеметрия; облачные сервисы. Во-первых, это стандартный антивирус Windows Defender. Как уже было изложено выше, антивирусы собирают множество информации о приложениях, запускаемых пользователем, о загружаемых из интерента файлах и т.д. Данный антивирус является частью Windows 10 и его нельзя удалять. Однако его можно деактивировать, либо установить сторонний антивирус, что автоматически отключит Windows Defender.

Следующая система контроля, это Advertising ID. Как уже было указано выше, различные поисковые системы (например Google и Яндекс) собирают базовую информацию о пользователе, для предоставления желаемых поисковых запросов и показа рекламы. Компания Microsoft долго не могла конкурировать с такими крупными проектами, поэтому в новой версии ОС каждому пользователю был присвоен специальный идентификатор -

Advertising ID. Благодаря ему производится подбор рекламы по предпочтениям пользователя.

Очередная система контроля - это строка поиска. Данный элемент интерфейса всегда был полезен в работе. Сейчас он так же важен, но потерпел некоторые изменения. Теперь поиском можно пользоваться как локально, так и глобально (в данном случае ОС пытается предугадать желания пользователя). Для корректной работы системы глобального поиска ОС отправляет данные нажатия клавиш и движения мыши каждые полчаса. Таким образом, некий злоумышленник, взломавший сервера Microsoft, может получить все данные о нажатии клавиш многих пользователей буквально за несколько минут. Например, если пользователь оплачивал с помощью карты какую-то покупку в интернет-магазине или счета, а так же заходил на сайты через разные логины и пароли, вводил чей-то номер телефона или адрес, то вся эта конфиденциальная информация будет в руках злоумышленника. Конечно, Microsoft крупная компания, которая будет оберегать данные своих пользователей, но она обязана предоставлять информацию по требованию властей. Этого требует как законодательство США, так и России, а так же законы ряда других стран. В таких случаях информация не будет использована в корыстных целях. Но от несанкционированного доступа (НСД) никто не может быть застрахован на все 100%, и это нужно учитывать.

В-четвертых - это телеметрия. Microsoft собирает данные о работе приложений, чтобы улучшить их функционал и исправить различные проблемы. Но так же это позволяет компании запрещать пользователю доступ к информации, которая по их мнению является нелегальной копией продукта, а так же к некоторым периферийным устройствам.

В-пятых, облачные сервисы [3]. Они очень распространены в последнее время, так как удобны в использовании. Но именно сервисы Windows 10 не пользуются большой популярностью у жителей стран СНГ. Облачный сервис OneDrive для хранения документов, игровой сервис Xbox, компоненты Office 365 в офисном пакете Microsoft Office успешно заменяются другими сервисами, более привычными рядовому пользователю. Но эти сервисы включены по умолчанию в новой версии ОС.

Пользоваться ли данными функциями и сервисами - личный выбор каждого пользователя. В то же время необходимо рассмотреть

и другую задачу-технологии защиты персональных данных (ПД) пользователя персонального компьютера (ПК) от систем слежения ОС.

Проведенный автором анализ рынка ОС (рис. 1) показал следующие особенности использования современных ОС пользователя [4].

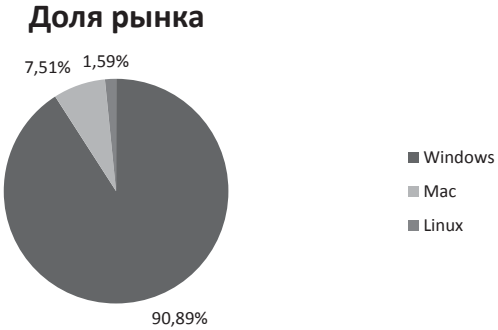


Рисунок 1 - Доля рынка ОС

Как видно из диаграммы выше (данные на ноябрь 2015), почти 91% пользователей ПК используют ОС от Microsoft. Логично предположить, что большую часть информации собирают именно с пользователей Windows для оптимизации рабочего процесса. Так же львиная доля вирусов, хакерских атак и попыток НСД приходится на эту ОС. Ее новая версия гораздо привлекательней для хакерских атак такого рода. Поэтому в последнее время некоторые пользователи стали переходить обратно на более привычную и удобную Windows 7.

По данным о числе пользователей различных версий ОС Windows можно проследить, как люди обновляли свои ПК на более новую версию. В августе этого года, на следующий месяц после релиза, число пользователей Windows 10 составило 5,21% от общего числа пользователей ПК, а число пользователей Windows 7 уменьшилось на 3,06%- с 60,73% до 57,67%.

Но на данный момент (ноябрь 2015) число пользователей Windows 7 снова начало расти (рис. 2).

Аудитория Windows 10 незначительно увеличилась и равна 9%. Для сравнения, на данный момент число пользователей уже не поддерживаемой ОС Windows XP равно 10%. Простая статистика говорит нам о том, что люди попробовали новую систему, но либо

привыкли к более старой версии и поэтому возвращаются к ней, либо минусы новой ОС перевешивают ее плюсы.

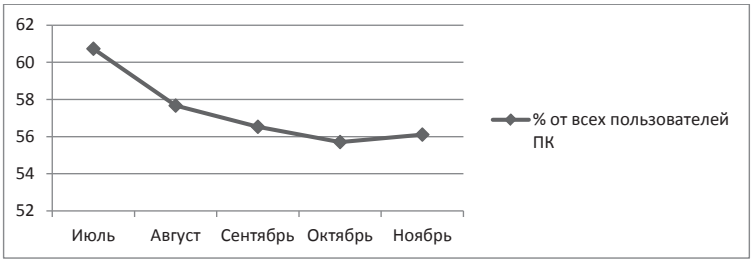


Рисунок 2 - Аудитория, использующая ОС Windows 7 (в процентах от числа пользователей во всем мире)

Об одном таком человеке хотелось бы поговорить подробнее [6]. Анонимный пользователь из Чехии следил за трафиком, который отсылает его ПК с Windows 10 на сервера Microsoft. Он узнал, когда Windows 10 отправляет данные, на какой сервер, с какой частотой и в каком объеме. Самым простым примером стало то, что каждые полчаса Windows 10 отправляет пакет данных с набранным на клавиатуре текстом. Этот же пользователь постарался ограничить доступ Windows 10 к информации, но получилось это лишь частично. Он заметил, что несмотря на изменение настроек, после того как он пользовался микрофоном в своем компьютере, система отправляла в Microsoft пакеты данных. Судя по их объему, это были звуковые файлы. Так же во время использования веб-камеры были отправлены пакеты данных общим объемом в 35 Мб. Этого вполне хватает на серию фотоснимков или короткое видео.

Так же следует отметить, что когда этот пользователь вводил названия американских фильмов, ОС отправляла пакет данных, а после проверяла содержимое жесткого диска. При вводе названий чешских фильмов ничего подобного не происходило. Скорее всего ОС будет сама искать пиратские копии лицензионных продуктов на вашем ПК и удалять их, если того потребуют авторы.

Так как же хоть частично скрыть конфиденциальную информацию и прежде всего персональные данные пользователя от Windows 10? Существует несколько способов:

Первый способ – Настройки (один из самых простых). Многие даже не догадываются, но большую часть данных, которые собирает Windows 10, можно обезопасить простым отключением ряда пунктов в настройках.

Во-первых, отключение Windows Defender. Как уже было сказано мною выше, он сам отключается при установке стороннего антивирусного ПО. Но если пользователь захотел отключить его вручную без установки нового антивируса (что не рекомендуется): в меню настроек «Параметры» перейти во вкладку «Обновление и безопасность»; далее перейти на опцию «Защитник Windows». В данном меню пользователь может отключить защиту ПК и отправку пакетов данных с подозрительными образцами кода в центр Microsoft.

Во-вторых, осуществить настройки конфиденциальности. Используем те же «Параметры», только теперь переходим во вкладку «Конфиденциальность», а затем на «Общие» (рис. 3). В этом меню можно отключить Advertising ID (идентификатор получателя рекламы), о котором указывалось ранее. Так же в данном меню можно отключить фильтр SamartScreen для проверки веб-содержимого и отсылку сведений о написании (распознавание рукописного ввода). Так же целесообразно внимательно просмотреть информацию во всех вкладках меню «Конфиденциальность»: таких как «Расположение», «Камера» и т.д., а так же отключить либо ограничить большинство функций (а не только для вкладки “общие”).

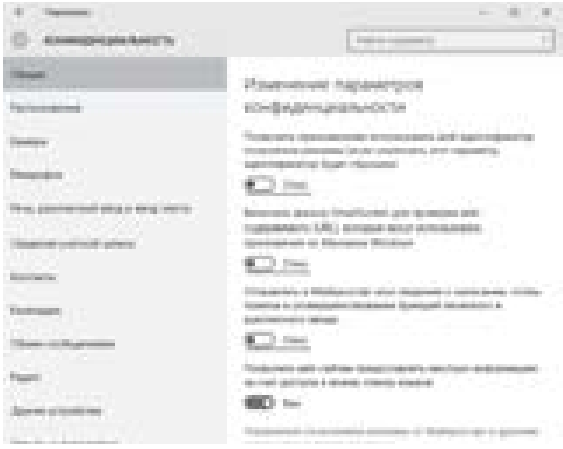


Рисунок 3 - Фрагмент меню общих параметров конфиденциальности в ОС Windows 10

Второй способ - Отключение телеметрии. Для этого потребуется ввести несколько команд в консольном режиме (комбинация кнопок Win+X → “командная строка (администратор)”) на встроенном языке программирования PowerShell.

Ниже указаны данные команды:

- sc delete DiagTrack;
- sc delete dmwappushservice;
- echo "" > C:\ProgramData\Microsoft\Diagnosis\ETLLogs\AutoLogger\AutoLogger-Diagtrack-Listener.etl;
- reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\DataCollection" /v AllowTelemetry /t REG_DWORD /d 0 /f.

Такая последовательность команд стирает данные, которые были собраны сервисом телеметрии, затем выключает его и, наконец, записывает в реестр запрет на дальнейший сбор данных. Команд, ограничивающих «шпионский» функционал Windows 10 гораздо больше и при желании вы можете найти их в интернете.

Третий способ - Использование стороннего ПО. Уже существует ряд программ, которые помогают защититься от сбора данных. Их принцип работы довольно прост: они не защищают данные от сбора, а просто перенаправляют их на другой ip-адрес, а именно на 0.0.0.0., который никуда не ведет. Таким образом, данные никуда не отправляются, а уходят в пустоту. Одной из таких программ является DisableWinTracking (рис. 4).

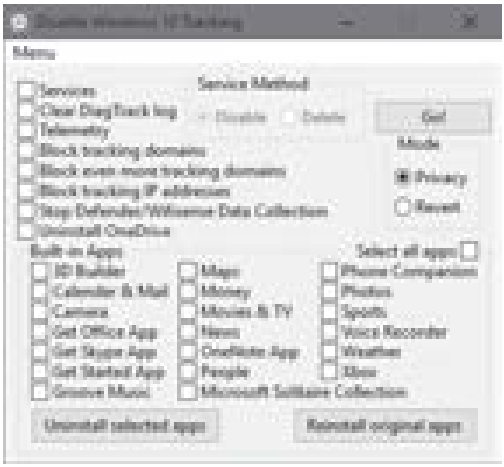


Рисунок 4 - Интерфейс DisableWinTracking

Это надежный метод защиты, но и у него есть свои минусы. Microsoft часто обновляет свою ОС и может изменить ip-адреса, куда поступают пакеты данных о пользователе, в любой момент. Так же некоторые приложения Windows 10 используют статический ip-адрес, который программа будет не в силах изменить. Разработчики данного

ПО должны постоянно следить за обновлениями Windows 10 и обновлять свои приложения.

Таким образом, в данной статье были получены следующие результаты:

1. Проведенный автором анализ функционала современных ОС для автоматизированного рабочего места (АРМ) показал, что новая ОС Windows 10 обладает возможностью сбора и анализа ряда конфиденциальной информации пользователя, в том числе и персональных данных.

2. Предположительными мерами защиты ПД пользователя, работающего с ОС Windows 10, следует рассматривать:

a. Изменение настроек ОС;
b. Использование консольных команд;
c. Использование стороннего ПО.

3. Наиболее эффективным будет использование стороннего ПО.

4. Следовательно, защититься от сбора информации новой ОС от Microsoft можно несколькими способами. Желательно использовать не один из них, а сразу несколько. Таким образом повысится безопасность данных на вашем персональном рабочем месте.

В заключение хотелось бы указать, что не стоит доводить до крайности желание обезопасить свои данные. Постоянно следить за своим поведением в сети интернет: не посещать сомнительные сайты; не отвечать на спам; не скачивать ПО с подозрительных источников и т.д. Прежде всего, именно от действий пользователя зависит целостность и сохранность его данных [1-8].

Литература

1. Блинов А.М. Информационная безопасность / СПб.: СПбГУЭФ, 2010.
2. Малюк А.А. Введение в информационную безопасность: Учебное пособие для вузов / В.И.Королёв, В.М. Фомичев. – М.: Горячая линия - телеком, 2013.
3. Петренко С.А. и Курбатов В.А. Политики безопасности компании при работе в интернет / М.: ДМК Пресс, 2011.
4. Соляной В.Н., Сухотерин А.И. Модульно-ориентированный подход формирования базовых дисциплин ФГОС ВО 3+ как основа реализации профессиональной подготовки бакалавров в области информационной безопасности Научно-практический журнал №25, том 2 2015г. Информационное противодействие угрозам терроризма

Материалы XIX Пленума учебно-методического объединения по образованию в области информационной безопасности «учебно-методическое обеспечение образовательных программ в области информационной безопасности» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН.ФЕД.УНИВ, 2015.-332 с. ISSN 2219-8792
5. Соляной В.Н., Сухотерин А.И. Становление направления «Радиоэлектронная безопасность информационных объектов» в системе дополнительного профессионального по информационной безопасности. Научно-практический журнал №25, том 2 2015г. Информационное противодействие угрозам терроризма Материалы XIX Пленума учебно-методического объединения по образованию в области информационной безопасности «учебно-методическое обеспечение образовательных программ в области информационной безопасности» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН.ФЕД.УНИВ, 2015.-332 с. ISSN 2219-8792
6. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Некоторые перспективы применения систем контроля и управления доступом в региональных ВУЗАХ. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международная научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.

ИНФОРМАЦИОННЫЕ УГРОЗЫ В ЛОКАЛЬНЫХ WI-FI СЕТЯХ ТИПОВОГО ПРЕДПРИЯТИЯ

Сирючкин Илья Андреевич, студент 1 курса кафедры Информационной безопасности
Научный руководитель: **Соляной Владимир Николаевич,** к.воен.н., доцент, заведующий кафедрой Информационной безопасности

В наши дни очень распространённо повсеместное использование сетей Wi-Fi. Более того эксперты предсказывают, что к 2016 году трафик в беспроводных сетях на 10% превзойдет трафик в проводном Internet. При этом каждый год количество частных точек доступа становится на 20% больше. При этом 80% пользователей, в том числе владельцы кампаний, организаций и предприятий не меняют пароли доступа по умолчанию. Именно по

этим причинам исследования в данной сфере информационной безопасности так актуальны.

Wi-Fi, точка доступа, «чужак», траффик.

INFORMATION THREATS IN LOCAL WI-FI NETWORKS OF THE STANDARD ENTERPRISE

Siryuchkin Ilya, 1 year student of the Department of information security
Scientific adviser: **Salyanoy Vladimir,** candidate of Military Sciences, Associate Professor, Head of the Department of information security

Today very popular universal use of the Wi-fi networks. Moreover, experts foretell that by 2016 the traffic in wireless networks for 10% will surpass a traffic in wire Internet. Thus, every year the quantity of private points of access becomes 20% more. Thus 80% of users, including owners of campaigns, the organizations and enterprises do not change passwords of access by default. For these reasons of research in this sphere of information security are so actual.

Wi-Fi, access point, "stranger", traffic.

Изначально технология Wi-Fi была ориентирована на организацию точек быстрого доступа в Интернет (hotspot) для мобильных пользователей. Преимущества беспроводного доступа очевидны, а технология Wi-Fi изначально стала стандартом, которого придерживаются производители мобильных устройств. Постепенно сети Wi-Fi стали использовать малые и крупные офисы для организации внутренних сетей и подсетей, а операторы создавать собственную инфраструктуру предоставления беспроводного доступа в Интернет на основе технологии Wi-Fi. Таким образом, в настоящее время сети Wi-Fi распространены повсеместно и зачастую имеют зоны покрытия целых районов города.

С точки зрения безопасности [1-7], следует учитывать не только угрозы, свойственные проводным сетям, но также и среду передачи сигнала. В беспроводных сетях получить доступ к передаваемой информации намного проще, чем в проводных сетях, равно как и повлиять на канал передачи данных. Достаточно поместить соответствующее устройство в зоне действия сети [3].

IEEE 802.11 — набор стандартов связи для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 0,9, 2,4, 3,6 и 5 ГГц (рис. 1).

Пользователям более известен по названию Wi-Fi, фактически являющемуся брендом, предложенным и продвигаемым организацией Wi-Fi Alliance. Получил широкое распространение благодаря развитию мобильных электронно-вычислительных устройств: КПК и ноутбуков.

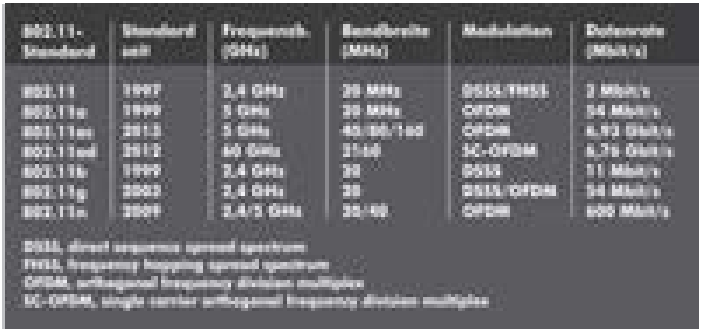


Рисунок 1 – Список стандартов IEEE 802.11

Угрозы информационной безопасности, возникающие при использовании Wi-Fi сетей, можно условно разделить на два класса:

1) прямые - угрозы информационной безопасности, возникающие при передаче информации по беспроводному интерфейсу IEEE 802.11 (рис. 2). К прямым угрозам относятся: «чужаки», нефиксированная природа связи, уязвимости сетей и устройств и взлом шифрования;

2) косвенные — угрозы, связанные с наличием на объекте и рядом с объектом большого количества Wi-Fi-сетей, а также утечка из проводной сети.

Чужаками (RogueDevices, Rogues) называются устройства, предоставляющие возможность неавторизованного доступа к корпоративной сети, обычно в обход механизмов защиты, определенных политикой безопасности. Запрет на использование устройств беспроводной связи не защитит от беспроводных атак, если в сети, умышленно или нет, появится чужак.

В роли чужака может выступать всё, у чего есть проводной и беспроводной интерфейсы: точки доступа (включая программные), сканеры, проекторы, ноутбуки с обоими включёнными интерфейсами и т.д. Беспроводные устройства могут менять точки подключения к

сети прямо в процессе работы. Например, могут происходить «случайные ассоциации», когда ноутбук с Windows XP (доверительно относящейся ко всем беспроводным сетям) или просто некорректно сконфигурированный беспроводной клиент автоматически ассоциируется и подключает пользователя к ближайшей беспроводной сети. Таким образом, нарушитель переключает на себя пользователя для последующего сканирования уязвимостей, фишинга или атак "человек посередине".

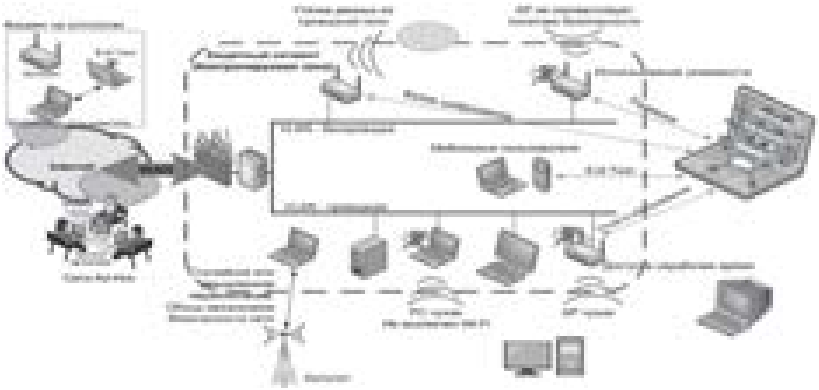


Рисунок 2 – Схема прямых угроз в Wi-Fi сетях

А если пользователь при этом подключен и к проводной сети, то он становится точкой входа - чужаком. К тому же многие пользователи, подключённые к внутренней сети и имеющие Wi-Fi интерфейс, недовольные качеством и политикой работы сети, переключаются на ближайшую доступную точку доступа (или операционная система делает это автоматически при отказе проводной сети). При этом вся защита сети терпит крах.

Ещё одна проблема - сети Ad-Hoc, с помощью которых удобно передавать файлы коллегам или печатать на принтере с Wi-Fi. Но такая организация сетей не поддерживает многие методы обеспечения безопасности, что делает их лёгкой добычей для нарушителя. Новые технологии Virtual WiFi и Wi-Fi Direct_только ухудшили ситуацию [1].

Некорректно сконфигурированные устройства, устройства со слабыми и недостаточно длинными ключами шифрования, использующие уязвимые методы аутентификации - именно такие устройства подвергаются атакам в первую очередь. Согласно отчётам аналитиков, большая часть успешных взломов происходит как раз из-

за неправильных настроек точек доступа и программного обеспечения клиента [4].

Достаточно подключить неправильно настроенную точку доступа к сети для взлома последней. Настройки "по умолчанию" не включают шифрование и аутентификацию, или используют ключи, прописанные в руководстве и поэтому всем известные. Маловероятно, что пользователи достаточно серьёзно озаботятся безопасной конфигурацией устройств. Именно такие привнесённые точки доступа и создают основные угрозы защищённым сетям.

Некорректно настроенные устройства пользователей - угроза опаснее, чем некорректно сконфигурированные точки доступа. Это устройства пользователей, и они не конфигурируются специально в целях безопасности внутренней сети предприятия. К тому же они находятся за периметром контролируемой зоны, так и внутри него, позволяя злоумышленнику проводить всевозможные атаки, как-то распространять вредоносное программное обеспечение или просто обеспечивая удобную точку входа.

О защищённости WEP и речи уже нет. Интернет полон специального и удобного в использовании ПО для взлома этого стандарта, которое собирает статистику трафика до тех пор, пока её не станет достаточно для восстановления ключа шифрования. Стандарты WPA и WPA2 также имеют ряд уязвимостей разной степени опасности, позволяющих их взлома [2]. Пока что нет информации об успешных атаках на WPA2-Enterprise (802.1x).

Имперсонация авторизованного пользователя – серьезная угроза любой сети, не только беспроводной. Однако в беспроводной сети определить подлинность пользователя сложнее. Конечно, существуют SSID и можно пытаться фильтровать по MAC-адресам, но и то и другое передается в эфире в открытом виде, и их несложно подделать, а подделав – как минимум снизить пропускную способность сети, вставляя неправильные кадры, а разобравшись в алгоритмах шифрования – устраивать атаки на структуру сети (например, ARP-spoofing). Имперсонация пользователя возможна не только в случае MAC-аутентификации или использования статических ключей. Схемы на основе 802.1x не являются абсолютно безопасными. Некоторые механизмы (LEAP) имеют сложность взлома схожую со взломом WEP. Другие механизмы, EAP-FAST или PEAP-MSCHAPv2 хотя и надёжнее, но не гарантируют устойчивость к комплексной атаке.

DoS атаки направлены на нарушение качества функционирования сети или на абсолютное прекращение доступа пользователей. В случае Wi-Fi сети отследить источник, заваливающий сеть "мусорными" пакетами, крайне сложно - его местоположение ограничивается лишь зоной покрытия. К тому же есть аппаратный вариант этой атаки - установка достаточно сильного источника помех в нужном частотном диапазоне.

Сигналы WiFi-устройств имеют достаточно сложную структуру и широкий спектр, поэтому эти сигналы, а тем более, окружающие устройства Wi-Fi невозможно идентифицировать обычными средствами радиомониторинга. Уверенное обнаружение сигнала WiFi современными комплексами радиомониторинга в широкой полосе частот возможно только по энергетическому признаку при наличии полос параллельного анализа шириной несколько десятков МГц на скорости не менее 400 МГц/с и лишь в ближней зоне. Сигналы точек доступа, находящихся в дальней зоне, оказываются ниже уровня шумов приёмника. Обнаружение Wi-Fi-передатчиков при последовательном сканировании узкополосными приёмниками вообще невозможно.

Исходя из того, что практически каждый объект окружает множество "чужих" Wi-Fi сетей, отличить легальных клиентов своей сети и соседних сетей от нарушителей крайне сложно, что позволяет успешно маскировать несанкционированную передачу информации среди легальных Wi-Fi-каналов.

Wi-Fi-передатчик излучает так называемый «OFDM сигнал». Это означает, что в один момент времени устройство передаёт в одном сигнале, занимающем широкую полосу частот (около 20 МГц) несколько несущих информацию - поднесущих информационных каналов, которые расположены так близко друг от друга, что при приёме их на обычном приёмном устройстве, сигнал выглядит как единый «купол». Выделить в таком «куполе» поднесущие и идентифицировать передающие устройства можно только специальным приёмником.

В крупных городах Wi-Fi сети общего пользования имеют достаточно обширную зону покрытия, чтобы отпала необходимость использовать мобильный пункт приёма информации рядом с объектом - несанкционированное устройство может подключиться к доступной Wi-Fi сети и использовать её для передачи информации через Интернет в любое требуемое место.

Пропускная способность Wi-Fi сетей позволяет передавать звук и видео в реальном времени. Это упрощает злоумышленнику использовать акустические и оптические каналы утечки информации - достаточно легально купить Wi-Fi-видеокамеру и установить её в качестве устройства негласного получения информации. Примеры:

1.С Wi-Fi видеокамеры с микрофоном информация передаётся на точку доступа, работающую в режиме ретранслятора. Точка расположена на крыше и имеет направленную антенну — таким образом можно значительно увеличить дальность сигнала — до нескольких километров. Сам сигнал принимается на контрольном пункте.

2.Смартфон сотрудника с помощью вируса записывает окружающий звук и передаёт его злоумышленнику с помощью Wi-Fi. В качестве контрольного пункта используется точка доступа со скрытым именем, чтобы обнаружить её было труднее.

3.Если на объекте ограничен вынос носителей информации и выход в Интернет ограничен, то одним из вариантов скрытой передачи большого объёма информации является Wi-Fi. Нужно подключиться к соседним Wi-Fi сетям, оставаясь незамеченным среди легальных пользователей.

Как правило, беспроводные сети соединяются с проводными. Значит, через точку доступа можно атаковать проводную сеть. А если наличествуют ошибки в настройке как проводной, так и беспроводной сети, то открывается целый плацдарм для атак. Пример - точки доступа, работающие в режиме моста (Layer 2 Bridge), подключённые в сеть без маршрутизаторов или в сеть с нарушением сегментации и передающие в радиоэфир широковещательные пакеты из проводной части сети (ARP-запросы, DHCP, кадры STP и д.р.). Эти данные в целом полезны для разведки, и на их основе можно проводить такие атаки, как "человек посередине", атаки отказа в обслуживании, отравление кеша DNS и др.

Другой пример - при наличии нескольких ESSID (Extended Service Set Identifier) на одной точке доступа. Если на такой точке настроена как защищённая сеть, так и публичная, при неправильной конфигурации широковещательные пакеты будут отправляться в обе сети. Это позволит злоумышленнику, например, нарушить работу DHCP или ARP в защищённом сегменте сети. Это можно запретить, организовав привязку ESS к BSS, что поддерживается

практически всеми производителями оборудования класса Enterprise (и мало кем из класса Consumer)

У беспроводных сетей наличествуют некоторые особенности, отсутствующие в проводных сетях. Эти особенности в целом влияют на производительность, безопасность, доступность и стоимость эксплуатации беспроводной сети. Их приходится учитывать, хотя они и не относятся напрямую к шифрованию или аутентификации. Для решения этих вопросов требуется специальный инструментарий и механизмы администрирования и мониторинга.

Исходя из того, что политикой безопасности логично ограничить доступ к сети вне рабочего времени (вплоть до физического отключения), беспроводная активность сети в нерабочее время должна отслеживаться, считаться подозрительной и подлежать расследованию.

Скорость подключения зависит от соотношения сигнал/шум (SNR). Если, скажем, 54 Мбит/с требует SNR в 25 dB, а 2 Мбит/с требует 6 dB, то кадры, отправленные на скорости 2 Мбит/с «пролетят» дальше, т.е. их можно декодировать с большего расстояния, чем более скоростные кадры. Также все служебные кадры , а также бродкасты, отправляются на самой нижней скорости. Это означает, что сеть будет видно на значительном расстоянии. Если в сети, где все работают на определённой скорости (офис территориально ограничен и скорости подключения у пользователей примерно одинаковые) появляется подключение на 1-2 Мбит/с - скорее всего это нарушитель. Также можно отключить низкие скорости, тем самым повысив скорость передачи информации в сети.

Качество работы Wi-Fi сети как радиоэфира зависит от многих факторов. Один из них - интерференция радиосигналов, которая может значительно снизить пропускную способность сети и количество пользователей, вплоть до полной невозможности использования сети. В качестве источника может выступать любое устройство, излучающее на той же частоте сигнал достаточной мощности. Это могут быть как соседние точки доступа, так и микроволновки. Эту особенность могут также использовать злоумышленники в качестве атаки отказа в обслуживании, или для подготовки атаки "человек посередине", заглушая легитимные точки доступа и оставляя свою с таким же SSID.

Существуют и другие особенности беспроводных сетей помимо интерференции. Неправильно настроенный клиент или сбоящая

антенна могут ухудшить качество обслуживания всех остальных пользователей. Или вопрос стабильности связи. Не только сигнал точки доступа должен достичь клиента, но и сигнал клиента должен достичь точки. Обычно точки мощнее, и чтобы добиться симметрии, возможно придётся снизить мощность сигнала. Для 5 ГГц следует помнить, что надежно работают только 4 канала: 36/40/44/48 (для Европы, для США есть еще 5). На остальных включен режим сосуществования с радарами (DFS). В итоге, связь может периодически пропадать.

Подытоживая все выше сказанное можно сделать вывод, что основными угрозами для Wi-Fi сети являются чужаки и взлом шифрования. Кроме того, существует ряд проблем, которые можно устранить при качественном оборудовании и должном инструктировании сотрудников. Так как беспроводные Wi-Fi сети в наши дни можно встретить буквально на каждом ходу, способов их взлом, а соответственно и их защиты невероятное множество. Беспроводная сеть – это самый простой, но и самый ненадежный способ обеспечения доступа в Интернет сотрудникам. Надеемся данная статья будет полезна, как частным пользователям беспроводных точек доступа, желающих обезопасить свой трафик, так и владельцам локальных Wi-Fi сетей, желающих обезопасить своё предприятие от несанкционированных взломов и организовать достойную защиту информации на предприятии.

Литература

1. Бандурян А., Журнал Компьютерное обозрение. Анализ угроз для беспроводных сетей. - 2010. - №12
2. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А // Учебное пособие для вузов/. – М.: Горячая линия – Телеком, 2006. – 544 с.
3. Белорусов Д. И., Корешков М. С. Специальная техника. WiFi-сети и угрозы информационной безопасности. - 2009. - №6. – С. 2-6.
4. Малюк А.А., Горбатов В. С., Королёв В. И Введение в информационную безопасность: Учебное пособие для вузов/. и др.; Под ред. Горбатова В. С., - М.; Горячая линия – Телеком, 2011. – 228 с.: ил. – ISBN 978-5-9912-0160-5
5. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Некоторые перспективы применения систем контроля и управления доступом в региональных ВУЗАХ. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества

российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.*Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
6. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Развитие сотрудничества российских и зарубежных ВУЗОВ по защите информационного ресурса. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
7. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.

РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ В СРЕДЕ BUSINESS INTELLIGENCE (BI)

Тюрин Владислав Сергеевич, студент 3 курса кафедры Информационной безопасности
Научный руководитель: **Сухотерин Александр Иванович**, к.воен.н., доцент кафедры Информационной безопасности

Информация является важным ресурсом во всех вопросах, в частности получения прибыли или какого-либо преимущества. Чем доступнее, достовернее и своевременно мы можем воспользоваться информацией, тем быстрее мы можем извлечь из этого выгоду или принять решение. С этими задачами может справиться технология Business Intelligence (BI). Её можно рассматривать, как методы и инструменты для перевода необработанной информации в осмысленную, удобную форму. Технологии BI обрабатывают большие объемы неструктурированных данных, чтобы найти стратегические возможности для бизнеса. Фактически это единая система отчётности и анализа.

Актуальность данной темы заключается в том, что многие компании, не придают должного внимания защите компонентов Business Intelligence, тем самым подвергая свою информацию опасности.

Политика информационной безопасности, защита, Business intelligence.

RECOMMENDATIONS ON THE ORGANIZATION OF INFORMATION SECURITY ENVIRONMENT IN BUSINESS INTELLIGENCE (BI)

Tyurin Vladislav, 3rd year student of the Department of information security
Scientific adviser: **Sukhoterin Alexander,** Candidate of Military Sciences, Associate Professor of the Department of information security

Information has always been an important resource in all matters, in particular, for profit or an advantage. The availability, reliability, and we can use the information in a timely manner, so we can quickly take advantage of it and make a decision. With these tasks can handle technology Business Intelligence (BI). It can be regarded as techniques and tools to translate raw data into meaningful, usable form. BI Technologies handle large volumes of unstructured data, to find strategic business opportunities. In fact, it is a unified system of reporting and analysis.

The relevance of this topic is that many companies do not give due attention to the protection components Business intelligence, thus exposing their information risk.

Information Security Policy, Protection, Business intelligence.

На данной схеме представлено, что каждый из основных компонентов BI-оболочки имеет "свою степень риска" и для обеспечения безопасности каждого компонента потребуется реализовать различные подходы (и различные технологии). Это крайне непростая задача, и, пожалуй, наибольшую сложность представляют "пробелы" между компонентами. Ведь BI-оболочка никогда не поставляется как одним поставщиком, так и в виде одной технологии, а бесшовная интеграция между компонентами невозможна. Более того, именно то, как компоненты работают друг с

другом, и то, как информация проходит между ними, и образует "точки риска". Сама суть Business Intelligence подталкивает бизнес-пользователей к расширению доступа к данным и контроля над ними.

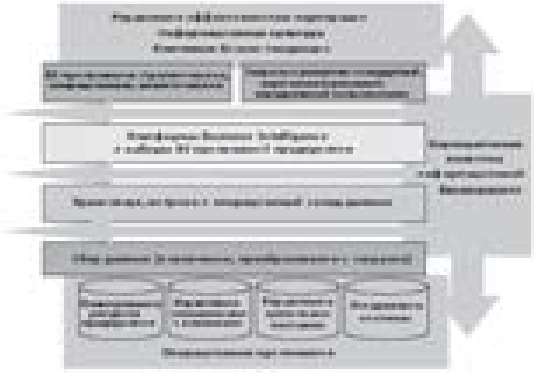


Рисунок 1 - Схема безопасности в BI-платформе [1]

Поэтому необходима жесткая политика по защите информации, которая должна помочь "залатать дыры", а также минимизировать огромный риск, присущий человеческому фактору [1-14].

Рисунок 2 - Структурная схема основных компонентов составляющих защиту информации в BI-среде

Данные в хранилище, витринах и операционных складах данных создают условия для осуществления всей BI-деятельности и, как правило, включают гигантские объемы детальных, транзакционных данных. Поскольку они часто отображают длительный отрезок времени, относящейся к истории существования компании, как, например, финансовая информация, обеспечение защищенности таких данных чрезвычайно важно. При построении модели защиты информации необходимо знать [4-6, 11-14]:

- кто располагает доступом к хранилищу, витрине данных, кубам и так далее;
- каковы рамки их доступа: одна предметная область, множество предметных областей или все области;
- каким типом доступа они обладают, например, только чтение или возможность модификации.

Обычно процесс сбора и подготовки данных для BI-среды очень сложный и "непрочный". Огромное число источников данных и значительное разнообразие данных приводят к многоступенчатым процессам, в которых данных интерактивно собираются и преобразуются для загрузки в Хранилище данных. Данные, подвергающиеся как процессу сбора, так и преобразования, также образуются "точки риска". Для защиты информации необходимо знать:

- кто располагает доступом к средствам извлечения данных из операционных систем;
- где находятся данные, пребывающие в процессе сбора, перед тем как оказаться в Хранилище данных, и кто имеется доступ к этой области;

Следующим компонентом можно считать пользовательские средства запроса/отчёта и BI-приложения. BI-средства и аналитические приложения - это в первую очередь механизмы, предназначенные для доступа к данным в Хранилище данных. Такие средства часто приобретались в большом количестве с целью широкого и глубокого развертывания BI по всему предприятию. Эти инструменты представляют особую ценность только для конечного числа пользователей, и их нахождение в "не тех руках" представляет серьезную опасность. Необходимо рассматривать следующие аспекты защиты информации:

- кто располагает разрешением на использование средств запроса и отчёта;
- назначенли каждому пользователю личный ID;
- насколько свободно ваши клиенты и поставщики обмениваются предоставленной им информацией в рамках своих предприятий;
- предоставляют ли они ее своим внешним акционерам;
- не может ли эта информация попасть в руки ваших конкурентов.

Политика информационной безопасности является основным компонентам, которой стоит уделять особое внимание. Она часто не затрагивает информации, которая хранится, анализируется и поставляется посредством BI-приложений. Поскольку BI усиливает доступность к информации, часто передавая ее в непосредственное распоряжение бизнес-пользователей, информация быстро оказывается вне пределов инфраструктуры безопасности IT-отдела. Поэтому при формировании корпоративной политики информационной безопасности следующие решать следующие вопросы [4, 5, 11-14]:

- учитывает ли корпоративная политика безопасности специфику IT;
- определять области значительного риска, которые могут быть устранены посредством такой политики;
- рассматривать затрагивает ли правительственные постановления информацию, которая хранится, анализируется и представляется BI-среде.
- не нарушают ли текущие или планируемые BI-мероприятия эти постановления.

Таким образом, BI - среда, является единой системой отчётности и анализа и при внедрении становится "единым источником правды" в компании. Но такая информация, как оказалась подвергается множествам угроз, которые рассмотрены в данной статье. Учитывая и решая вопросы, которые были поставлены в данной статьеможно организовать достаточную защиту информации в среде Business Intelligence.

Литература

1. ГОСТ Р ИСО/МЭК 15408-3-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
2. ГОСТ Р ИСО/МЭК 27001 — «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования». Прямое применение международного стандарта — ISO/IEC 27001:2005.
3. ГОСТ Р 51898-2002 — Аспекты безопасности. Правила включения в стандарты.
4. Безбогов, А.А. Б391 Методы и средства защиты компьютерной информации : учебное пособие / А.А. Безбогов, А.В. Яковлев, В.Н.

Шамкин. – Тамбов : Изд-во Тамб. гос. техн. ун-та, 2006. – 196 с. – 100 экз. – ISBN 5-8265-0504-4.
5. Голиков А.М. Основы информационной безопасности: Учебное пособие для практических и семинарских занятий. – Томск: ТУСУР, 2007. – 154 с.
6. Соляной В.Н., Сухотерин А.И. Практика применения инновационного научно-образовательного комплекса по подготовке бакалавров и магистров в области информационной безопасности. Научно-практический журнал №25, том 1 2015г. Информационное противодействие угрозам терроризма. Материалы XIX Пленума учебно-методического объединения по образованию в области информационной безопасности «опыт и передовые практики образовательных организаций по формированию и использованию в учебном процессе специализированной учебно- лабораторной базы» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН.ФЕД.УНИВ, 2015.-416 с. ISSN 2219-8792
7. Соляной В.Н., Сухотерин А.И. Модульно-ориентированный подход формирования базовых дисциплин ФГОС ВО 3+ как основа реализации профессиональной подготовки бакалавров в области информационной безопасности Научно-практический журнал №25, том 2 2015г. Информационное противодействие угрозам терроризма Материалы XIX Пленума учебно-методического объединения по образованию в области информационной безопасности «учебно-методическое обеспечение образовательных программ в области информационной безопасности» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН.ФЕД.УНИВ, 2015.-332 с. ISSN 2219-8792
8. Соляной В.Н., Сухотерин А.И. Становление направления «Радиоэлектронная безопасность информационных объектов» в системе дополнительного профессионального по информационной безопасности. Научно-практический журнал №25, том 2 2015г. Информационное противодействие угрозам терроризма Материалы XIX Пленума учебно-методического объединения по образованию в области информационной безопасности «учебно-методическое обеспечение образовательных программ в области информационной безопасности» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН.ФЕД.УНИВ, 2015.-332 с. ISSN 2219-8792
9. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Некоторые перспективы применения систем контроля и управления доступом в региональных ВУЗАХ. Научная статья. «Перспективы

организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
10. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Развитие сотрудничества российских и зарубежных ВУЗОВ по защите информационного ресурса. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
11. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
12. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
13. Соляной В.Н., Сухотерин А.И Выработка коммуникативной компетенции при подготовке профессионалов по информационной безопасности с использованием технологии модерации. «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7

14. Соляной В.Н., Сухотерин А.И, Антоненко В.И. Проблемно-ориентированная подготовка специалистов по информационной безопасности с использованием имитационного метода (мозговой штурм). «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. – М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7.

УТОЧНЕНИЕ ТИПОВ ТЕСТИРОВАНИЯ IP СЕТЕЙ С ИСПОЛЬЗОВАНИЕМ АНАЛИЗАТОРОВ СЕТЕЙ

Тюрин Владислав Сергеевич, студент 3 курса кафедры Информационной безопасности.
Научный руководитель: **Журавлёв Сергей Иванович,** к.т.н., доцент кафедры Информационной безопасности

Основным составным компонентом, обеспечивающим надёжную работу любой сети, является проведение ее контроля и осуществление постоянного мониторинга. В настоящее время с этой проблемой успешно справляются сетевые анализаторы.

Сетевой анализатор - диагностическое средство широкого назначения, позволяющее измерять основные характеристики сигналов, оценивать качество каналов связи (в виде процента ошибочных кадров и т.п.), осуществлять функции мониторинга сети и проводить статистический анализ трафика.

Сетевой анализатор подключается к сети точно так же, как обычный узел. Однако в отличие от абонентских станций, ему доступен весь трафик сети, а не только тот, который адресован данному узлу. Но чтобы определить качество или слабые звенья сети, проводится тестирование.

Сеть, тест, анализатор.

CLARIFICATION OF IP NETWORK TESTING USING A TYPE OF NETWORK ANALYZERS

Tyurin Vladislav, 3rd year student of the Department of information security.
Scientific adviser: **Zhuravlev Sergey,** Candidate of Technical Sciences, Associate Professor of the Department of information security

The main component in the reliable operation of any network, it controls and constant monitoring. Currently, this problem successfully cope network analyzers.

Network Analyzer - Diagnostic tool of wide application, which allows to measure the basic characteristics of the signals to assess the quality of communication channels (as a percent error rate, etc.) to carry out network monitoring function and carry out a statistical analysis of the traffic.

A network analyzer is connected to the network in the same way as a normal node. However, in contrast to subscriber stations available to him the entire network traffic and not just the one that is addressed to this node. But in order to determine the quality or weak network units being tested.

Network test analyzer.

Для того чтобы анализировать или проводить тестирование IP сетей, нужно знать что такое стеки телекоммуникационных протоколов.

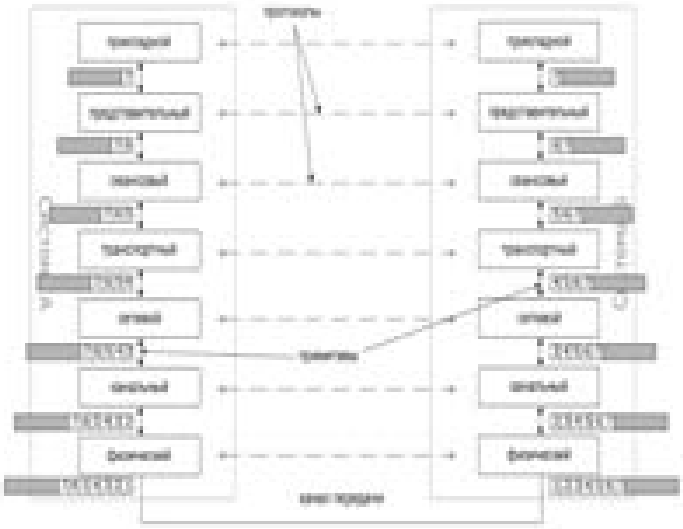


Рисунок 1 - Модель взаимодействия открытых систем. Протоколы и примитивы

Протоколы являются языком, на котором коммутационные узлы, станции и другие телекоммуникационные устройства общаются

в сети. В более формальной трактовке протоколом является согласованная система правил и процедур, которая дает описание принципа взаимодействия множественных объектов. На рисунке 1 представлена модель взаимодействия открытых систем и соответствующие механизмы взаимодействия между уровнями модели - протоколы и примитивы [1, 2, 5].

Данная модель показывает, что более низкий уровень всегда предоставляет услуги более высокому. Взаимодействие между разными уровнями одной системы осуществляется по средствам примитивов, а взаимодействие между одноименными уровнями разных систем по средствам протоколов Совокупность этих протокольных уровней называется стеком протоколов.

Итак, для тестирования протоколов сигнализации и обеспечения взаимодействия сетевых элементов в телекоммуникационной сети существует несколько методологий. Уточненная схема типов тестирования IP сетей представлена на рисунке 2.

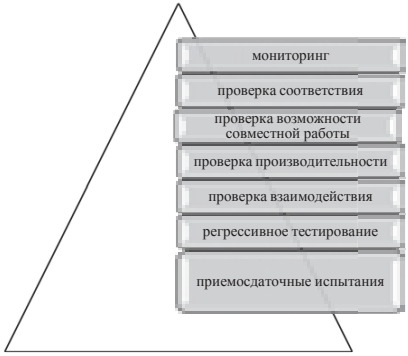


Рисунок 2 - Схема типов тестирования IP сетей

Каждый из этих механизмов проверок гарантирует подтверждение соответствия протокола требованиям, предъявляемым на той или иной стадии жизненного цикла IP сетей. Далее уточним содержание отмеченных типов тестирования IP сетей.

Тестирование соответствия

Первым этапом в тестировании протокола является обеспечение того, чтобы он работал в соответствии со спецификацией, на основе которой он был создан. Этот процесс называется проверкой согласованности. На практике, роль проверки согласованности заключается в том, чтобы увеличить уверенность в том, что протокол

соответствует своей спецификации, и уменьшить риск неправильного срабатывания.

Проверка согласованности представляет собой хорошо отлаженную методологию тестирования, основанную на международном стандарте ISO 9646. Главная идея стандарта ISO 9646 состоит в том, что спецификация нового протокола должна содержать комплект тестовых сценариев его проверки. Тестирование на соответствие заданной спецификации является единственным стандартизированным и широко распространенным методом проверки корректности реализации протокола. Этот метод основан на применении специализированного языка написания тестов TTCN.

Тесты соответствия включают в себя проверку корректности работы протокольных объектов, т. е. соблюдения очередности следования сообщений, правильности перехода объектов из одного состояния в другое под воздействием определенных внешних событий, кодировки обязательных информационных элементов [1, 2, 4].

Тестирование производительности

Одно лишь тестирование на соответствие не может гарантировать корректность реализации протокола полностью, так как не предполагает проведение тестирования под нагрузкой и проверку поведения системы при неопределенных значениях параметров спецификации, оставленных для возможного применения в будущем. При тестировании производительности измеряются те параметры, которые зависят от поступающей на систему нагрузки, и производится их сравнение с допустимыми значениями (например, измерение интенсивности потерь вызовов). Этот вид тестирования сводится к измерению параметров качества обслуживания (QoS) или производительности сети (NP, Network Performance) при известных значениях параметров поступающей нагрузки.

Тестирование производительности производится с использованием эталонной системы (что не всегда возможно и дорого) или с использованием системы тестирования, имитирующей эталонную систему. Для имитации эталонной системы, с которой должно стыковаться тестируемое оборудование, используются симуляторы протоколов и генераторы вызовов. При использовании реальной системы в качестве эталонной применяются анализаторы протоколов, осуществляющие мониторинг интерфейса, который соединяет тестируемую систему с эталонной. Для измерения значений параметров QoS и NP используются генераторы вызовов

(сигнального трафика), создающие нагрузку определенного вида на тестируемую систему посредством генерации последовательностей сообщений определенного протокола и измеряющие значения интенсивности потерь вызовов, интенсивности появления ошибок протокола, интервалы времени между передачей и приемом сообщений (таймеры) и т. п.

Тестирование совместимости

Тестирование возможности совместной работы является следующим логическим этапом после выполнения проверок согласованности и производительности. Спецификация протокола нередко содержит области неоднозначного понимания, подверженные различной интерпретации разработчиками и, следовательно, различной реализации. Такими областями спецификации являются опциональные процедуры и параметры, разные значения параметров и величины таймеров.

Тестирование совместного функционирования является ключевым аспектом для сетевых операторов, эксплуатирующих оборудование разных производителей. Очевидно, что сетевые элементы одного производителя должны корректно работать с сетевыми элементами другого производителя. Проверка этой возможности может проводиться в лабораторных условиях или непосредственно в сети оператора.

На этапе тестирования совместного функционирования проверяется, в какой степени и при каких условиях разные реализации одного и того же протокола могут совместно работать, производя ожидаемый результат. Тесты этого вида могут применяться как ко всем протоколам стека, используемого на интерфейсе, так и к какому-либо одному выбранному протоколу.

Тестирование взаимодействия

Тестирование взаимодействия разных протоколов и систем сигнализации приобретает важное значение для современных телекоммуникационных сетей. Тестирование взаимодействия охватывает весь процесс обслуживания вызова и предоставления дополнительных услуг. Иными словам и тестирование взаимодействия является итоговым тестированием, обеспечивающим проверку функционирования системы в целом. Цель тестов взаимодействия показать, что функциональность из конца в конец между двумя связанными системами отвечает требованием стандартов, на которых эти системы основаны. Как показывает

практика, проведение тестов взаимодействия существенно увеличивает вероятность того, что в одной сети будет успешно взаимодействовать оборудование, выпущенное разными производителями.

Регрессионное тестирование

Редко бывает, чтобы только одна версия программного обеспечения узла коммутации работала в течение его жизненного цикла. Последующие программные версии, как правило, включают зафиксированные и исправленные ошибки программирования, усовершенствования, новые функции, дополнительные услуги и т. д. Регрессивное тестирование является методикой, обеспечивающей по мере развития и замены версий программного обеспечения надлежащее мигрирование ранее оттестированных протокольных реализации IUT.

Приемосдаточные испытания

Приемосдаточные испытания объединяют серию стандартных тестов, определяемых программой и методиками приемосдаточных испытаний. Обычно эти тесты выполняются на сети Оператора после того, как телекоммуникационное оборудование установлено, смонтировано и запущено. Приемосдаточные испытания могут включать регрессивное тестирование каждый раз, когда устанавливается новая версия программного обеспечения с новыми функциями или градациями емкостей.

Мониторинг

Мониторинг телекоммуникационных протоколов является не только последней фазой тестирования протоколов, но и самой длительной и, пожалуй, самой важной [1, 4].

Мониторинг интерфейса между находящимися в эксплуатации сетевыми элементами обеспечивает:

- выявление ошибок при взаимодействии протоколов, не обнаруженных на других этапах тестирования;
- обнаружение несанкционированного доступа к ресурсам со стороны отдельных абонентов;
- сбор информации о вызовах (CDR) и транзакциях (TDR);
- трассировку вызовов;
- обнаружение зацикливания сообщений;
- контроль источников и маршрутов прохождения трафика.

Системы мониторинга и анализа сигнализации декодируют принимаемые от многочисленных каналов сети сигнализации

сообщения и сигналы, проверяют их на предмет соответствия заданной спецификации, выделяют (как правило, красным цветом) сообщения или их отдельные параметры, не соответствующие спецификации, точно таким же образом они отображают перегрузки, аварийные ситуации и многое другое.

Одним из технических средств для тестирования сети можно представить сетевой анализатор Fluke OptiView xg (рисунок 3).

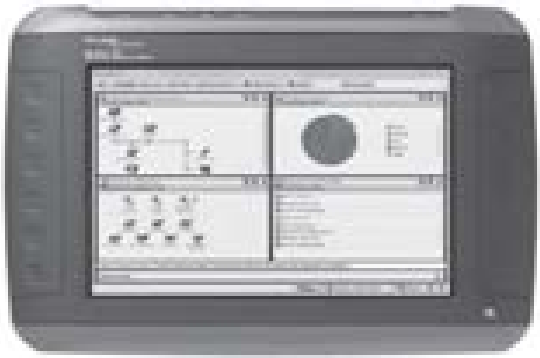


Рисунок 3 - Сетевой анализатор Fluke OptiView xg

Представленный сетевой анализатор позволяет специалистам анализировать любые показатели в любом участке сети, в любое время. Благодаря автоматизации глубокого анализа причин неполадок сети и приложений сетевые специалисты могут значительно сократить время выполнения повседневных задач. При этом специалисты могут больше времени уделить реализации новых проектов [3, 4].

Проводя тестирование с использованием анализаторами сетей, мы можем проверять сеть по следующим параметрам: проверка соответствия, проводить мониторинг, проверять возможности совместной работы, проверять производительности, проверять взаимодействия, проводить регрессивное тестирование и проведение приемосдаточных испытаний. Все эти типы тестов позволяют максимально оптимизировать работу сети.

Литература

1. Сетевые анализаторы IP сетей : учебное пособие / Б. С. Гольдштейн, В. Ю. Гойхман, Ю. В. Столповская ; СПбГУТ. – СПб., 2013. – 56 с.

2. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей, Платонов В.В. М.: Издательский центр "Академия", 2006. — 240 с.
3. Компьютерные сети: учебник для студ. учеб . заведений: в 2 т. Т. 2. Сети ЭВМ/Р.Л. Смелянский. - М.: Издательский центр "Академия", 2011. - 240с.
4. Журавлев С.И., Мирсаитов Р.С. Один из подходов статистического анализа защищенного трафика ведомственных IP-сетей. Статья в журнале «Двойные технологии» № 1, 2015, с. 34-39.
5. [Электронный ресурс]. Режим доступа: http://www.protehnology.ru

ОСНОВНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ ЗАЩИТЫ СОВРЕМЕННОГО КРИПТОВАЛЮТНОГО ОБОРОТА

Унич Евгений Владимирович, студент 1 курса кафедры Информационной безопасности
Научный руководитель: **Соляной Владимир Николаевич**, к.воен.н., доцент, заведующий кафедрой Информационной безопасности

Одной из новаций последнего времени стало появление особого вида валют, который получил название «криптовалюта». Данный феномен привлекает к себе особое внимание, при этом большинство изучающих ее людей в основном рассматривают технические аспекты обращения криптовалют.

Информационная безопасность, криптовалюта, защита информации.

THE MAIN PROBLEMS OF INFORMATION PROTECTION MODERN CRYPTOCURRENCY TURNOVER

Unich Evgeny, 1st year student of the Department of information security
Scientific adviser: **Solyanoy Vladimir,** Candidate of Military Sciences, Associate Professor, Head of the Department of information security

One of the innovations of recent times is the emergence of a special type of currency, which was named "cryptocurrency". This phenomenon has attracted special attention, with the majority of people studying it basically consider the technical aspects of handling cryptocurrenc.

Information security, cryptocurrency, protection of information.

На сегодняшний день в мире существует более 500 видов криптовалют, общая капитализация которых на 1 октября 2014 года составляла 5,4 млрд. долл. США. Самое большое распространение получил Bitcoin (6,8 млрд. долл. На 15.12.2015, больше чем стоимость абсолютно всех видов год ранее).

Сравнительный анализ курса криптовалюты Bitcoin и золота свидетельствует о том, что уже в середине 2013 года курсы сблизились (в конце 2015 Биткоин стоит в 10 раз дороже), что позволило говорить о Bitcoin как об «электронном золоте».

Разработчики криптовалюты Bitcoin, функционирование которой основано на принципах пиринговых сетей, за последнее время выпустили ряд критических обновлений безопасности клиента, направленные на исключение неправомерного использования средств на счетах пользователей. Необходимость подобных «заплаток» стала очевидна после относительно недавнего взлома крупнейшей биржи по обмену денежных знаков Mt Gox. Добычей злоумышленников стали данные и хешированные пароли более 62 000 пользователей сети Bitcoin, а обменный курс резко упал с 17 долларов до ноля (а точнее - до 0,01$ по информации mtgoxlive.com). Злоумышленникам удалось подобрать пароль к одной из административных учётных записей биржи Mt Gox, что предоставило им возможность совершить транзакцию в размере 432 000 BTC (платёжных единиц системы Bitcoin), и по курсу на момент взлома их стоимость оценивалась в 8 млн долларов США. Учитывая, что в свободном обращении, на тот момент, находилось около 7 млн. «монет» BTC, неизвестным хакерам были подконтрольны около 6% всей платёжной системы [1-10].

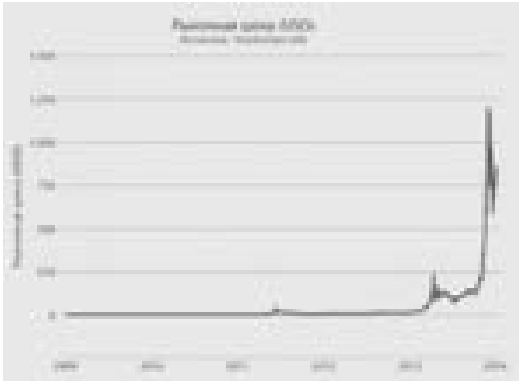


Рисунок 1 - Курс Биткоина с 2009 по 2014 г.

После такого случая необходимость защиты данного вида валюты стала ясна как никогда, так как при малейшем нарушении безопасности криптовалюты ее ценность падает от огромных чисел почти до нуля и если такое случается, то большое количество людей теряют свои деньги.

На рис. 2 можно увидеть, как осуществляется перевод денег. В Bitcoin вся информация хранится в цепочке блоков. Каждый блок содержит заголовок и список транзакций. Заголовок состоит из нескольких свойств, среди которых есть хэш предыдущего блока. Таким образом вся цепочка блоков хранит все транзакции за все время работы Bitcoin. Из этого следует вывод, что обмануть систему в данном месте попросту невозможно, следовательно рассматривать его больше нет смысла [1-10].

Для того, чтобы распоряжаться своими криптовалютными ресурсами нужно использовать специальное программное обеспечение, например Bitcoin Core, официальный клиент биткоин сети. Стоит рассмотреть его подробнее, так как именно в этом месте вводятся все данные пользователя и это наиболее уязвимое для взлома место. Идея самой системы состоит в том, что каждая транзакция необратима и подтверждается вновь генерируемыми блоками, отвечающим определенным требованиям. Эти блоки вычисляются всем сообществом, объединяются в цепочку и доступны всем для просмотра в виде единой базы данных. Процедура вычисления блоков называется майнинг. Сеть построена таким образом, что один блок находится с определенной периодичностью, независимо от вычислительных мощностей, — то есть сложность вычислений саморегулируется. При этом, пока сеть растет, каждый вновь сгенерированный блок содержит еще и новые монеты.

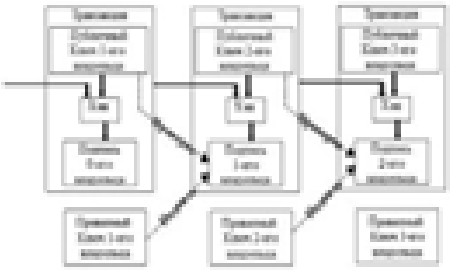


Рисунок 2 - Схема работы транзакций

В случае с Bitcoin и еще некоторыми видами криптовалют количество монет, которые могут находиться в обращении, ограничено на уровне протокола, и количество вновь добываемых монет постепенно уменьшается в геометрической прогрессии так, что оно никогда не превысит заданного лимита. Каждый пользователь, который сгенерировал блок, получает фиксированную награду, а также комиссию транцакций, которые он подтвердил, включив их в блок. То есть саму систему обмена и хранения криптовалюты взломать невозможно из-за огромного количества блоков, которое постоянно увеличивается, значит остаются варианты с кражей средств определенных людей или компаний, посредством доступа к их данным [1-10].

Казалось бы, протокол OpenSSL должен предоставлять неразрушимую защиту для файлов и ресурсов клиента. Так оно и есть, до тех пор, пока злоумышленник не получит одновременно доступ к файлу кошелька и к ключам от него. Первое серьёзное улучшение безопасности по сравнению с базовой версией было реализовано в релизе Bitcoin 0.4.0, выпущенном 23 сентября 2011 года. С этого момента всем владельцам BTC стало доступно шифрование файла кошелька, а вернее той его части, в которой содержится клиентская часть открытого ключа, передаваемая контрагенту при совершении перевода. При выполнении любых операций с имеющейся криптовалютой требуется ввод пароля, что делает невозможным использование украденных файлов кошельков. Однако, при утере пользователем пароля от кошелька, восстановление контроля над ним невозможно. То же самое относится и к утере самого файла. Именно поэтому при использовании Bitcoin необходимо надёжно хранить пароли и делать резервные копии кошелька.

Рисунок 3 - Интерфейс программы Bitcoin Core

Также версия клиента 0.4.0 предлагает пользователям более оптимизированное строение древовидной системы хэшей и базы данных с поддержкой защиты от атак типа denial-of-service (отказ в обслуживании). На первый взгляд, пиринговой сети не стоит опасаться DDoS-атак, ведь в структуре Bitcoin отсутствует главный пул серверов, нет каких либо сервисов, представляемых пользователям централизованно. Но основное достоинство распределённой сети – полная децентрализованность, в ряде случаев может быть и самым серьёзным недостатком, особенно если злоумышленник пытается получить доступ одновременно к большому количеству кошельков участников системы, например, использовав бот-сети (связанные между собой компьютеры, которыми может управлять один человек) [1-10].

Эта вероятность также исключена, потому что в сети Биткоин находится огромное количество компьютеров и для того, чтобы получить контроль над ней с помощью бот-сети нужна мощность в тысячи раз больше, чем у современных суперкомпьютеров, а построить такую сеть с помощью вирусов очень сложно, так как они легко блокируются антивирусами и даже стандартным фаерволлом

Вышеизложенные положения определили основные проблемы в области защиты криптовалютного оборота.

Первой проблемой следует рассматривать защиту от вредоносного ПО и вирусов, нацеленные на Bitcoin-кошельки. Это широко используемый метод кражи личной информации, довольно опасен, работает далеко не только с криптовалютой. При использовании такого метода, злоумышленник прикладывает все усилия, чтобы его файлы попали на компьютер человека, хранящего нужные ему данные. После скачивания, эти файлы пытаются найти на компьютере файл wallet.dat. Так как в этом файле содержатся личные ключи, отвечающие за доступ к биткоинам, хакер старается его заполучить.

Важно защитить Bitcoin-кошелек хорошим паролем, как минимум из 15 символов в разном регистре вперемешку с цифрами. Таким образом, хакерам будет сложнее получить данные из файла wallet.dat. Еще один хитрый метод заключается в специальном вредоносном ПО, которое находится на компьютере в состоянии сна, и запускается только когда пользователь копирует Bitcoin-адрес. В этот момент ПО тут же заменяет скопированный адрес на адрес злоумышленника, и получается, что вы отправляете средства на его

адрес. Наконец, существует такой тип «вымогательского» вредоносного ПО, которое блокирует компьютер, и обещает разблокировать его только после того, как вы отправите определенную сумму биткоинов на указанный адрес. Это очень продвинутый способ, так как такое ПО практически невозможно удалить. Однако, компьютер действительно разблокируется, как только вы отправите выкуп.

Это очень эффективный метод для злоумышленников, так как, опять же, все транзакции проходят анонимно, и отследить получателя практически невозможно. Пожалуй, единственная хорошая защита от всех этих методов – это комплект из хорошего антивируса и аккуратное использование сети интернет.

Второй проблемой следует рассматривать защиту от использования другого метода фишинга. При этом методе хакер создает клон сайта, когда пользователь открывает его и вводит данные логина и пароля, эта информация высылается хакеру, который тут же ворует деньги. Следовательно, перед тем, как вводить данные, важно проверить домен и информацию на сайте. К примеру, посещая blockchain.info, нужно всегда проверять содержимое ssl-сертификата. Также, поможет использование разных логинов и паролей на разных сайтах. Вдобавок, можно активировать двухфакторную аутентификацию в Bitcoin-сервисах, - это позволит оградиться от большинства хакеров, поэтому данный способ опасен только при невнимательном ипользовании биткоин-кошельком

Третьей проблемой следует рассматривать защиту Онлайн-обменников или интернет-сервисов для управления кошельком Bitcoin, которые также могут подвергнуться хакерской атаке. Это самая большая угроза для рядового пользователя и для сети в целом. Для пользователя опасность состоит в том, что избежать подобного можно только пользуясь надежными сервисами, а до первого взлома узнать надежность сервиса довольно сложно. Для сервиса же опасность состоит в том, что он будет потерян для владельца, никто просто не будет пользоваться его сайтом после первого же большого взлома.

Так же возможна физическая кража криптовалюты, например злоумышленник может считать оставленный где-то QR-код, украсть резевные копии или даже листок с записанным на нем паролем, поэтому основной проблемой защиты криптовалюты останется человеческая лень, неосведомленность и невнимательность, так как

она является причиной почти всех взломов, от маленьких кошельков, до краж миллионов долларов.

Таким образом, в данной статье были получены следующие результаты:

1. Проведенный анализ уязвимостей криптовалюты показал, что существуют некоторые опасности ее потери при недостаточном уровне осведомленности пользователя

2. Наиболее значимыми проблемами защиты хранилищ криптовалюты стоит считать:

a. Использование злоумышленником вредоносного ПО и вирусов

b. Создание злоумышленником фишинговых сайтов

c. Взлом онлайн-обменников или сервисов для управления кошельками

3. Наиболее эффективным способом обеспечения безопасности будет выбор доверенных хранилищ, использование антивируса и внимательность при посещении сайтов, требующих реквизиты кошелька.

Литература

1. Малюк А.А. Введение в информационную безопасность: Учебное пособие для вузов / В.И.Королёв, В.М. Фомичев. – М.: Горячая линия- телеком, 2013.

2. Петренко С.А. и Курбатов В.А. Политики безопасности компании при работе в интернет / М.: ДМК Пресс, 2011.

3. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.

4. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский

Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
5. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Развитие сотрудничества российских и зарубежных ВУЗОВ по защите информационного ресурса. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международная научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
6. Учебное пособие для вузов/ Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. – М.: Горячая линия – Телеком, 2006. – 544 с.
7. [Электронный ресурс]. Режим доступа: http://bitkurs.ru
8. [Электронный ресурс]. Режим доступа: http://bits.media/bitcoin-core
9. [Электронный ресурс]. Режим доступа: http://habrahabr.ru/post/119749
10. [Электронный ресурс]. Режим доступа: http://www.profvest.com.

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ

Хромова Кира Геннадьевна, Попова Полина Михайловна,
студентки 3 курса кафедры Информационной безопасности
Научный руководитель: **Сухотерин Александр Иванович,** к.воен.н.,
доцент кафедры Информационной безопасности

В данной работе рассматривается правовой документ – Концепция информационной безопасности детей. В статье определенны основные проблемы в области обеспечения информационной безопасности детей, цели и задачи Концепции. В результате анализа данного документа были выявлены и усовершенствованны пробелы в законодательной базе, а так же представлены предполагаемые результат его реализации.

Концепция, ключевые проблемы информационной безопасности детей, интернет, законодательная база, ожидаемый результат.

MODERN PROBLEMS OF INFORMATION SECURITY OF CHILDREN

Khromova Kira, Popova Polina, 3rd year studenst of the Department of information security
Scientific adviser: **Sukhoterin Alexander**, Candidate of Military Sciences, Associate Professor of the Department of information security

This project concerns such a legal document as the Concept of the information security of children. the main problems in the sphere of ensuring the information security of children, the goals and objectives of the Concept are identified in this article. As the results of the analysis of this document the gaps in the legal framework have been identified and improved, moreover, the anticipated results of its implementation are presented.

The concept, key issues of the information security of children, the Internet, the legislative framework, the expected result.

Потребность в информации — одна из базовых естественных потребностей человека, не менее важная, чем потребности физиологические — еда, сон, тепло и т. д. С самых древних времен человек искал и создавал информацию об окружающем мире, прошел гигантский путь от мифа до научной картины мира. Любая человеческая деятельность неразрывно связана с обменом информацией [1-9].

Раз информация неизбежно оказывает воздействие на человека, значит, она должна фильтроваться. Если взрослый человек справляется с этой задачей (и то не всегда и не каждый), то ребенок этого делать еще не умеет. А значит, он нуждается в защите своего информационного окружения со стороны взрослых людей.

Процесс социализации через традиционные институты (семьи, школы) все активнее дополняется средствами массовой информации и массовых коммуникаций, особенно информационно - телекоммуникационной сетью "Интернет". Следовательно, вопросы связанные с выявлением и поиском путей решений современных проблем информационной безопасности является актуальным [1-9].

Обосновать актуальность данного вопроса и сформулировать основные проблемы, связанные с информационной безопасностью детей, можно с помощью статистических данных, которые в общем виде покажут нам медиапотребление подростков.

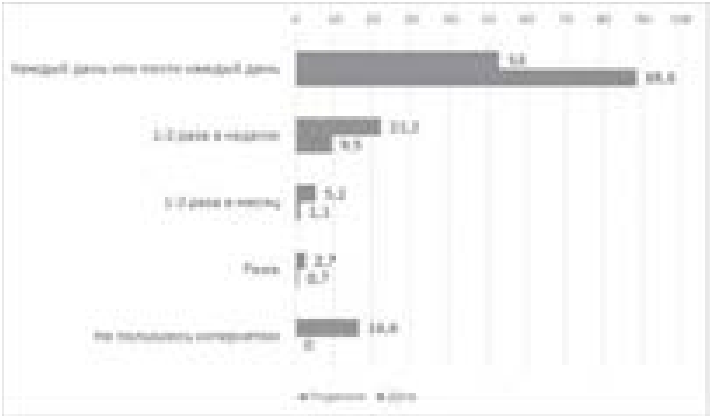


Рисунок 1 - Частота потребления Интернета детьми и взрослыми, % [2]

Проанализировав данные, представленные на рисунке 1, мы можем говорить о том, что подростки достаточно большое количество времени проводят в Интернете (ежедневно), а так же можно заметить, что среди опрошенных детей не оказалось тех, кто не пользуется интернетом вообще.

Рисунок 2 - Возрастные различия в использовании Интернета подростками, % [2]

В соответствии с информацией, которая отображена на рисунке 2, мы можем сказать, что с увеличением возраста подростка потребности в использовании Интернета увеличивается. Следовательно, такая динамика увеличения может говорить о том, что родители начинают меньше контролировать своих детей в данной области [1-9].

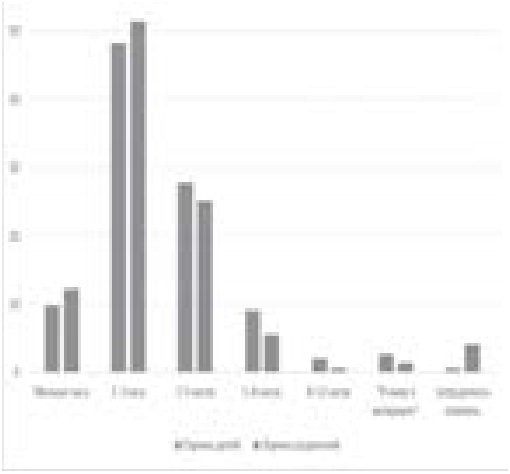


Рисунок 3 - Время детей в Интернете в будни – сравнение оценок детей и родителей, % [2]

По сравнительным оценкам детей и их родителей, представленные на рисунке 3 и рисунке 4, можно сказать, что в будние дни подростки проводят меньше временив сети Интернет (1-3 часа), нежели в выходные дни (3 – 5 часов).

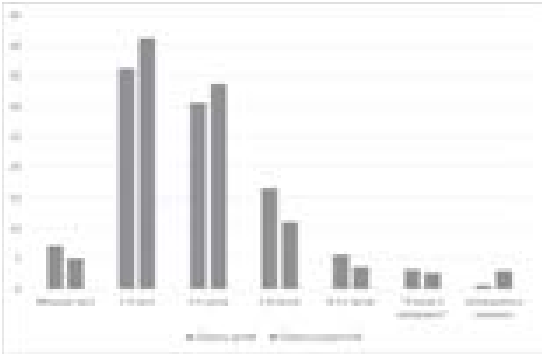


Рисунок 4 - Время детей в Интернете в выходные – сравнение оценок детей и родителей, % [2]

Проанализировав все данные, которые были представлены выше, можно сформулировать современные проблемы информационной безопасности детей.

К ним можно отнести:

- потеря родительского авторитета;

- отклонения в физическом развитии (избыточный вес, нарушения
сна, проблемы со зрением);
- негативные эмоциональные состояния (страх, ужас, паника, тревога);
- киберзависимость (привыкание к online-играм, интернету);
- проблемы, связанные с сексуальным поведением (установление
подростками беспорядочных связей благодаря сомнительным сайтам знакомств);
- поведение, связанное с риском для жизни или опасное для здоровья (психическая анорексия, суицидальное поведение, потребление психотропных препартов, легкодоступных для приобретения посредством специальных сайтов) [3].

Для решения данных проблем и улучшения качества медиасреды была принята Концепция информационной безопасности детей, утвержденная распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р, которая является правовым документов, обеспечивающим защиту детей от информации, причиняющей вред их здоровью и развитию.

В Концепции дается определение понятию «информационная безопасность детей» - это защита ребенка от дестабилизирующего воздействия информационной продукции и создание условий информационной среды для позитивной социализации и индивидуализации, оптимального социального, личностного, познавательного и физического развития, сохранения психического и психологического здоровья и благополучия, а так же формирование позитивного мировосприятия [1].

Основной целью государственной политики в области информационной безопасности детей является обеспечение гармоничного развития молодого поколения при условии минимизации всех негативных факторов, связанных с формированием гиперинформационного общества в России.

Обеспечение информационной безопасности детей возможно исключительно при условии эффективного сочетания государственных и общественных усилий при определяющей роли семьи [1].

Важнейшей задачей является налаживание согласованного взаимодействия семьи с государством и всеми элементами

современного медиарынка - производителями и распространителями контента, психолого-педагогическими экспертными сообществами и экспертными сообществами в области художественного образования. Только тесное сотрудничество всех участников медиаиндустрии позволит построить эффективную систему регулирования потребления информационной продукции, максимально безопасную для психического и физического развития и здоровья подрастающего поколения [1].

Проанализировав основные задачи и цели данной Концепции, можно сформулировать пути решения существующих проблем.

К ним относят:

- формирование у детей навыков самостоятельного и ответственного потребления информационной продукции;
- повышение уровня медиаграмотности детей;
- формирование у детей позитивной картины мира и адекватных базисных представлений об окружающем мире и человеке;
- ценностное, моральное и нравственно-этическое развитие детей;
- развитие системы социальных и межличностных отношений и общения детей;
- удовлетворение и развитие познавательных потребностей и интересов ребенка, детской любознательности и исследовательской активности;
- формирование у детей чувства ответственности за свои действия в информационном пространстве [1].

Важную роль в регулировании потребления информации детьми и подростками, а так же формирование у них критической оценки получаемых сведений играют их родители.

Усилия семьи, общества и государства должны быть направлены на то, чтобы ребенок с детства привыкал свободно ориентироваться в медиапространстве, умел взаимодействовать с различными источниками информации, не поддавался манипуляциям извне и мог делать самостоятельные выводы о качестве информационных продуктов [1].

Так же необходимо затронуть вопрос, связанный с совершенствованием законодательной базой в области информационной безопасности детей. В таблице 1 представленные

федеральные законны и дополнения, которые необходимо внести в существующую законодательную базу [4].

Таблица 1 - Совершенствование норм федеральных законов Российской Федерации

Федеральные законы (ФЗ)	Совершенствованию норм ФЗ
Федерального закона от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»	1. Дополнить часть 2 статьи 4 Федерального закона № 436-ФЗ нормой, предусматривающей меры государственной поддержки оборота, в том числе производства и распространения информационной продукции, предназначенной для детей, на федеральном, региональном и местном уровнях [4]. 2. Дополнить совокупность закреплѐнных в части 3 статьи 6 и статьях 7 -Федерального закона № 436-ФЗ категорий информационной продукции категорией «Универсальная», к которой отнести информационную продукцию, не причиняющую вред здоровью и развитию детей, допускаемую для оборота без ограничений среди потребителей любых возрастных групп и не подлежащую обязательной маркировке [4]. 3. Внести в статью 19 Федерального закона № 436-ФЗ дополнения, направленные на регламентацию в законодательном порядке правовых последствий экспертизы информационной продукции, содержащей информацию, причиняющую вред здоровью и развитию детей, для производителей и распространителей указанной информационной продукции [4].
Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	1. Подпункт «б» части 5 статьи 15.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» после слов «наркосодержащих растений» дополнить словами «, а также пропаганды или незаконной рекламы наркотических средств, психотропных веществ или их прекурсоров, растений, содержащих наркотические средства или психотропные вещества либо их прекурсоры, и их 13 частей, содержащих наркотические средства или психотропные вещества либо их прекурсоры» [4].
Кодекс об административных правонарушениях Российской Федерации	1. Внести в статьи 6.13 КоАП РФ дополнительную часть 2 следующего содержания: «Распространение информации о способах, методах разработки,изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, о способах и местах культивирования наркосодержащих растений….» [4].

Реализация Концепции обеспечит формирование в Российской Федерации поколения молодых граждан, которые смогут свободно и самостоятельно ориентироваться в современном информационном

пространстве. Будет создана новая медиасреда, соответствующая следующим характеристикам:

- наличие развитых информационно-коммуникационных механизмов, направленных на социализацию молодого поколения и раскрытие его творческого потенциала;
- свободный доступ детей к историко-культурному наследию предшествующих поколений;
- качественный рост уровня медиаграмотности детей;
- увеличение числа детей, разделяющих ценности патриотизма;
- гармонизация меж- и внутрипоколенческих отношений;
- популяризация здорового образа жизни среди молодого поколения;
- формирование среди детей устойчивого спроса на получение высококачественных информационных продуктов;
- снижение уровня противоправного и преступного поведения среди детей;
- формирование у детей уважительного отношения к интеллектуальной собственности и авторскому праву, сознательный отказ от использования "пиратского" контента [1].

Руководитель Роскомнадзора. Александр Жаров, подчеркнул, что документ ориентирован не только на детей, но также и на их родителей. Государство лишь задает общие рамки регулирования, однако наиболее важным участником в этом процесса являются взрослые, которые сами должны определять, что можно, а что нельзя смотреть их ребенку.

Влияние Интернета на детей и информационная безопасность в XXI веке — тема огромная. К сожалению, логика родителей, которые считаю, что если их ребенок находится дома, то он в безопасности, все еще чересчур популярна. Это глубоко ошибочная логика, ведущая к серьезным последствиям. Под угрозой психика ребенка, его образ мышления, его жизненные ценности. Одним словом, под угрозой то, что делает человека человеком.

Литература

1. Концепция информационной безопасности детей, утверждена распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р.

Раздел 2. Анализ потребления детьми и подростками информационной продукции, распространяемой в теле- и радиопередачах, теле- и радиопрограммах, сетевых средствах массовой информации, печатных средствах массовой информации, информационной продукции, распространяемой посредством сети Интернет.

2. Концепция информационной безопасности детей, утверждена распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р.

Раздел 4. Методология Концепции информационной безопасности детей и подростков.

3. Концепция информационной безопасности детей, утверждена распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р.

Раздел 13. Предложения по совершенствованию нормативно-правовых актов Российской Федерации в сфере информационной безопасности детей.

4. Федерального закона от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

5. Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Соляной В.Н., Сухотерин А.И., Воронов А.Н. Развитие сотрудничества российских и зарубежных ВУЗОВ по защите информационного ресурса. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» При поддержке Посольства Туркменистана в Российской Федерации. Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.

6. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.

7. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация

менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
8. Соляной В.Н., Сухотерин А.И Выработка коммуникативной компетенции при подготовке профессионалов по информационной безопасности с использованием технологии модерации. «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7
9. Соляной В.Н., Сухотерин А.И, Антоненко В.И. Проблемно-ориентированная подготовка специалистов по информационной безопасности с использованием имитационного метода (мозговой штурм). «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7.

СОЗДАНИЕ ПРИКЛАДНОГО ПРОГРАММНОГО КОМПЛЕКСА ПРОГНОЗИРОВАНИЯ ПЕРЕМЕЩЕНИЯ НАРУШИТЕЛЯ

Цвырко Снежана Олеговна, студентка 2 курса кафедры Информационной безопасности, **Бессонов Александр Владимирович**, студент 4 курса кафедры Информационной безопасности
Научный руководитель: **Соляной Владимир Николаевич**, к.воен.н., доцент, заведующий кафедрой Информационной безопасности

Решение задачи незаконного проникновения на заданную охраняемую территорию: расчёт и демонстрация области, в которой предполагаемо находится нарушитель в конкретно взятый момент времени. Выполняются цели: повышение эффективности перехвата злоумышленника, снижение ожидаемого ущерба за счет моделирования оптимальных действий охраны. В результате создан авторский алгоритм построения области предполагаемого

нахождения и прогнозирования перемещения нарушителя на территории, разработан программный комплекс, ведутся разработки полной реализации алгоритма с учетом новых факторов: наличия действий охраны, учетом перемещений нескольких групп нарушителей, оптимизации учитываемой обстановки.

Проникновение, программный комплекс, прогнозирование перемещения.

CREATING APPLICATION SOFTWARE PACKAGE FORECASTING OFFENDER MOVEMENT

Tsvyrko Snezhana, 2nd year student of the Department of information security, **Bessonov Alexander,** 4th year student of the Department of information security
Scientific adviser: **Solyanoy Vladimir,** Candidate of Military Sciences, Assistant Professor, Head of the Department of information security

Solution of the problem of illegal entry on a given protected area: the calculation and demonstration area, which the offender is supposed to be in a given time. Our purposes: improving the efficiency of interception attacker, reducing the expected losses due to the optimal simulation of protection. As a result, the authors created an algorithm for constructing the area involves finding and predicting movement in the territory of the offender, it has developed a software complex, being developed full implementation of the algorithm, taking new factors: the availability of protection, taking the movement of several groups of offenders accounted optimization environment.

The invasion, the software system, the outlook of movements.

В работе решается одна из ключевых задач успешного функционирования критического объекта - быстрая, эффективная защиты от возникающих угроз, среди которых следует особо выделить незаконные действия физических лиц: на заданную охраняемую территорию защищаемого критического объекта происходит незаконное проникновение; требуется рассчитать и продемонстрировать область, в которой предполагаемо находится злоумышленник в конкретно заданный момент времени в интересах обоснования оптимальных путей передвижения оперативных групп реагирования.

Последствия их воздействия непредсказуемы и широко варьируются: от хищения имущества предприятия до создания чрезвычайных ситуаций на защищаемом критическом объекте. В этих условиях безопасность предприятия должна отвечать принципам «разумной достаточности», «эффективность – стоимость», а также теоретически разработанной и практически применяемой концепции физической безопасности предприятия.

Решаются ключевые цели: повышение эффективности перехвата злоумышленника, снижение ожидаемого ущерба (рисков) от нарушителей за счет моделирования оптимальных действий служб безопасности и разработка прикладного программного комплекса.

Научная новизна проекта заключается в применении методов хромоматематики, использовании зонно-рубежного отображения перемещения злоумышленника и рекурсивных алгоритмов оптимизации. Также имеются большие перспективы коммерциализации (практическая значимость): возможно создание ППО с целью улучшения эффективности систем физической защиты критически важных объектов, поскольку существующие программные средства по ряду параметров уступают предложенной разработке; планируется выход на рынок систем охраны.

Введем понятие «нарушитель». Нарушитель – лицо или группа лиц, которые в результате предумышленных или непредумышленных действий обеспечивает реализацию угроз информационной безопасности [6].

Приказом министерства промышленности и энергетики РФ от 04.05.2007 №150 «Об утверждении рекомендаций по антитеррористической защищенности объектов промышленности и энергетики» определены шесть различных типов нарушителей:

1. Внешний нарушитель первого типа: террористическая группа численностью 5-12 человек. Цель: совершение террористического акта. Последствия выходят за рамки федеральной, региональной или территориальной зон ЧС.

2. Внешний нарушитель второго типа: малочисленная группа лиц (2-4 человека). Цель: совершение террористического акта. Последствия: выходят за пределы санитарной зоны объекта.

3. Внешний нарушитель третьего типа: одиночный подготовленный нарушитель, не имеющий санкционированного доступа на территорию объекта. Данный тип действует под

принуждением или воздействием психотропных препаратов. Цель: террористический акт.

4. Внешний нарушитель четвертого типа: одиночный нарушитель, не имеющий санкционированного доступа на территорию объекта, имеющий целью хищение материальных ценностей (похититель).

5. Внутренний нарушитель пятого типа: работник объекта (специалист), имеющий санкционированный доступ на территорию объекта. Цель: хищение ради собственной наживы, однако не исключается возможность совершения террористического акта.

6. Внутренний нарушитель шестого типа: работник охраны объекта. Может осуществить хищение с территории предприятия материальных ценностей, а также вступить в сговор с внешним нарушителем первого и второго типа, с целью наживы. Не исключено, что может действовать из соображений мести.

Вероятности дальнейших действий злоумышленника могут быть представлены следующей моделью (рисунок 1) [8].

Рисунок 1 – Вероятность динамических (имитационных) моделей действий злоумышленника

Вероятностная модель действий злоумышленника на объекте во время совершения им НСД при оказании на него воздействий, где:

I Приближение к объекту и визуальный осмотр объекта.
II Выбор пути проникновения на объект.
III Попытка проникновения на объект.
IV Проникновение на объект (нарушение целостности объекта).
V Перемещение злоумышленника внутри объекта.

VI Приближение злоумышленника к наиболее ценным предметам в помещении и попытка овладеть ими.

VII Уход с объекта.

Таким образом, одной из важнейших составляющих вероятного сценария осуществления противоправных действий по доступу к информации является модель нарушителя. Наличие такой модели нарушителя безопасности, которая постоянно корректируется на основе получения новых знаний о возможностях нарушителя и изменениях в системе защиты, на основе анализа причин произошедших нарушений, позволит повлиять на сами эти причины, а также точнее определить требования к системе обеспечения информационной безопасности от данного вида нарушений [7, 9].

Для того чтобы модель нарушителя приносила максимальную пользу, она должна быть сориентирована на конкретный объект защиты, учитывать мотивы действий и социально-психологические аспекты нарушения, потенциальные возможности по доступу к информационным ресурсам различных категорий внешних и внутренних нарушителей на различных пространственно-временных срезах объекта защиты [5].

Перед началом работы был проведён комплексный анализ рынка.

Выявлены следующие аналоги проекта:

- EASI;
- ASSESS;
- Спрут;
- Спрут-ИМ;
- «Вега-2»;
- «Контрфорс».

Был выявлен ряд недостатков:

- ✓ Заложена жесткая тактика действий сил реагирования.
- ✓ Отсутствует база данных по реальным-тактико-техническим характеристикам ТСФЗ и ФБ, относящихся к чувствительной информации.
- ✓ Погрешности в расчетах.
- ✓ Произведено за рубежом.
- ✓ Государственные (не продаются).

Ключевые отличительные характеристики от аналогов:

- Представление пространственной структуры объекта.
- Автоматический поиск наиболее опасных маршрутов.

- Ввод характеристик рубежей с помощью шаблонов.
- Наличие баз данных по средствам охраны.
- Количество исследуемых маршрутов.
- Учет случайного характера времени действий нарушителей и сил охраны.
- Учет вида тактики действий сил охран.
- Моделирование действий нескольких тактических групп нарушителей и сил охраны.
- Моделирование боевого столкновения.

Для построения областей распространения использовали хромоматематические методы [10], которые описаны в книге (рисунок 2) [5].

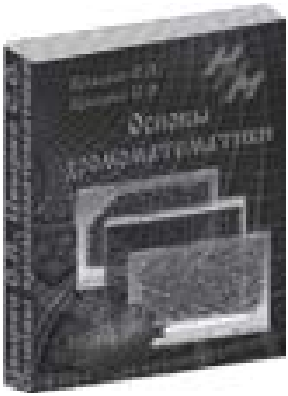


Рисунок 2 - Цвырко О.Л., Цвырко С.О. Основы хромоматематики

В книге на многочисленных примерах показана эффективность хромоматематического похода. Хромоматематика предполагает активное (осмысленное) использование цвета при конструировании математических моделей. Указана методика использования хромоматематического подхода для создания прикладных математических программ исследовательского характера.

Безусловно, пособие может быть рекомендовано к использованию в учебном процессе ВУЗа и школы, на дополнительных занятия, факультативах, кружках как обучающимся, так и преподавателям, учителям и методистам ВУЗов и школы.

Программный комплекс создан для работы в двух режимах:

1. Моделирование проникновения (прогнозируемое).
2. Моделирование проникновения (реальное).

В первом случае на работу программы будут влиять различные факторы: действия сил экстренного реагирования, работа датчиков охранной системы объекта, выбранная модель злоумышленника и др. Во втором случае все эти факторы задаются искусственно, тем самым производится проверка территории защищаемого объекта на наличие уязвимостей и соответствие принципам физической безопасности.

Рассмотрим алгоритм работы программы (рисунки 3-6).

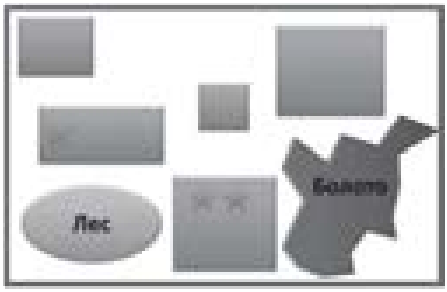


Рисунок 3 – Пример схемы защищаемого объекта для загрузки в программу

Расчет и построение путей прохождения злоумышленника по защищаемой территории является решением задачи поиска пути (рисунок 4).

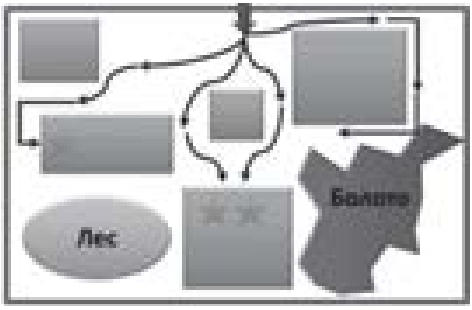


Рисунок 4 – Пример нахождения путей перемещения

От программы требуется рассчитать и продемонстрировать:

- область, в которой предполагаемо находится злоумышленник в конкретно взятый момент времени;
- предполагаемые пути перемещения злоумышленника;
- предложить службам экстренного реагирования оптимальную последовательность действий по перехвату и нейтрализации незаконно проникнувшего физического лица.

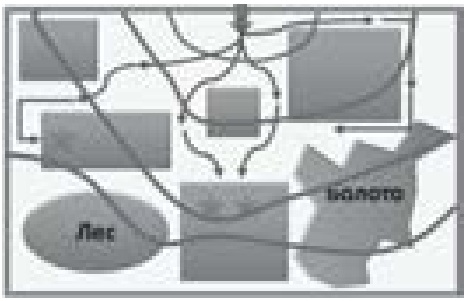


Рисунок 5 – Построение зон предполагаемого местонахождения злоумышленника

Очевидно, что при данном подходе использование модернизированного варианта алгоритма поиска путей A* требуется исключительно для расчета и построения путей предполагаемого перемещения злоумышленника по защищаемой территории.

Рисунок 6 – Построение областей предполагаемого местонахождения злоумышленника

Алгоритм:

1) задаем точку проникновения;

2) задаем точку цели;

3) в цикле выполняем следующие действия (рекурсивный вызов):

а) из крайних точек строим 8 векторов;

б) анализируем их на пересечение;

4) соединяем крайние точки непрерывной линей.

Алгоритм использует тайловую или плиточную графику (от англ. tile — плитка) [2]. Это метод создания больших изображений, когда изображение составляется из маленьких фрагментов одинаковых габаритов (рисунок 8). Перемещение по тайлам в традиционном подходе происходит по 8 направлениям (рисунок 7).

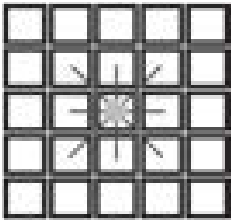


Рисунок 7 – Традиционный подход

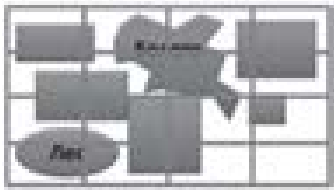


Рисунок 8 – Пример разбиения карты на тайлы

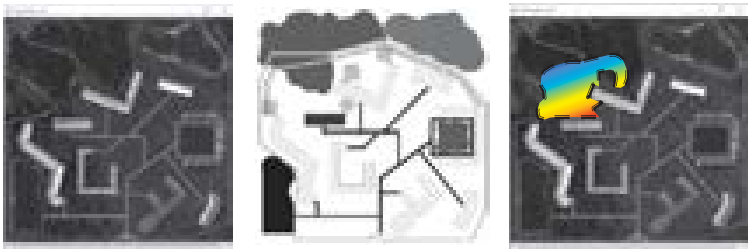
Для того, чтобы комплексно рассмотреть весь массив факторов, влияющих на работу алгоритма, был введен принцип многослойности графического представления, т.е. наложение исходных условий (рисунок 9).

Рисунок 9 – Представление «слоеного пирога» условий

Наглядно можно посмотреть на принцип работы «слоев» на следующем примере (рисунок 10). На карте объекта не видно местоположение элементов системы физической защиты (и наличие таковых), в отличие от схемы. Следует отметить, что построенная область распространении на карте смотрится нетривиально, поскольку опять же не видно элементы СФЗ, которые влияют на деятельность нарушителя.

В работке создан авторский алгоритм перехвата нарушителей, совмещающий в себе методы системного анализа, теории множеств, теории графов, теории нечетких систем, теории имитационного моделирования, модифицированный алгоритм Дейкстры, методы хромоматематического анализа, многослойную структуру объекта,

позволяющую учитывать всевозможные условия, влияющие на решение поставленной задачи, модели нарушителя.



Слой «карта» Слой «схема» Слой «область распространения»

Рисунок 10 – Различные слои

Путь нарушителя – упорядоченная последовательность действий против предприятия, которая при успешном завершении приведёт к краже, диверсии или другому враждебному акту. Критический путь – путь, у которого наименьшая вероятность суммарного обнаружения. Критический путь нарушителя характеризует эффективность СФЗ предприятия [3].

После создания этой диаграммы и введения данных об обнаружении и задержке аналитик может просмотреть возможные пути нарушителей, определить наиболее легкий путь и общую эффективность СФЗ.

На увеличенном фрагменте (рисунок 11) демонстрируется часть области предполагаемого местонахождения злоумышленника, где бихромоматематическая модель раскрашивания интуитивно подсказывает наибольшую степень опасности.

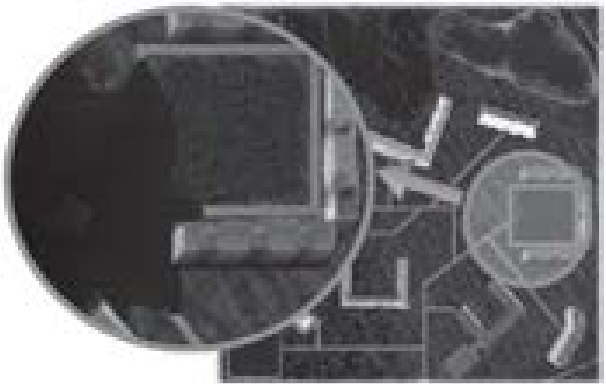


Рисунок 11 – Пример работы формы прогнозирования

Для анализа эффективности СФЗ используется метод качественной оценки эффективности EASI (Estimate of Adversary Sequence Interruption), количественно показывающий эффект от изменения параметров физической защиты [1, 9]. EASI – модель на уровне «пути», для защиты более крупных и сложных систем требуются усовершенствованные компьютерные модели. Например, диаграмма последовательности действий (ДПД) нарушителя [4].

Рассмотрим работу алгоритма на конкретном примере (рисунок 12). Предположим, происходит проникновение на абстрактный важный государственный объект (ВГО). На территории есть три проранжированных объекта и некоторые элементы СФЗ. Программа анализирует возможность проникновения в каждое здание и вероятность перехвата. После этого предлагается способ распределения групп экстренного реагирования и пути их перемещения для максимальной эффективности.

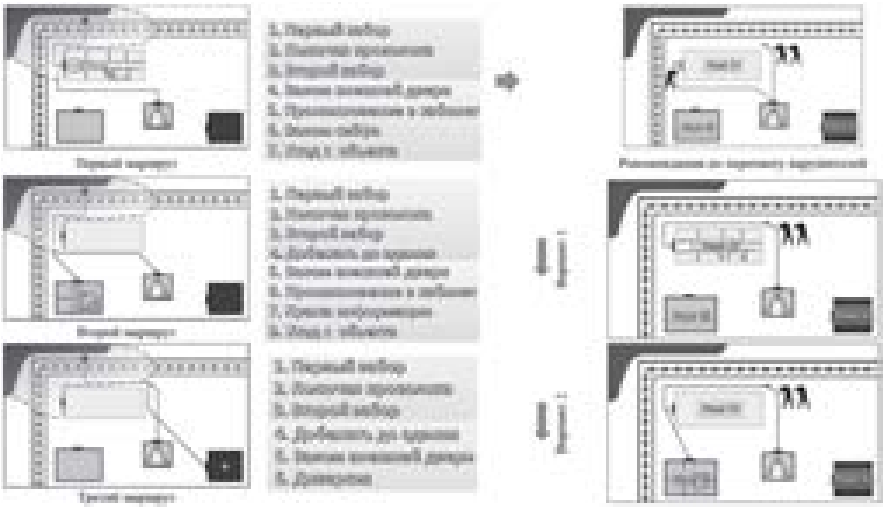


Рисунок 12 – Пример программного анализа для решения задачи

Заключение

1. Результатом проведенной научно-исследовательской работы стало создание пилотного варианта прикладного программного обеспечения на базе инновационного использования методов хромоматематики, рекурсивных алгоритмов на плоскости и "многослойности" представлений параметров для моделирования действий злоумышленника с целью улучшения эффективности систем физической защиты критически важных объектов любого

профиля в условиях специфических особенностей их функционирования.

2. Создан авторский алгоритм моделирования области предполагаемого нахождения и прогнозирования перемещения злоумышленника на защищаемой территории.

3. Разработан прототип программного комплекса, позволяющий на первом этапе прогнозировать во времени действия злоумышленника с графическим отображением.

4. Ведется разработка усовершенствованного алгоритма с учетом новых факторов:

- действий служб безопасности,
- учетом одновременных перемещений нескольких групп злоумышленников,
- расширением учитываемых факторов обстановки.

Литература

1. Боровский. А.С., автоматизированное проектирование и оценка систем физической защиты потенциально-опасных (структурно-сложных) объектов. Часть 1: Системный анализ проблемы проектирования и оценки систем физической защиты: монография / А.С.Боровский, А.Д.Тарасов – Самара-Оренбург: Сам ГУПС, ОрИПС – филиал Сам ГУПС, 2012. -163 с. ISBN 978-5-98941-171-9.

2. В.Н. Костин, С.Н. Шевченко, Н.В. Гарнова «Проектирование систем физической защиты потенциально опасных объектов на основе развития современных информационных технологий и методов синтеза сложных систем». Монография ISBN 978-5-4417-0413-7.

3. Гарсиа, М. проектирование и оценка систем физической защиты. Пер. с англ./М.Гарсиа-М.:Мир: ООО «Издательство АСТ», 2002.-386с.

4. Драгунов А.Г., Измайлов А.В., Скорцов Д.А. «Изучение компьютерных программ оценки эффективности систем физической защиты ядерных материалов и установок на примере специализированной компьютерной программы «Вега-2»: Лабораторный практикум. М.: МИФИ, 2002. -32с ISBN 5-7262-0439-5.

5. Защита от несанкционированного доступа к информации. Термины и определения: Руководящий документ. — М.: Гостехкомиссия России, 1992.

6. Лорьер Ж.-Л. Системы искусственного интеллекта / Пер. с фр. и ред. В. Л. Стефанюка. — М.: Мир, 1991. — С. 238—244.
7. Нильсон Н. Искусственный интеллект: методы поиска решений = Problem-solving Methods in Artificial Intelligence / Пер. с англ. В. Л. Стефанюка; под ред. С. В. Фомина. — М.: Мир, 1973. — С. 70 — 80.
8. Рассел С. Дж., Норвиг, П. Искусственный интеллект: современный подход = Artificial Intelligence: A Modern Approach / Пер. с англ. и ред. К. А. Птицына. — 2-е изд. — М.: Вильямс, 2006. — С. 157—162. — ISBN 5-8459-0887-6.
9. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Некоторые перспективы применения систем контроля и управления доступом в региональных ВУЗАХ. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» При поддержке Посольства Туркменистана в Российской Федерации. Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
10. Цвырко О.Л., Цвырко С.О. Основы хромоматематики. Монография. – Ишим: Изд-во ИГПИ им. П.П. Ершова, 2013. – 122 с.

МЕРЫ ПРОТИВОДЕЙСТВИЯ РЕАЛИЗАЦИИ СОВРЕМЕННЫМ УГРОЗАМ ПЛАТЕЖНЫХ ТЕРМИНАЛЬНЫХ УСТРОЙСТВ (БАНКОМАТОВ)

Черкашин Владислав Владимирович, Леандров Иван Николаевич, студенты 3 курса кафедры Информационной безопасности
Научный руководитель: **Сухотерин Александр Иванович**, к.воен.н., доцент кафедры Информационной безопасности

Платежные терминальные устройства динамично развиваются в коммерческом секторе услуг. Банкоматы и другие устройства являются лидерами безналичных способов оплаты. В настоящее время процесс развития платежных терминальных устройств направлен на усовершенствование способов оплаты. Такой прогресс не может без внимания злоумышленников. Крупные денежные суммы, находящиеся в обороте платежных терминалов, являются важнейшей целью злоумышленников. Поэтому необходимо внедрять новые меры от различных типов угроз, которые развиваются параллельно терминальным устройствам.

Электронная коммерция, банкоматы, угрозы, платежные терминалы, меры защиты.

MEASURES AGAINST THE IMPLEMENTATION OF THE CURRENT THREATS PAYMENT TERMINAL DEVICES (ATMS)

Cherkashin Vladislav, Leandrov Ivan, 3rd year students of the Department of information security
Scientific adviser: **Sukhoterin Alexander,** Candidate of Military Sciences, Associate Professor of the Department of information security

Payment terminal devices are dynamically developing in the commercial services sector. ATMs and other devices are the leaders of non-cash payment methods. At present, the development of the payment terminal devices aimed at improving the methods of payment. Such progress cannot ignore intruders. Large sums of money in circulation of payment terminals are the most important goal of hackers. It is therefore necessary to introduce new measures from the different types of threats that are developing in parallel terminal devices.

Electronic commerce, ATMs, threats, payment terminals, measures of protection.

В последнее время значительно возросло количество криминогенных действий при использовании банкоматов. Банкоматное мошенничество – противоправные деяния в отношении банкоматов (их технологической инфраструктуры), направленные на хищение денежных средств и информационных ресурсов (в том числе приготовление к такому хищению) [5].

Вопрос стоит довольно остро, особенно в случаях, когда применяются комбинированные методы, в результате которых совершаются особо крупные хищения. Статистика, приведенная на рисунке 1, показывает основные способы противоправных действий по отношению к банкоматам.

Исходя из данных статистики, мы можем классифицировать все преступления с банкоматами на несколько больших групп:

- Хищение банкоматов целиком.
- Взлом сейфа банкомата на месте установки.
- Кибератаки.
- Мошеннические установки на банкомат для кражи с карточек.

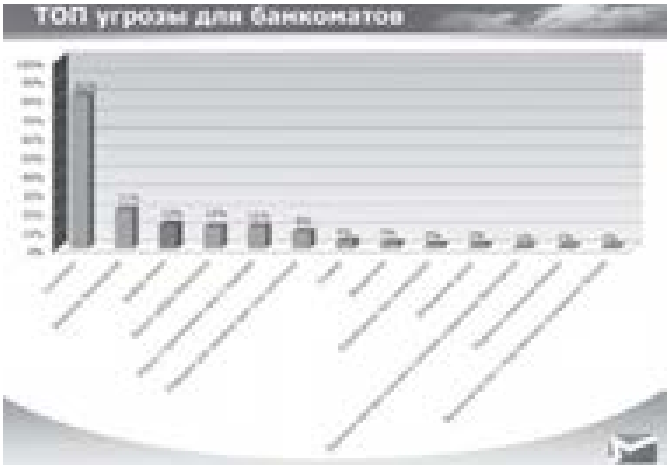


Рисунок 1 - Рейтинг угроз для банкоматов

Хищение банкомата подразумевает собой снятие банкомата с места установки и последующим взломом его сейфа в удаленном месте.

Сумма ущерба от кражи каждого банкомата в среднем составляет несколько миллионов рублей, что является, в свою очередь, кражей в особо крупном размере.

Как правило, взлом происходит в хорошо оборудованном помещении, а занимаются этим в основном подготовленные группировки.

Таким образом, для серьезного противодействия такому виду криминальных угроз сегодня необходимо создание комплекса специализированных технических средств охранной сигнализации, которые могли бы обеспечить оперативное реагирование полиции на попытки совершения краж банкоматов и задержание злоумышленников на месте совершения преступления.

Сразу следует отметить, что эффективность работы любых средств обнаружения взлома или хищения обеспечивается при условии выполнения необходимых требований по инженерно-технической укрепленности объекта охраны, в данном случае – банкомата [1-11].

В этих условиях основной упор по защите необходимо перенести на мероприятия по физической защите денежных средств внутри банкоматов и самих банкоматов. Эти мероприятия можно условно разделить на:

- действия по обеспечению технического укрепления;
- действия по передаче сигнала на пульт, в центр мониторинга или на системы автоматического реагирования;
- действия по оборудованию банкоматов техническими средствами воздействия на преступника;
- действия по приведению денег в непригодное состояние.

Наиболее эффективной мерой по предотвращению преступлений, связанных с физическим похищением денег из банкоматов, является использование специальных кассет, которые в случае несанкционированного вскрытия окрашивают содержащиеся в них купюры [12].

Однако, для обеспечения наиболее полной защиты банкоматов от хищения следует придерживаться следующих требований:

1. Крепление банкомата к конструкционным элементам помещения должна максимально защищать его от кражи.

2. В банкомате должен быть установлен сейф, класс взломостойкости которого соответствует времени реагирования тревожной группы.

3. Помещение, где находится банкомат, и сам банкомат должны быть оборудованы системой сигнализации с выводом на пульт охраны и системой видеомониторинга.

4. Помещение должно быть оборудовано техническими средствами воздействия - генератором тумана для защиты банкомата с первых секунд преступления.

5. При получении сигнала от тревожной сигнализации на объект должна выезжать тревожная группа.

6. Помещение, где расположен банкомат, должно быть оборудовано табличками с указанием, что банкомат оборудован сейфом N-класса взломостойкости, находится под охраной, оборудован сигнализацией и системой защиты с помощью тумана.

Каждый элемент данной системы отвечает за свою часть в защите банкомата, и исключение любого из них приведет к тому, что в какой-то момент объект останется без защиты.

Взлом сейфа банкомата на месте является более распространенным способом преступлений. Данный способ довольно прост: 1-2 грабителя, используя слесарный инструмент (лом, кувалда и др.) ломают корпус банкомата, а затем и переднюю стенку сейфа. После чего уносят с собой находящиеся там кассеты с деньгами.

Данный способ является более простым в исполнении, поэтому он больше подходит для одиночных грабителей без должной подготовки.

Однако, поскольку времени на непосредственный взлом банкомата в среднем уходит в 3 раза больше в сравнении с хищением банкомата целиком, способы защиты против этого целесообразно использовать те же самые, что и против кражи банкомата.

Для противодействия такого рода преступлениям, прежде всего, необходимо соблюдение требований по инженерно-технической укрепленности как самого банкомата, так и помещения, в котором он установлен. Данные вопросы достаточно подробно отражены в Рекомендациях Р 78.36.035-2013 МВД России [4].

Кроме того, на рынке систем безопасности имеется целый арсенал технических средств охранной сигнализации, с помощью которых можно построить достаточно надежную защиту банкоматов. Начнем с самого, пожалуй, важного этапа построения такой защиты - выбора средств обнаружения несанкционированного проникновения нарушителей в зону размещения банкомата и совершения криминальных воздействий на него.

Для блокировки «на открывание» дверных и оконных конструкций помещения, в котором установлен банкомат, а также открываемых или перемещаемых конструкций самого банкомата, обеспечивающих доступ к нижнему кабинету (сейфу) или верхнему кабинету (процессорному блоку), обычно используют магнитоконтактные извещатели, которые должны соответствовать требованиям ГОСТ Р 54832-2011 [3], с учетом видов, размеров и материалов охраняемых конструкций.

При выборе конкретных типов магнитоконтактных извещателей, устанавливаемых внутри банкомата, в частности, для блокировки «на открывание» основной двери нижнего кабинета необходимо учитывать ограничения по размерам свободного пространства, связанные с высокой плотностью расположения внутренних механизмов (кассет с наличными деньгами), периодически перемещаемых и извлекаемых при инкассации, а также при обслуживании и ремонте.

Для блокировки «на открывание» пластиковой декоративной двери нижнего кабинета банкомата (при ее наличии) рекомендуется использовать магнитоконтактные извещатели, обладающие функцией защиты от саботажа внешним магнитным полем, чтобы нарушитель,

воспользовавшись мощным магнитом, не мог вывести магнитоконтактный извещатель из строя, а если кто и попытается это сделать, то извещатель должен подать сигнал тревоги.

Для обнаружения разрушения обычных и защитных стекол, стеклопакетов, а также стекол со специальными свойствами, применяемых для остекления помещений, как правило, используют акустические (звуковые) извещатели, которые должны соответствовать требованиям ГОСТ Р 51186-1998 [2], а также обладать функциями активной защиты от маскирования и автоматического контроля работоспособности.

Для обнаружения попытки умышленного разрушения, повреждения или взлома ограждающих строительных и защитных конструкций помещения, в котором установлен банкомат, особенно, если данные конструкции не обладают высокой степенью устойчивости к взлому, рекомендуется использовать специальные вибрационные извещатели, которые должны соответствовать требованиям ГОСТ Р 53702-2009 [1], обнаруживать все типы разрушающих воздействий по ГОСТ Р 50862-2012 [11] и выбираться в соответствии с видами, размерами и материалами охраняемых конструкций.

Для обнаружения проникновения нарушителя через дверной или оконный проем помещения, в котором установлен банкомат, рекомендуется использовать оптико-электронные (инфракрасные) извещатели не ниже 3 класса по ГОСТ Р 50777-2014 [10], имеющие поверхностную зону обнаружения типа «занавес» [6].

Мошеннические устройства в последнее время являются одними из самых популярных способов кражи денег с банкоматов. Они нацелены не столько на деньги, находящиеся в банкомате, сколько на карточки клиентов, воспользовавшихся банкоматами. К данным мошенническим методам относятся:

- скимминг;
- ливанская петля;
- кража наличных денег путем удержания их в банкомате при выдаче;
- ложная отмена операций.

Для удержания купюр в банкомате достаточно небольшой клейкой пластины, мешающей купюрам выйти из банкомата. Как правило, купюры изымаются мошенником сразу же, как только первая жертва идёт разбираться с администрацией банка.

Ливанская петля представляет из себя специальное устройство, вставленное в картридер. Его целью является удержание карточки в банкомате. Цель мошенника - под предлогом помощи узнать ПИН-КОД жертвы. После нескольких неудачных попыток возврата карты жертва уходит, а мошенник извлекает карту и снимает с неё средства.

Под скиммингом подразумевается установка специального устройства - скиммера - на картридер банкомата. При вставке карты в банкомат — это устройство считывает все данные карты, после чего злоумышленники имеют возможность создать дополнительную карту, с помощью которой снимаются средства со счета владельца.

Существует 2 метода защиты от него - активный и пассивный антискимминг. Под пассивным антискиммингом подразумевается установка владельцем банкомата специального антискиммера.

Рисунок 2 - Картридер банкомата с антискиммером

Проблема данного метода заключается в том, что клиенты просто боятся пользоваться такими банкоматами. И это правильно, поскольку даже сотрудники банка не всегда могут отличить скиммер (изображён на рисунке 3) от антискиммера.

Рисунок 3 - Картридер банкомата со скиммером

Активный антискиммер - более качественный способ защиты, но и более затратный. Это специальное устройство, установленное внутри банкомата, незаметное снаружи. При установке какого-либо дополнительного устройства такой антискиммер сразу реагирует и сигнализирует о несанкционированной установке. Благодаря такому устройству также происходит защита от ливанской петли, ложной отмены операций и удержания купюр в банкомате, поскольку для их реализации также требуются дополнительные мошеннические устройства.

Кибератаки - самый перспективный и развивающийся метод атак на банкоматы, поскольку он является самым безопасным для мошенников. Сущность кибератак заключается в проникновении в верхнюю часть (процессор) банкомата непосредственно или удалённо. Завладение злоумышленником доступом к системе управления банкоматом дает ему возможность:

- получать персональные данные, находящиеся в банковской сети;
- получать прямой доступ к транзакциям, операциям;
- получать права администратора, имеющего возможность выдать любое количество и вид купюр;
- подменить номинал купюр;
- и другое.

Как видно из приведенного выше списка, попадание в систему банкомата дает злоумышленнику всё, что ему нужно. И то, как воспользоваться предоставленными возможностями, зависит лишь от уровня умений и фантазии самого нарушителя.

Проникновение в систему управления банкоматом становится возможным, исходя из того, что:

- банкомат - это маломощный и устаревший ПК;
- операционная система банкомата в большинстве случаев - Windows XP, который с 2014 года не поддерживается на официальном уровне и является очень уязвимым к вирусам;
- как правило, система защиты и антивирусы также являются устаревшими;
- даже при наличии хорошей системы защиты на самой системе банкомата, интерфейс клиента во многих случаях сделан на основе интернет-браузера Internet Explorer, и имеет те же уязвимости;

- банковская сеть зачастую связана с Internet, что даёт возможность проникнуть в сеть банкоматов удалённо;
- всегда остаётся возможность перехватить транзакции с банкомата на сервер, даже не получая доступ к самому банкомату.

В качестве одного из примеров кибератак можно привести широко известный вирус Tyupkin, который в октябре 2014г. был обнаружен "Лабораторией Касперского". Данный вирус загружался на банкомат, после чего злоумышленник мог единовременно получить 40 купюр из банкомата при удачном вводе ключа, известного только ему. Если ввод происходил неудачно - банкомат блокировался. На территории РФ банки лишились миллионов благодаря этому вирусу [7].

На данный момент, по словам "Лаборатории Касперского", кибератаки не грозят банкоматам, если придерживаться определенных требований:

- усилить физическую защиту банкоматов (важно, чтобы банкомат надежно стоял на месте – был прикреплен к стене или полу либо помещен в специальный защитный бокс);
- установить надежную охранную сигнализацию на каждый банкомат (по данным «Лаборатории Касперского», Tyupkin заражал только банкоматы без сигнализации);
- заменить все замки и мастер-ключи от производителя, запирающие верхние отсеки банкоматов;
- сменить установленные по умолчанию пароли BIOS (отмечено, что разработчикам ПО следует в целом уделять больше внимания безопасности устройств: уникальные пароли BIOS должны быть сложными, состоящими не только из цифр, но и букв и спецсимволов);
- регулярно обновлять антивирусную защиту банкоматов;
- регулярно выполнять полную проверку файловой системы каждого банкомата;
- регулярно проверять банкоматы на наличие сторонних устройств (скиммеров);
- использовать только проверенные Whitelisting-продукты на банкоматах, чтобы снизить вероятность определения антивирусами чистого программного обеспечения как вредоносного и наоборот.

Литература

1. ГОСТ Р 50777-2014 Извещатели пассивные оптико-электронные инфракрасные для закрытых помещений и открытых площадок. Общие технические требования и методы испытаний.
2. ГОСТ Р 50862-2012 Сейфы, сейфовые комнаты и хранилища ценностей. Требования и методы испытаний на устойчивость к взлому и огнестойкость.
3. ГОСТ Р 54832-2011 Извещатели охранные точечные магнитоконтактные. Общие технические требования и методы испытаний.
4. Р 78.36.035-2013 МВД России «Рекомендации по организации комплексной централизованной охраны банковских устройств самообслуживания».
5. Выдержка из книги «Платежные карты. Бизнес-энциклопедия», 2008 г. 760 с. Переплет. ISBN 5-7958-0237-4
6. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Развитие сотрудничества российских и зарубежных ВУЗОВ по защите информационного ресурса. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
7. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
8. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.

9. Актуальные вопросы противокриминальной защиты банкоматов и платежных терминалов // URL: http://nicohrana.ru/78-aktualnye-voprosy-protivokriminalnoy-zaschity-bankomatov-i-platezhnyh-terminalov.html
10. Банкоматный вирус Tyupkin: будут ли новые атаки? // URL: https://www.icpress.ru/articles/detail.php?ID=18215
11. Основные виды криминальных угроз банкоматам и способы противодействия этим угрозам // Алгоритм Безопасности" № 3, 2015 год // URL: http://www.algoritm.org/arch/arch.php?id=76&a=1795
12. Физическая защита банкоматов // Каталог "Системы цифровой видеорегистрации (DVR)" #1, 2013 URL: http://www.secuteck.ru/articles2/dvr/fizicheskaya-zaschita-bankomatov/

ОСНОВЫ ПОСТРОЕНИЯ ПРОАКТИВНОЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Шмелев Александр Владимирович, студент 4 курса кафедры Информационной безопасности
Научный руководитель: **Соляной Владимир Николаевич**, к.воен.н, доцент, заведующий кафедрой Информационной безопасности

Проактивная безопасность компьютерной системы - это органичное структурное свойство, которое позволяет такой системе сохранять свою функциональность, даже если некоторые из компонентов системы становятся в силу ряда причин «неработоспособными». Свойство проактивной безопасности позволяет на этапе эксплуатации компьютерной системы не выделять ресурсы на внедрение дополнительных механизмов защиты, не привлекать высококвалифицированных специалистов и службы информационной безопасности, дополнительные сервисы и системные ресурсы. Все ресурсозатраты при таком подходе к созданию компьютерной системы (временные, материальные, финансовые, интеллектуальные, «людские») переносятся с этапа ее эксплуатации на этап создания (проектирования, разработки, испытании).

Компьютерная система, информационная безопасность, средство скрытого информационного воздействия, проактивная безопасность.

FORMATION FUNDAMENTALS OF PROACTIVE SECURITY OF COMPUTER SYSTEMS

Shmelev Alexander, 4rd year student of the Department of information security
Scientific adviser: **Solyanoy Vladimir,** Candidate of Military Sciences, Associate Professor, Head of the Department of information security

Proactive security of computer systems - is an organic structural feature that allows a system to maintain its functionality, even if some of the components of the system are "unworkable" due to several reasons. The property allows for proactive safety during operation of the computer system does not allocate resources for the implementation of additional security mechanisms do not attract highly qualified specialist and information security services, additional services and system resources. All resource consumption in such an approach to the creation of a computer system (time, material, financial, intellectual, "human") transferred from the stage of its operation to the step of creating (design, development, test).

The computer system, information security, covert means of information influence, proactive security.

Проактивная безопасность компьютерных систем эта сравнительно новая парадигма в области создания безопасных информационных технологии, которая позволит дать асимметричный ответ создающимся «мощным» киберструктурам [4], призванным осуществлять глобальные наступательные действия в киберпространстве, и фактически свести их «к нулю», затрачивая при этой гораздо меньшее количество ресурсов, чем «наступающая» сторона.

Если универсальные механизмы создания проактивно безопасной КС будут реализованы, то потенциальный пользователь (эксплуатирующая организация) в большинстве случаев сможет фактически не заботиться о том, подвергается ли его КС кибератакам или нет. Такая КС просто «изолирует» кибератаку, сохраняя при этом свою функциональность.

На протяжении нескольких десятков лет многими специалистами в области информационной безопасности объектов информатизации различного назначения объективно признается, что наиболее целесообразно решать весь комплекс проблем защиты

информации с самого начала жизненного цикла КС, то есть еще с момента разработки системных, проектных, алгоритмических решении. В то же время сколько-нибудь строгой (формальной) аргументации такой позиции, по существу, нигде не приводится [5].

В условиях эффективного использования выделяемых ресурсов, применения новейших технических н технологических достижений проактивные решения позволят повысить уровень защиты современных КС, что, в свою очередь, будет влиять на уровень защищенности различных объектов информатизации, в том числе критически важных [1-11].

В этом случае с учетом проактивного измерения процесса создания КС главная цель комплексного решения проблемы информационной безопасности при защите КС – создание комплекса мер:

— проактивных – на методологическом, общественном и алгоритмическом уровнях;

— реактивных, обеспечивающих устойчивость функционирования компонентов КС на этапе эксплуатации.

Суть процесса обеспечения проактивной безопасности КС заключается в необходимости:

— предотвращения внедрения средств скрытого информационного воздействия (ССИВ) в КС их авторам, на этапе разработки;

— предотвращения внедрения ССИВ в компоненты КС посредством системных средств и инструментальных средств разработки (через операционные системы, системы управлении базами данных, CASE-средства, трансляторы, отладчики и подобные им средства) в процессе создания компонентов КС, их тестирования и испытаний.

Даже «потенциально» защищенные от несанкционированного доступа компоненты КС на этапе их эксплуатации могут иметь в своем составе ССИВ, а средства защиты в этом случае с большой вероятностью становятся малоэффективными. Следовательно, отсутствие мер проактивной защиты КС может привести к блокированию этих систем, непредсказуемому нарушению режимов их функционирования или блокированию (утечке) оперативной (конфиденциальной) информации.

Тем не менее обеспечение защиты КС при наличии в них ССИВ относится к совокупной проблеме обеспечения проактивной и реактивной безопасности КС, когда методы разработки защищенных

компонентов КС, методы их тестирования, вероятностные методы расчета наличия ССИВ и методы оценивания уровня информационной безопасности КС могут в значительной мере пересекаться и дополнять друг друга.

Процесс разработки КС включает набор этапов и операций в последовательности их выполнения и взаимосвязи, обеспечивающих ведение разработки на всех стадиях от технического задания до завершения испытаний. С точки зрения обеспечения проактивной безопасности чрезвычайно важно организовать этот процесс таким образом, чтобы на каждом его этапе выполнялся необходимый и достаточный комплекс организационно-технических мероприятий, предотвращающих (существенно затрудняющих) постановку на эксплуатацию готовых компонентов КС с внедренными ССИВ [1-11].

Типовой процесс включает описание исходной информации, способов и методов выполнения операций и этапов работ, устанавливает требования к результатам и правилам их контроля, определяет формы технологических и программных документов, а также организационную структуру коллектива, обеспечивает распределение, планирование работ и контроль за ходом разработки. Повышение эффективности разработки компонентов КС в целом достигается регламентацией порядка проведения работ, автоматизацией этапов и операций, разделением труда между специалистами разной квалификации и проблемной ориентацией применяемой технологии.

Индустриализация технологий проектирования вызывает необходимость унификации и стандартизации языков проектирования, создает предпосылки для модернизации и развития компонентов КС, а также для повторного использования отработанных компонентов.

В случае программного обеспечения (ПО), разрабатываемого в интересах КС современные инструментальные средства автоматизации разработки ПО (CASE-средства) и его отладка в той или иной мере поддерживают весь процесс разработки ПО. Использование CASE-средств значительно осложняет действия по выявлению и устранению ССИВ. Это обусловлено тем обстоятельством, что программист практически не имеет возможности контролировать непосредственно создаваемые программы, так как работает на уровне логических конструкций языковых средств. Если целью атаки является нанесение как можно

большего вреда, то наиболее подходящей целью для злоумышленника, пытающегося внедрить ССИВ, являются программы, которые используются большим числом различных пользователей, например, компиляторы, трансляторы, интерпретаторы, ассемблеры. Кроме них целый ряд других инструментальных средств автоматизации программирования может иметь встроенные средства автоматического генерирования ССИВ [1-11].

Сложность проведения исследований в области проактивной безопасности обусловлена, главным образом, неопределенностью, в которой можно выделить два аспекта:

неопределенность технологических приемов, используемых различными разработчиками программного обеспечения, особенно при создании крупномасштабных КС;

неопределенность, которая обусловлена развитием новых технических средств разведки и возможностью появления новых способов и средств внедрении ССИВ в разрабатываемое программное обеспечение.

В данных условиях при исследовании методов и средств обеспечения проактивной зашиты необходимо исходить из предположения о том, что такая защита будет обеспечена, если до внедрения КС в эксплуатацию будут созданы условия, при которых имеет место одно из следующих событий:

— на предприятии-разработчике КС выполнены мероприятия предупредительного характера, при которых невозможно любое нарушение проактивной безопасности в процессе создания КС;

— даже при обнаружении попыток нарушения проактивной безопасности компонентов КС последствия таких попыток будут ликвидированы до введения КС в штатную эксплуатацию;

— даже если попытки нарушения проактивной безопасности компонентов КС имели место и не обнаружены, их последствия будут своевременно выявлены, локализованы и ликвидированы до введения КС в штатную эксплуатацию.

Такие попытки нарушения защиты, в том числе за счет внесения ССИВ в компоненты КС и их активизации «в нужное время и в нужном месте»» представляют реальную опасность для разрабатываемых КС. Посредством ССИВ, таким образом, можно заблокировать возможность применения средств автоматизации в крупных корпоративных системах и даже отраслях промышленности, снизить эффективность работы этих средств, а также влиять на выполнение

этими средствами своих функций, что недопустимо с точки зрения национальной безопасности.

Учитывая все сказанное выше, для предотвращения всей совокупности воздействия ССИВ на современные КС, в том числе и использующиеся на критически важных объектах, необходимо реализовать комплекс научно обоснованных мероприятий, к числу которых, в первую очередь, можно отнести разработку методологии обеспечения проактивной безопасное) и КС.

Основные составляющие методологии обеспечения проективной безопасности КС (рис. 1).

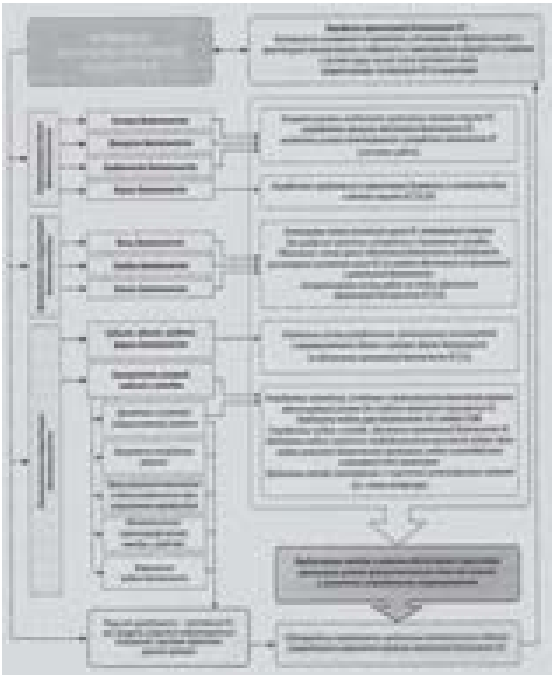


Рисунок 1 - Состав и структура методологии обеспечения проактивной безопасности КС

К основным составным элементам методологии обеспечения проактивной безопасности КС следует отнести:

-характеристики комплекса работ (особенности организации процесса защиты КС, принципы обеспечения их безопасности, условия проектирования, разработки и эксплуатации компонентов компьютерной системы, нормы деятельности, понятийная и нормативно-методическая база в области защиты КС);

-логической структура деятельности (предмет, субъекты, объекты, формы и средства деятельности по защите КС, модели, методы и организационно-технические решения по защите КС, модели угроз безопасности, таксономия моделей ССИВ, результат и оценка деятельности в данной области);

-временная структура деятельности (жизненный цикл КС и содержание основных этапов, связанных с обеспечением их проактивной и реактивной безопасности).

Такой подход имеет определяющее значение для создания компонентов КС, являющихся, по определению, изделиями информационных технологий с высоким оценочным уровнем доверия.

Исторически известны разные типы организации деятельности. Современным является проектно-технологический тип, который состоит в том, что продуктивная деятельность человека (или организации) разбивается на отдельные завершенные циклы, которые называются проектами.

Таким образом, процесс осуществления деятельности целесообразно рассматривать в рамках проекта, реализуемого в определенной временной последовательности по фазам, стадиям и этапам, причем последовательность эта является общей для всех видов деятельности. Завершенность цикла деятельности (проекта) определяется тремя фазами:

-фазой проектирования, результатом которой является построенная модель создаваемой системы и план ее реализации;

-технологической фазой, результатом которой является реализация системы;

-рефлексивной фазой, результатом которой является оценка реализованной системы и определение необходимости либо ее дальнейшей коррекции, либо «запуска» нового проекта.

Характеристики деятельности по защите КС:

— особенности организации процесса защиты компонентой КС;

— принципы обеспечения безопасности КС;

— условия проектирования, разработки и эксплуатации КС;

— понятийная база, нормативно-правовые, нормативно-методические, нормативно-технические документы в области создании и применения КС.

Логическая структура деятельности по обеспечению безопасности КС:

— субъект-разработчик (проектная организация), пользователь (эксплуатирующая организация), нарушитель (-ли), противник(-ки);

— объект - КС;

— предмет деятельности - процесс защиты КС;

— формы деятельности - зашита компонентов КС от ССИВ;

— средства - средства и механизмы зашиты компонентов КС;

— модели и методы - модели и методы обеспечения безопасности КС, модели уязвимостей/угроз/атак/ противника;

— результат деятельности - компоненты КС, как продукты (изделия) информационных технологий с высоким оценочным уровнем доверия.

Временная структура деятельности по обеспечению безопасности КС:

— фазы - этапы создания и применения КС;

— стадии - все этапы жизненного цикла КС;

— этапы деятельности по защите КС-этапы обеспечения проактивной и реактивной зашиты КС.

Модели и методы обеспечения проактивной безопасности КС

Известные методы (классы методов) проактивной защиты ПО с привязкой к его жизненному циклу приведены далее (рис. 2.).

Рисунок 2 – Классы методов проактивной защиты КС

К ним относятся классы:

— методов и инструментальных методик диагностического контроля инструментальных средств разработки компонентов КС (трансляторов, компиляторов, отладчиков, CASE-средств) [1, 2];

— моделей и методов верификации программ, верификации моделей программ [2];

— методов контроля проактивной безопасности КС на этапах их автономных испытаний, комплексных испытаний, рекламационных доработок [6];

— средств проактивной защиты на этапе подготовки КС к функционированию: средств обновления ОС, антивирусных баз данных, баз данных сигнатур атак IDS/IPS-систем, систем активного аудита и т. п.;

— моделей и методов проактивной защиты посредством методов Data Mining [3].

Из рис. 2 видно, что этапы (задачи) разработки функционально эквивалентных алгоритмов с введенными элементами защиты и их кодирования на конкретных языках программирования или кодирования в машинных кодах ранее практически не рассматривались в рамках единой технологии разработки защищенных компонентов КС. В том числе именно разработке проектных решений, моделей и методов защиты на этих этапах посвящена настоящая работа. Кроме того, в перечисленных выше классах методов обеспечения проактивной безопасности компьютерных систем, как правило, не выдвигалось предположение о том, что при их разработке действует злоумышленник.

Разработанные методы и решения по обеспечению проактивной безопасности КС на этапах системного анализа, разработки требований, математического и алгоритмического обеспечения, программирования (кодирования программ), их компиляции и отладки в совокупности с известными методами и решениями по проактивной защите на этапах тестирования и испытаний может составить полный методический базис структуры деятельности по проактивной защите КС. Это, в свою очередь, позволяет говорить о достаточности и обоснованности набора лежащих в ее основе моделей и методов проактивной защиты КС [11]. Таким образом, разработанные методы и решения позволяют охватить все этапы жизненного цикла КС, предшествующие этапу его эксплуатации по назначению.

В то же время анализ возможных решений показал [2, 5] — математических моделей и методов проактивной защиты от действий злоумышленника на ранних этапах жизненного цикла ПО, скорее всего, не может быть много, но они есть ввиду как сложности формализации таких решений, так и сложности самих решений.

Таким образом, методология обеспечения проактивной защиты КС представляет собой совокупность организационно-технических решений, моделей и методов, рассматриваемых в рамках данной методологии, которые позволяют выполнить вышеназванный сценарий разработки КС.

В последнее время появилась насущная необходимость в создании новых технологий разработки КС, изначально (с самого начала жизненного цикла) ориентированных на создание безопасных программных продуктов, даже если на этапе их проектирования и разработки действуют злоумышленники. Демонстрация возможности создания проактивно безопасных компьютерных систем в соответствии с выдвинутой методологией создания подобных систем и предпринята в настоящей статье.

В ней излагаются элементы методологии обеспечения проактивной безопасности КС, рассматриваются принципы обеспечения проактивной безопасности, условия, требования и ограничения при проектировании и разработке компонентов КС в «проактивном исполнении». При этом применение новых подходов, алгоритмов, схем и протоколов защиты позволяет перенести процесс внесения в компоненты КС защитных функций на более ранние этапы их жизненного цикла.

В силу чрезвычайной сложности проблематики обеспечения проактивной безопасности КС в условиях информационного противоборства полученные результаты, конечно же, не исчерпывают всего круга проблем обеспечения такой защиты для КС [1-11].

Тем не менее предлагаемые научно-практические и организационно-технические решении по обеспечению безопасности КС на этапе проектирования позволят их использовать при задании технических требований к компонентам КС, входящих в состав современных объектов информатизации, в том числе критически важных, при подготовке и проведении организационно-технических мероприятий по защите КС на этапе их создания, при проведении научных и прикладных исследований по проблематике обеспечения проактивной безопасности компьютерных систем.

Литература

1. Ефимов А. К. Методика построения тестов проверки технологической безопасности инструментальных средств автоматизации программирования на основе их функциональных диаграмм / А. К. Ефимов Б. П. Пальчун, Л. М. Ухлинов // Вопросы защиты информации -1995. -№3(30). -С. 52-54.
2. Казарин О. В. Методология защиты программного обеспечения. / О. В. Казарин // М.: МЦНМО. - 2009. - 464 с.
3. Комашинский Д. Б. Исследование проактивных механизмов обнаружения вредоносного программного обеспечения на базе методов Data Mining / Д. Б. Комашинский, И. В. Котенко // В кн. Математика и безопасность информационных технологий. Материалы конференции в МТУ 30-31 октября 2008 г. // -М.: МЦНМО. -2009. -Т.2. –С. 226-231.
4. Сальников А. А. Новые факторы и безопасность в киберпространстве / А. А. Сальников Р. А. Шаряпов, В. В. Ященко // Вестник Московского университета. Серия политическая. // – 2010. -№ 2. -С. 71-84; -№ 3. -С. 90-103.
5. Скиба В. Ю. Парадигма проактивной безопасности компьютерных систем / В. Ю. Скиба // Защита информации. Инсайд. // -2009. -№ 5. -С. 2-9; М-6. -С. 2-7.
6. Соляной В.Н., Сухотерин А.И Выработка коммуникативной компетенции при подготовке профессионалов по информационной безопасности с использованием технологии модерации. «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7
7. Соляной В.Н., Сухотерин А.И, Антоненко В.И. Проблемно-ориентированная подготовка специалистов по информационной безопасности с использованием имитационного метода (мозговой штурм). «Инновационные технологии в современном образовании» //Сборник трудов по материалам III Международной научно-практической Интернет - конференции 18 декабря 2015 г. –М. Издательство «Научный консультант», 2016. – 784 с. ISBN: 978-5-9907976-9-7.
8. Соляной В.Н., Сухотерин А.И, Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества.

Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
9. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4.
10. Соляной В.Н., Сухотерин А.И., Воронов А.Н. Некоторые перспективы применения систем контроля и управления доступом в региональных ВУЗАХ. Научная статья. «Перспективы организационные формы и эффективность развития сотрудничества российских и зарубежных ВУзов» *При поддержке Посольства Туркменистана в Российской Федерации.* Текст Сборник материалов III Ежегодная международной научно-практическая конференция 6-7 апреля 2015 г.: Королёв МО: ФТА. Издательство «Канцлер», 2015-52 с.
11. Ухлинов Л. М. Обеспечение безопасности информации в центрах управления полетами космических аппаратов. / Л. М. Ухлинов, М. П. Сычев, В. Ю. Скиба, О. Б. Казарип //- М. -Изд-во МГТУ им. Н.Э. Баумана -2000. - 366 с.

КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И УПРАВЛЯЮЩИХ СИСТЕМ

ВЛИЯНИЕ ЭЛЕКТРОМАГНИТНЫХ ВОЛН НА ОРГАНИЗМ ЧЕЛОВЕКА

Антонов Никита Аркадьевич, студент 3 курса кафедры Информационных технологий и управляющих систем
Научный руководитель: **Теодорович Наталия Николаевна,** к.т.н., доцент кафедры Информационных технологий и управляющих систем

В данной статье рассмотрены основные принципы распространения электромагнитных волн, влияние на их прохождение различных препятствий и сред, проанализировано влияние электромагнитных излучений на организм человека, зависимость этого влияния от частоты. В рамках статьи также показаны некоторые методы и способы минимизации негативных воздействий ЭМП на живые организмы, приведены примеры научных разработок в этой области.

Электромагнитные волны, радиоволны.

THE INFLUENCE OF ELECTROMAGNETIC WAVES ON THE HUMAN BODY

Antonov Nikita, 3rd year student of the Department of information technologies and control systems
Scientific adviser: **Teodorovich Natalia**, Candidate of Technical Sciences, Associate Professor of the Department of information technologies and control systems

This article describes the basic principles of electromagnetic waves propagation, their influence on the passage of different obstacles and environments, and analyzed the impact of electromagnetic radiation on the human body, the dependence of this effect on frequency . The article also shows some methods and ways to minimize the negative effects of electromagnetic fields on living organisms, are examples of scientific developments in this area.

Electromagnetic waves, radio.

Радиоволны — электромагнитное излучение с длинами волн в электромагнитном спектре длиннее инфракрасного излучения, со скоростью распространения, равное скорости света (300 000 км/сек).

Законы распространения радиоволн в свободном пространстве сравнительно просты, но чаще всего радиотехника имеет дело не со свободным пространством, а с распространением радиоволн над земной поверхностью. Поверхность Земли сильно влияет на распространение радиоволн. Здесь сказываются как физические свойства так и общая кривизна поверхности. Это влияние различается для волн различной длины, а также зависит от расстояния между передатчиком и приемником.

Дифракция сильно зависит от соотношения между длиной волны и размерами тела, находящегося на пути волны. Следовательно, кривизна земной поверхности, а также ее рельеф по-разному сказываются на распространении волн в зависимости от их длины.

В качестве примера можно привести горную цепь, которая отбрасывает «радиотень» в случае коротких волн. При этом достаточно длинные (километровые) волны хорошо огибают это препятствие и в результате ослабляются незначительно (рис. 1).

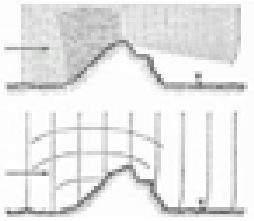


Рисунок 1 - Пример радиотени для коротких волн и огибание препятствия длинными волнами

Земля для радиоволн представляет проводник электричества, проходя над поверхностью земли, радиоволны постепенно ослабевают, что связано с возбуждением этими волнами в поверхности земли электротоков, на что и тратится часть энергии [1].

Энергия волны ослабевает, в том числе и из-за того, что излучение распространяется во все стороны пространства - чем дальше от передатчика находится приемник, тем меньшее количество энергии приходится на единицу площади и тем меньше ее попадает в антенну.

Передачи длинноволновых станций можно принимать на расстоянии до нескольких тысяч километров, при этом уровень сигнала уменьшается плавно, без скачков. Средневолновые можно принимать в пределах тысячи километров. Энергия же коротких волн

резко убывает по мере удаления от передатчика, но исследования коротких и ультракоротких волн показали, что они быстро затухают только когда идут у поверхности Земли, а когда излучение направлено вверх, то короткие волны возвращаются обратно [1].

Рисунок 2 - Распространение радиоволн между Землей и ионосферой

Высота отражения зависит от длины волны: чем короче волна, тем на большей высоте происходит ее отражение, тем больше «мертвая зона». Эта зависимость верна лишь для коротковолновой части спектра (до 25–30 МГц). Для более коротких волн ионосфера является прозрачной. Волны пронизывают ее насквозь и уходят в космическое пространство [5, 6, 7].

Международными соглашениями весь спектр радиоволн, применяемых в радиосвязи, разбит на диапазоны, приведенные в таблице 1.

Таблица 1 - Диапазоны радиоволн

Диапазон частот	Наименование диапазона	Наименование диапазона волн	Длина волны
3–30 кГц	Очень низкие частоты (ОНЧ)	Мириаметровые	100–10 км
30–300 кГц	Низкие частоты (НЧ)	Километровые	10–1 км
300–3000 кГц	Средние частоты (СЧ)	Гектометровые	1–0.1 км
3–30 МГц	Высокие частоты (ВЧ)	Декаметровые	100–10 м
30–300 МГц	Очень высокие частоты (ОВЧ)	Метровые	10–1 м
300–3000 МГц	Ультравысокие частоты (УВЧ)	Дециметровые	1–0.1 м
3–30 ГГц	Сверхвысокие частоты (СВЧ)	Сантиметровые	10–1 см
30–300 ГГц	Крайневысокие частоты (КВЧ)	Миллиметровые	10–1 мм
300–3000 ГГц	Гипервысокие частоты (ГВЧ)	Децимиллиметровые	1–0.1 мм

Электромагнитное излучение характеризуется частотой, длиной волны и мощностью переносимой энергии.

$$\lambda = 299{,}79/f,$$

Где f – частота электромагнитного излучения в Мгц

С увеличением частоты длина волны уменьшается, и наоборот.

За радиоволнами (по убывающей длине) следуют тепловые или инфракрасные лучи. После них идет узкий участок волн видимого света, далее - спектр ультрафиолетовых, рентгеновских и гамма лучей - все это электромагнитные колебания одной природы, отличающиеся только длиной волны и, следовательно, частотой. Хотя весь спектр разбит на области, границы между ними намечены условно. Области следуют непрерывно одна за другой, переходят одна в другую, а в некоторых случаях перекрываются. С учётом особенностей распространения, генерации и излучения весь диапазон радиоволн принято делить на ряд поддиапазонов: сверхдлинные волны, длинные волны, средние волны, короткие волны, метровые волны, дециметровые волны, сантиметровые волны, миллиметровые волны и субмиллиметровые волны.

Во всем мире проблемы, касающиеся человека и окружающей среды, возрастают с каждым днем, в том числе возникает вопрос о влиянии электромагнитного излучения на организм человека. Так, сегодня беспроводные технологии активно внедряются в нашу жизнь. К таким технологиям относятся Wi-Fi, Zigbee, WiMax, Dect и.т.д. [5].

В последние годы появилось достаточно много статей на данную тему, отражающих результаты широкомасштабных исследований о взаимосвязи здоровья человека, вынужденного находится среди разночастоных излучений.

Многие знают, что злоупотреблять солнечными ваннами нельзя. Но мало кто задумывался над тем, что включенный телевизор, электробритва или даже обычная лампа, испускают не менее вредные для нас излучения. До недавнего времени считалось, что электромагнитные волны, которые излучают бытовые электроприборы и электросеть практически безвредны для здоровья человека. Однако последние исследования американских специалистов подтверждают, что это совсем не так. Проводя эксперименты над клетками животных, ученые установили, что электромагнитное поле при определенных условиях воздействует на деятельность гормонов, которые обеспечивают прохождение нервных импульсов. Подобное воздействие и на организм человека может привести к целому ряду расстройств, в том числе с нарушением биоритмов, бессоннице и даже хронической депрессии [2,3].

Тем не менее, достоверного подтверждения того, что клетки человека будут реагировать на излучение подобным образом, пока нет. Интересно, что во время ряда экспериментов было доказано, что

пульсирующее излучение, например, телевизоров или дисплеев больше вредит живым клеткам, чем стабильное излучение высоковольтных линий электропередач.

Ученые формулируют свои выводы очень осторожно, хотя большинство экспериментов требует тщательной перепроверки, хотя категорично отрицать вредное воздействие бытовой техники нельзя. Сейчас никто не возьмется также преждевременно говорить и о существовании большого риска. В каждом случае, подчеркивают ученые, негативное влияние электромагнитного поля на здоровье человека, не выдерживает сравнения с вредом от курения и алкоголя.

Американские исследователи обследовали людей, которые работают недалеко от различных генераторов электромагнитных волн и также установили, что у многих из них замечено ослабление памяти, кроме этого, они быстро устают и страдают потерей аппетита. Было выявлено, что работники, имеющие вставные зубы, жаловались на появление металлического привкуса во рту в период работы [3].

Зарубежные исследования о влиянии электромагнитных волн на здоровье человека носят неоднозначный характер. В связи с этим отечественные ученые из НПО «Радон» начали исследования о взаимосвязи между местом жительства москвичей и заболеваемостью от возможного радиоактивного или электромагнитного излучения. Как известно в Москве предостаточно мест с такого рода источниками излучений. Особый акцент делается на предрасположенность к болезням и опухолям. Результаты работы позволят шире взглянуть на проблему, что позволит прогнозировать нежелательные последствия от воздействия электромагнитных волн на гены человека.

Исследования воздействия радиоволн на человека, наряду с отрицательными сторонами этой проблемы, помогли выявить и положительные, что позволило создать больницы для лечения с помощью установок высокочастотного прогрева. В основе лежит явление, вызывающее разогрев живых тканей при увеличении интенсивности воздействия радиоволн.

Радиоэлектроника получает все более широкое распространение во всех сферах жизни. Это заставляет ученых в разных странах искать эффективные методы защиты специалистов, которые вынуждены из-за специфики работы подолгу контактировать с приборами и оборудованием, излучающим электромагнитные волны. В результате

была разработана специальная ткань, одежда из которой надежно защищает от электромагнитных колебаний. Такая одежда отражает до 99,9% электромагнитных волн, приходящих от радиоэлектронной техники [4].

В свое время открытие Г. Герца произвело ошеломляющее впечатление, но в наши дни оказалась видна и его обратная сторона: негативное воздействие электромагнитного излучения на живые организмы, которое делает людей заложниками электромагнитных волн. Эти факты заставляют человечество иначе смотреть и на привычную радиоэлектронную аппаратуру, которая находится у каждого дома.

С началом научно-технической революции в жизнь людей внедрились новые изобретения: компьютеры, спутниковая связь, мобильные и радио-телефоны. Это увеличило количество источников электромагнитного излучения – появились радиорелейные и радиолокационные станции, телевизионные вышки. Людей все чаще стало интересовать влияние электромагнитных волн на организм человека. Электромагнитное излучение частотой 40 – 70 ГГц представляет огромную опасность для человека, так как здесь длина волны соизмерима с размерами клеток человека.

В начале 21 века связь со спутниками являлась самой высокочастотной – 11 ГГц. Но до земной поверхности доходили лишь микроватты, несмотря на то, что мощность передаваемого сигнала была большой. В 2009 году операторами мобильной связи была повышена частота связи между базовыми станциями до 25 ГГц. Это обеспечило более качественную мобильную связь и увеличило количество передаваемых данных. Резко увеличилось влияние электромагнитного излучения на организм человека на частотах 40 – 70 ГГц.

Электромагнитные устройства очень широко применялись и применяются в быту. Спустя некоторое время, после начала научно – технической революции, людей стал волновать вопрос о влиянии электромагнитных волн на организм человека. Все приборы, которые включаются в розетку и проводят ток – это источники электромагнитного излучения, которое пагубно действует на организм человека. На сегодняшний день, количество таких устройств возрастает в геометрической прогрессии, которые с одной стороны облегчают жизнь, но с другой – оказывающие негативное влияние на организм человека.

Современный человек очень часто находится под влиянием электромагнитных полей (ЭМП): на работе и дома на частотах 10 – 70 ГГц, те же компьютеры и бытовая техника, создающая ЭМП, влияют на организм не лучшим образом. Электромагнитные волны несут определенную энергию, которая при взаимодействии с веществом превращается в тепло. Превращение тепла – одно из немаловажных условий для жизнедеятельности живых существ, но при малых дозах.

Влияние электромагнитной волны на живой организм определяется:

- Частотой или длиной волны, фазовой скоростью распространения, поляризацией волны и т. д., или говоря иначе особенностями самого излучения;
- Свойствами биологического объекта, рассматриваемого в качестве среды, в которой распространяется волна – диэлектрическая проницаемость, электрическая проводимость, глубина проникновения волн и т.д.

Рассмотрим механизм воздействия электромагнитного излучения.

Электромагнитные волны насыщают воздух положительными зарядами, что вредно для человека. Поэтому необходимо как можно чаще проветривать помещение.

Основное влияние на биологическую реакцию оказывают следующие параметры ЭМП:

- интенсивность электромагнитных полей;
- частота излучения;
- длительность облучения;
- сочетание частот ЭМП;
- периодичность воздействия.

Сочетание этих параметров может быть опасным для детей и беременных женщин, а так же людей, с заболеваниями сердечно – сосудистой системы, центральной нервной и гормональной системы, людей с ослабленным иммунитетом, аллергиков. Люди, которые длительное время проводят в зоне излучения, часто жалуются на раздражительность, быструю утомляемость, ослабление мыслительных процессов, нарушение сна. Частое воздействие на организм может приводить к раковым заболеваниям и расстройствам нервной и сердечно – сосудистой системы.

При использовании мобильного телефона во время во время разговора воздействию в первую очередь подвергается головной мозг

человека, а также периферические рецепторы вестибулярного, зрительного и слухового анализаторов. Несущая частота большинства телефонов составляет 450-900 Мгц и эта длина волны сопоставима с линейными размерами головы человека. В этом случае происходит неравномерное поглощение излучения, что может приводит к образованию «горячих точек», чаще всего в центре головы. Длительное воздействие предельно допустимых доз излучения может дает существенные изменения биоэлектрической активности различных структур мозга, также может привести к расстройствам его функций, в том числе состояния кратковременной и долговременной памяти.

Еще один пример: микроволновая печь. Они занимаю довольно прочные позиции на кухнях у большинства людей, но помимо полезных сторон, микроволновые печи имеют и негативные.

Исследования выявили причины, которые свидетельствуют о вреде СВЧ – печей на организм человека:

Электромагнитное излучение (торсионные поля) – именно содержание торсионной компоненты является основным фактором отрицательного влияния микроволн на человеческий организм. Очень часто, человек может испытывать бессонницу, частые головные боли и повышенную возбудимость.

Температура – при постоянном и длительном использовании СВЧ – печей высокочастотное излучение начинает нагревать организм человека. Это тепловое взаимодействие может привести к помутнению и разрушению хрусталика глаза.

Воздействие излучения на пищу – при обработке пищи в СВЧ – печах может произойти ионизация молекул. Это влечет за собой изменения в структуре вещества. Микроволновая печь способна создавать соединения, которых нет в природе – радиолитические изменения – они и способствуют разрушению и изменению структуры веществ. СВЧ – лучи разрушают витамины D, C, E и уменьшают питательность и ценность пищи на 60% [2].

Излучение организма – микроволновые печи так же оказывают разрушительное влияние на клетки организма. Это чревато тем, что организм перестанет препятствовать проникновению в организм различных грибков и вирусов. Процессы регенерации клеток подавляются, пища, облученная в микроволновых печах, может вызвать злокачественные новообразования в пищеварительной системе человека [3].

Таким образом, электромагнитные поля, которые окружают человека в повседневной жизни, могут представлять серьезную опасность для его здоровья и требуют дальнейшего серьезного изучения.

Литература

1. Гохберг М.Б., Колосницын Н.И., Лапшин В.М. Электрокинетический эффект в приповерхностных слоях Земли //Физика Земли. 2009. № 8. С.13-19.
2. Елин А.М. Воздействие электромагнитных излучений на здоровье человека. Меры по обеспечению безопасности / А. М. Елин//Справочник специалиста по охране труда. -2007. -N 7. -С. 37-41.
3. Коптева Н.Н. Влияние электромагнитных волн на организм человека // Современные научные исследования и инновации. 2015. № 11 [Электронный ресурс]. URL: http://web.snauka.ru/issues/2015/11/58908.
4. Николаев С.Д., Сильченко Е.В. Защита человека от электромагнитного излучения при помощи тканей // Вестник Казанского технологического университета. 2015. Т. 18. № 15. С. 161-166.
5. Теодорович Н.Н. Основы функционирования комплексного интеллектуального здания // Промышленные АСУ и контроллеры. 2010. № 8. С. 21-22.
6. Теодорович Н.Н. Расчет передачи сигналов радиоволн для автоматизированных систем через материалы различной химической природы // Башкирский химический журнал. 2009. Т. 16. № 4. С. 175-177.
7. Теодорович Н.Н. Расчет передачи сигналов радиоволн для автоматизированных систем через материалы различной химической природы // Башкирский химический журнал. 2009. Т. 16. № 4. С. 175-177.

МОДЕРНИЗАЦИЯ СЕРИИ КА «ЭКСПРЕСС-АМ» ДЛЯ ВЕЩАНИЯ В K_A-ДИАПАЗОНЕ

Барначук Александр Владимирович, студент 3 курса кафедры Информационных технологий и управляющих систем
Научный руководитель: **Аббасова Татьяна Сергеевна**, к.т.н., доцент кафедры Информационных технологий и управляющих систем

Сформированы предложения по модернизации аппаратуры, разрабатываемой в Государственном космическом научно-производственном центре имени М.В. Хруничева. В качестве объекта исследования выбран КА серии «Экспресс-АМ». Проведен анализ методов повышения эффективности. Предложены методы расширения функциональных возможностей КА серии «Экспресс-АМ».

Спутниковая связь, частотные диапазоны, эквивалентная изотропно-излучаемая мощность.

MODERNIZATION SERIES SATELLITE "EXPRESS-AM" BROADCAST IN THE K_A-BAND

Baranchuk Alexander 3rd year student of the Department of information technologies and control systems
Scientific adviser: **Abbasov Tatiana,** Candidate of Technical Sciences, Associate Professor of the Department of information technologies and control systems

Formed proposals for the modernization of equipment, developed at the State Research and Production Space Center named after MV Khrunichev. As the object of study selected spacecraft series "Express-AM". The analysis methods to improve efficiency. Methods for expanding the functionality of the SC series "Express-AM".

Satellite connection, frequency ranges, equivalent isotropic radiated power.

Цель данной статьи – проанализировать растущие потребности государственных структур, регионов, а также населения страны в космических средствах и услугах на основе:

– расширения и повышения эффективности использования космического пространства для решения стоящих перед Российской

Федерацией задач в экономической, социальной, научной, культурной и других областях деятельности, а также в интересах безопасности страны;

– расширения международного сотрудничества в области космической деятельности и выполнения международных обязательств Российской Федерации в этой области, разработки, применения и поставок ракетно-космической техники;

– укрепления и развития космического потенциала Российской Федерации, обеспечивающего создание и использование требуемой номенклатуры космических систем и комплексов с характеристиками, соответствующими мировому уровню развития космической техники, а также гарантированный доступ и необходимое присутствие в космическом пространстве.

Основные задачи исследования:

– развитие, восполнение и поддержание орбитальной группировки космических аппаратов в интересах социально-экономической сферы, науки и безопасности страны (связь, телевещание, ретрансляция, дистанционное зондирование Земли, гидрометеорология, экологический мониторинг, контроль чрезвычайных ситуаций, фундаментальные космические исследования, космические микрогравитационные исследования);

– создание, развертывание и эксплуатация элементов российского сегмента международной космической станции для проведения фундаментальных и прикладных исследований, реализация долгосрочной программы научно-прикладных исследований и экспериментов, планируемых на российском сегменте международной космической станции;

– обеспечение функционирования российского сегмента международной спутниковой системы поиска и спасания КОСПАС – САРСАТ;

– создание перспективных средств выведения космических аппаратов;

– поддержание объектов космодрома Байконур и их развитие;

– обеспечение создания изделий ракетно-космической техники с характеристиками мирового уровня

Назначение КА серии «Экспресс-АМ»

Спутники серии «Экспресс-АМ» предназначены для ретрансляции теле- и радио-передач, а также для обеспечения

телеграфной и телефонной мобильной связи на территории Российской Федерации и других стран [11].

Для дальнейшего анализа был выбран КА «Экспресс-АМ44», внешний вид которого приведен на рисунке 1, а технические характеристики представлены в таблице 1.

Рисунок 1 – КА «Экспресс-АМ44»

Таблица 1 – Характеристика «Экспресс-АМ44»

Орбитальная позиция, град.:	11 з.д
Диапазон частот:	C-6/4; Ku-14/11; UHF-1,6/1,5
Кол-во ретрансляторов (в диапазоне, ГГц):	10(6/4), 54 (14/11), 1(1,6/1,5)
ЭИИМ, дБВт (в диапазоне, ГГц):	41…47 (6/4), 50/53 (14/11)
Мощность передатчиков, Вт:	100(6/4), 150(14/11), 85(1,6/1,5)
Масса стартовая/полезная нагрузка, кг:	2560/590
Мощность, Вт:	6770 (полезная нагрузка 4410)
Ресурс, лет:	12
Дата запуска:	февраль 2009
Ракета-носитель:	Протон-М, РБ Бриз-М.
Генеральный подрядчик (платформа):	ИСС, Alcatel Space (МСС-767)

Космический аппарат по заказу ФГУП «Космическая связь» создан НПО «Прикладная механика» им. М. Ф. Решетнева совместно с компанией Thales Alenia Space. Спутник «Экспресс-АМ44» предназначен для предоставления услуг телерадиовещания, телефонии, передачи данных, услуг мультимедиа, подвижной связи. Космический аппарат оборудован перенацеливаемыми антеннами, которые обеспечивают устойчивое покрытие стран Европы, Ближнего Востока, Африки и восточного побережья Америки.

Модернизация серии КА «Экспресс-АМ» для вещания в $К_а$-диапазоне

Все крупные консалтинговые компании мира утверждают, что основным двигателем мирового рынка спутниковой связи в настоящее время является услуга высокоскоростного

(широкополосного) доступа (ВСД, broadband access) в Ka-диапазоне частот в Internet. Под широкополосным каналом связи МСЭ (ITU-T I.113) понимает канал, в котором скорость передачи данных в прямом направлении составляет не менее 2 Мбит/с, при этом в обратном канале скорость не оговаривается [3].

K_a-диапазон - диапазон частот сантиметровых и миллиметровых длин волн, используемых в основном для спутниковой радиосвязи и радиолокации. По определению IEEE, этот диапазон простирается от 26,5 до 40 ГГц электромагнитного спектра (что соответствует длинам волн от 1,13 до 0,75 см). Название диапазона происходит от смеси английского и немецкого слов: «короткий» (нем. *kurz*) и «над» (англ. above), что указывает на положение K_a-диапазона: «над» K-диапазоном (18 — 26,5 ГГц).

Одна из основных областей применения K_a-диапазона это спутниковая связь.

В спутниковой связи этот диапазон называется *K_a*-диапазон *30/20 ГГц* и полосы частот, зарезервированные для этих целей, лежат между 18,3-18,8 и 19,7-20,2 ГГц для линии Спутник — Земля, и между 27,5 и 31 ГГц для линии Земля — Спутник. То есть фактически канал Спутник — Земля полностью лежит в K-диапазоне, а канал Земля — Спутник в K_a-диапазоне.

Среди российских космических аппаратов этот диапазон должен был использоваться в спутнике «Экспресс АМ4», выведенном в 2011 году на нерасчётную орбиту, транспондеры K_a-диапазона предусмотрены на спутниках «Экспресс АМ5» и «Экспресс АМ6».

Преимущество K_a-диапазона

Ka-диапазон устраняет проблему нехватки спутникового сегмента, которая сдерживала развитие спутниковой связи в последние несколько лет в Ku-диапазоне. Появление спутников K_a-диапазона в сочетании с многолучевой технологией обеспечило этой отрасли дополнительный частотный ресурс, использование которого обходится значительно дешевле, чем использование аналогичной емкости Ku- или C-диапазонов в традиционном использовании. Примером этого является европейский рынок, где использование Ka-диапазона обеспечивает существенно более высокую скорость передачи данных, доступную для конечного абонента, — до 20 Мбит/с — по привлекательной цене, при этом спутниковой емкости вполне достаточно для обслуживания сотен тысяч и даже миллионов абонентов в перспективе.

Спутники Ku- и С-диапазонов обычно используют широкие лучи, охватывающие целый континент или крупную страну, такую, например, как Россия. При этом передаваемые по этому лучу данные могут приниматься в любой точке этой зоны. Широкая зона обслуживания является преимуществом для корпоративных приложений или телевизионного вещания, но неэффективна для доступа в Интернет.

Спутники K_a-диапазона работают по-другому принципу: они используют много точечных лучей, каждый из которых покрывает заданный регион. Благодаря этому, используя один и тот же спектр, спутник Ка-диапазона способен передавать принципиально больше данных, чем традиционный спутник Ku-диапазона с широким контурным лучом. Примерно пропорционально числу лучей, умноженному на полосу частот, поддерживаемую в одном луче. И хотя спутники K_a-диапазона дороже в 2—3 раза, общая стоимость передачи данных в расчете на один бит информации для них оказывается значительно ниже, чем для спутников Ku-диапазона. Поэтому эта архитектура идеально подходит для обеспечения доступа в сеть Интернет.

Таким образом, при меньшей стоимости за один бит информации и большей пропускной способности, чем в случае спутников Ku-диапазона, спутники K_a-диапазона открывают новые возможности для развития отрасли спутниковых коммуникаций.

K_a-диапазон имеет широкие перспективы в России: применение этой технологии позволит быстро и сравнительно недорого обеспечить широкополосную связь во всех регионах Российской Федерации.

По нашему мнению, K_a-диапазон даст жителям России три основных преимущества:

Доступный широкополосный доступ для жителей пригородов больших городов, малых городов, сел и деревень, в которых отсутствуют оптоволоконные соединения. Основным достоинством K_a-диапазона является то, что он позволяет обеспечить всем желающим доступный высокоскоростной широкополосный доступ в Интернет, сравнимый по цене и качеству с перспективными наземными сетями. Сегодня россияне, живущие за пределами мегаполисов, автоматически оказываются в невыгодном положении. Обычно они не могут получить доступ в Интернет на тех же

скоростях, что и жители крупных городов. Кроме того, даже более медленный доступ в Интернет обычно обходится им дороже.

Доступ в Интернет для школ, правительственных учреждений и прочих государственных организаций на всей территории России. Отсутствие высокоскоростного доступа затрагивает не только частных граждан, но и государственные и общественные учреждения, возникает проблема организации государственных электронных услуг. Применение Ка-диапазона позволит обеспечить широкополосный доступ школам и правительственным учреждениям в любой точке России. В качестве примеров возможного применения Ка-диапазона можно назвать общегосударственные программы, потоковую передачу видео в учебных целях, общественные точки доступа по технологии Wi-Fi и высококачественные услуги электронного правительства.

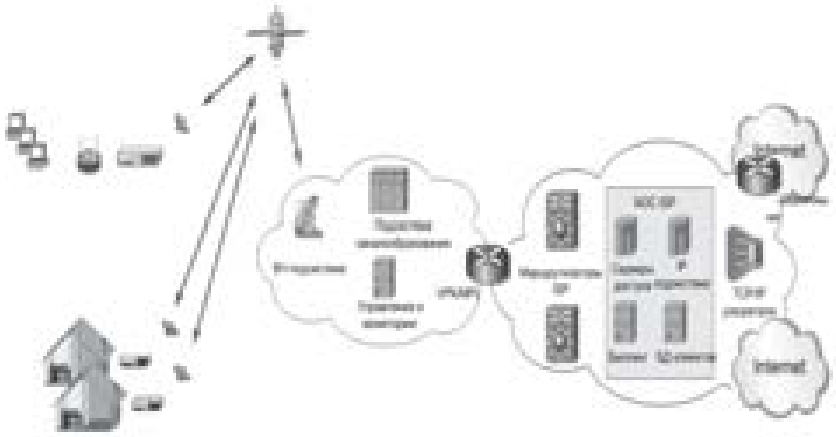


Рисунок 2 – Архитектура и топология спутниковой сети высокоскоростного (широкополосного) доступа в Internet

Мобильный широкополосный доступ в корпоративном и общественном секторе. Одним из достоинств $К_а$-диапазона является возможность его применения для обеспечения мобильного широкополосного доступа в Интернет. $К_а$-диапазон позволяет налаживать высокоскоростной доступ в поездах, автобусах и на самолетах. Возможность обеспечения высокоскоростной широкополосной связи на мобильных платформах также важна для вооруженных сил, служб экстренного реагирования и аварийно-спасательных операций.

Способы создания спутниковых систем многостанционного абонентского доступа в Internet в $К_а$-диапазоне.

На рисунке 2 представлена обобщённая архитектура спутниковой сети высокоскоростного доступа, включающая сеть доступа, сеть распределения (обеспечивает информационный обмен абонента с базовой сетью) и базовую сеть (предоставляет доступ в Internet).

На рисунке 2 обозначены: АЗС – абонентская земная станция. БД – база данных. ВЧ – высокочастотная часть базовой станции.

Расчет диапазона

Если передатчик или приемник настроен на определенную частоту, то можно говорить только об одной рабочей частоте. Если в процессе работы можно перестраивать рабочую частоту, то надо определить диапазон используемых частот, в пределах которого может осуществляться данная регулировка.

Как правило, в расчете диапазона чаще используют не частоту, а длину волны. Именно поэтому диапазоны классифицируют как: диапазоны ДВ (длинных волн), СВ (средних волн), КВ (коротких волн), УКВ (ультракоротких волн).

Чтобы рассчитать длину волны в частоту, нужно поделить на нее скорость света (300 000 000 м/с) согласно формуле 1.

$$F = c/\lambda \qquad (1)$$

где λ – длина волны (м), c – скорость света (м/с), F – частота (Гц).

С развитием техники и освоением новых частотных диапазонов, появились новые частотные диапазоны, такие как «сверхкороткие», «гиперкороткие» и т.п. [3-19].

Зависимость выходной мощности от входной

Во всех современных бортовых ретрансляторах в качестве усилительных выходных приборов используются либо лампы бегущей волны (ЛБВ), либо транзисторы.

Важнейшей характеристикой любого ретранслятора является амплитудная характеристика выходного усилителя, т.е. зависимость выходной мощности усилителя от входной мощности. Эта зависимость в целом имеет нелинейный характер (рисунок 3).

$$P_{вых}=f(P_{вх}) \qquad (2)$$

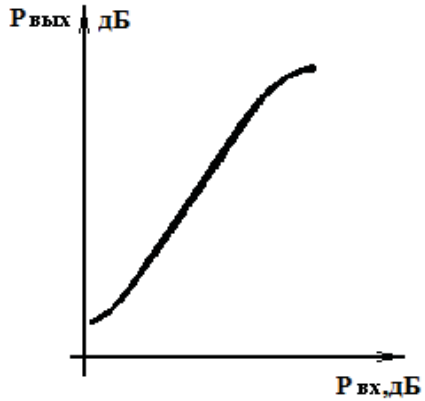


Рисунок 3 – Пример амплитудной характеристики усилителя мощности бортового ретранслятора

Начальная часть характеристики достаточно линейная, далее наступает так называемый участок насыщения. На этом участке характеристики выходная мощность практически не меняется от входной мощности.

Эта существенная деталь во многом определяет построение систем многостанционного доступа, уровень возникающих переходных искажений между парциальными каналами, реальный ЭИИМ спутника, его КПД.

Ещё одной особенностью выходной мощности на фазовую характеристику усилителя. Эта зависимость выражается как

$$K_\Theta = f(P_{вх}) \qquad (3)$$

где K_Θ – коэффициент АМ-ФМ преобразования.

Заключение

Проведен анализ назначения, задачи и характеристики КА «Экспресс-АМ44». Предложены организационные мероприятия, заключающиеся в добавлении частотного диапазона $К_а$. Представлены формулы расчета диапазона частот, зависимости выходной от входной мощности, влияния выходной мощности на фазовую характеристику усилителя.

Литература

1. Abbasova, T. S., Artyushenko, V. M., Samarov, K. L. Modern methods of processing of video information and evaluating the quality of

streaming video perception // Biosciences Biotechnology Research Asia. 2014. T. 11. C. 265-268.
2. Artyushenko, V. M., Abbasova, T. S. Increasing noise immunity of electric communication channels in high-speed telecommunication systems // Biosciences Biotechnology Research Asia. 2014. T. 11. C. 277-279.
3. Аббасов, А. Э. Совершенствование технологического процесса отработки и сборки приборов и устройств ракетно-космической техники: сб. тр. по материалам Отраслевой научно-технической конференции приборостроительных организаций Роскосмоса «Информационно-управляющие и измерительные системы – 2015». 26-27.03.2015 – [Текст] / Королёв МО.
4. Аббасова, Т. С. Восстановление и проверка корректности телеметрических данных [Текст] / Т. С. Аббасова, А. А Комраков // Информационно-технологический Вестник. – №2(04). – 2015. – С. 55 – 64.
5. Аббасова, Т. С. Совмещение управляющих и измерительных функций при интерактивном управлении телекоммуникационными системами [Текст] / Т. С. Аббасова // Информационно-технологический Вестник. – №2(04). – 2015. – С. 14 – 38.
6. Артюшенко, В. М. Анализ эффективности уменьшения межкабельных переходных помех в экранированных кабельных системах [Текст] / В.М. Артюшенко, К.А. Енин, М.Н. Буткевич // Электротехнические и информационные комплексы и системы. – 2009. – Т.5. – №1. – С.19-23.
7. Артюшенко, В. М. Комплекс полунатурного моделирования систем автоматического управления летательных аппаратов и ракетно-космической техники [Текст] / В. М. Артюшенко, Н. А. Васильев, Т. С. Аббасова // Сб. тр. Международной научно-практической Интернет-конференции «Современные образовательные технологии, используемые в очном, заочном и дополнительном образовании»: Финансово-Технологическая Академия. – Королёв: ФТА, 2013.
8. Артюшенко, В. М. Особенности отражения зондирующих сигналов радиотехнических устройств обнаружения от протяженных объектов сложной формы [Текст] / В.М. Артюшенко, В.И. Воловач // Школа университетской науки: парадигма развития. – 2012. №2-6. С.42-46.

9. Артюшенко, В. М. Оценка экономической эффективности использования автоматизированной системы распределения средств управления космическими аппаратами в условиях ресурсных ограничений [Текст] / В.М. Артюшенко, Б.А. Кучеров // Вестник Поволжского государственного университета сервиса. Серия: Экономика. – 2013. №5(31). С. 131-136.
10. Артюшенко, В. М. Повышение эффективности систем спутниковой связи путем оптимизации параметров земных станций [Текст] / В. М. Артюшенко, Т. С. Аббасова, Б. А. Кучеров // Радиотехника. – 2015. – № 2. – С. 76-82.
11. Артюшенко, В. М. Современные направления развития корпоративных сетей спутниковой связи [Текст] / В. М. Артюшенко, Т. С. Аббасова, Б. А. Кучеров // Двойные технологии. – 2014. – №3(68). – С.67–72.
12. Багров Лео. История картографии. — М., Центрполиграф, 2004. — 320с.
13. Багров Лео. История русской картографии. — М., Центрполиграф, 2005. — 524с.
14. Вокин, Г. Г. Космические услуги: особенности инфраструктурного обеспечения и потребления [Текст] / Г. Г. Вокин, Л. Г. Азаренко // Сервис в России и за рубежом, № 4(23) – 2011.
15. Данилова, А. Д. Научные исследования на базовой кафедре Финансово-технологической академии [Текст] / А. Д. Данилова, Т.С. Аббасова // сборник материалов Международной научно-практической конференции 24-25 апреля 2014 г. «Перспективы, организационные формы эффективность развития сотрудничества российских и зарубежных ВУЗов»: Королёв МО: Финансово-технологическая академия, ФТА, Изд-во «Канцлер», 2014. – С. 342 – 350 (512 с.) – ISBN 978-5-91730-388-8.
16. Кучеров, Б. А. Адаптация мощности земных станций узловой сети спутниковой связи при работе в стволе с прямой ретрансляцией [Текст] / Б. А. Кучеров // Двойные технологии, №1, 2015 г., с. 53 – 58.
17. Кучеров, Б. А. Проектные решения для автоматизированной системы распределения средств управления космическими аппаратами [Текст] / Б. А. Кучеров // Информационно-технологический Вестник. – №3(05). – 2015. – С. 91 – 99.
18. Панченко, В. А. Применение аддитивных технологий при проектировании изделий и блоков для ракетно-космических систем: тезисы докладов XX-ой научно-технической конференции молодых

ученых и специалистов – Россия, [Текст] / г. Королёв, Ракетно-космическая корпорация «Энергия» имени С.П. Королёва, 10-14.11.2014. – С. 400 – 402 (707 с.) (Россия)
19. Постников А. В. Развитие картографии и вопросы использования старых карт / Отв. ред. И. А. Федосеев. — М.: Наука, 1985. — 216 с.

ВОЗМОЖНОСТИ ИМПОРТОЗАМЕЩЕНИЯ ИНОСТРАННЫХ КОМПЬЮТЕРНЫХ КОМПЛЕКТУЮЩИХ

Наумушкин Василий Анатольевич, студент 1 курса кафедры Информационных технологий и управляющих систем
Научный руководитель: **Штрафина Елена Дмитриевна**, доцент кафедры Информационных технологий и управляющих систем

В политике России в последнее время произошли радикальные изменения, что коренным образом повлияло на внутренний рынок. Это связано с вводом санкций западными государствами, ограничивающие количество продукции и технологии, поступающие на Российский рынок. Известно, что Российская индустрия электроники находится в упадке уже долгое время и неспособна конкурировать с развитыми иностранными компаниями. Вместе с этим разрабатываются и внедряются законодательные проекты, обязующие закупать именно отечественную электронику.

Импортозамещение, процессоры, Российский рынок, комплектующие, Прикладная информатика.

POSSIBILITIES OF IMPORT SUBSTITUTION FOREIGN COMPUTER ACCESSORIES

Naumushkin Vasili, 1 st year student of the Department of information technologies and control systems
Scientific adviser: **Shtrafina Elena**, Associate Professor of the Department of information technologies and control systems

In recent years Russian policy has undergone radical changes that much affected the domestic market. This is due to the introduction of sanctions by Western countries, limiting the number of products and technologies that come to the Russian market. It is known that the Russian electronics industry has been in decline for a long time and is unable to compete with the advanced foreign companies. At the same time developed

and implemented legislative projects that require the purchase is domestic electronics.

Import substitution, the processors, the Russian market, components, Applied Informatics.

Человечество сегодня живет в эпоху повсеместного использования электронно-вычислительных средств. Начиная с 2009 года, в Российской экономике наблюдается рост потребления электроники практически во всех отраслях. Особой популярностью пользуются персональные компьютеры (ПК) (рис.1).

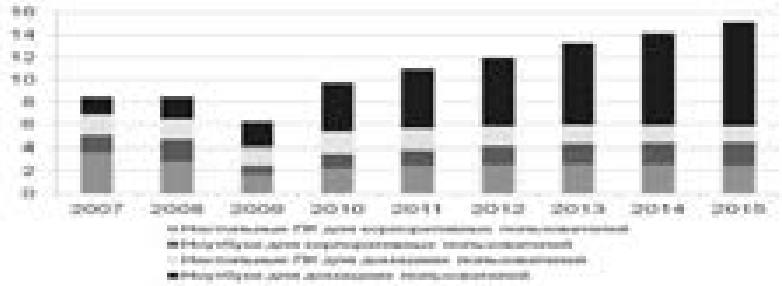


Рисунок 1 – Продажи Персональных компьютеров в России (млн.шт.)

При этом в условиях повышенного давления на российский рынок комплектующих, собственное производство давно находится в упадке. Однако в последнее время наметились некоторые изменения. Это связано с введением санкций западными государствами, ограничившими количество продукции и технологий на Российском рынке.

Толчком к развитию отрасли послужило Постановление №109 от 17 февраля 2016 года, в котором утверждены правила предоставления из федерального бюджета субсидий российским организациям на возмещение части затрат на создание научно-технического задела по разработке базовых технологий производства приоритетных электронных компонентов и радиоэлектронной аппаратуры.

Постановлением №110 от 17 февраля 2016 года утверждены правила предоставления из федерального бюджета субсидий российским предприятиям радиоэлектронной промышленности на компенсацию части затрат на уплату процентов по кредитам, полученным в российских кредитных организациях на реализацию

проектов по созданию инфраструктуры отрасли, в том числе кластеров в сфере радиоэлектроники.

Что касается программного обеспечения (ПО), то согласно постановлению Правительства "Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд", с 1 января 2016 года заказчики обязаны ограничить закупки ПО для государственных и муниципальных нужд программным обеспечением, включенным в реестр российского ПО.

Также существуют законодательные проекты. Так, Минкомсвязи готовит проект плана «гарантированных закупок российской гражданской микроэлектронной продукции на среднесрочную перспективу для вычислительной техники и аппаратно-программных комплексов». Документ разрабатывается во исполнение поручения премьер-министра Дмитрия Медведева от 29 октября 2015 года. По состоянию на 7 декабря 2015 года проект плана, по сообщениям информационного агенства TAdviser, проходит согласование в заинтересованных ведомствах.

Закупать вычислительную технику «на базе центрального процессора отечественного производства» должны будут федеральные органы власти и Госкорпорация «Росатом». План будет рассчитан на 2016-2018 годы.

Рассмотрим современный рынок отечественных комплектующих.

Процессоры

В России разработано как минимум два микропроцессора – «Эльбрус» и Baikal-T1. Также имеются опытные наработки Миландр, НИИСИ, Элвис, К211 и других.

I. «Байкал»

1. Процессоры «Байкал» рассчитаны в первую очередь на промышленную автоматику и телекоммуникационное оборудование нежели на серверы и стационарные компьютеры.

2. На данный момент практически отсутствуют полноценные разработки настольных компьютеров и серверов. Идет активное обсуждение с внутренними и внешними заказчиками.

3. Отсутствуют полностью Российские решения. Существуют только иностранные решения на базе Российского процессора.

4. Продукт исключительно коммерческий. Особенностей по безопасности или повышенной стабильности нет.

Тем не менее, процессоры «Байкал» будут востребованы. Рассмотрим характеристики:

- 2 супер-скалярных ядра P5600 MIPS 32 r5
- Рабочая частота 1,2 ГГц
- Кэш L2 1 Мбайт
- Контроллер памяти DDR3-1600

Интегрированные интерфейсы:

- 1 порт 10Gb
- PCIe Gen.3 x4
- 2 порта SATA 3.0
- USB 2.0
- Энергопотребление < 5 Вт
- Технологический процесс 28 нм
- Корпус 25x25 мм.

Стоимость ~ $60

Процессоры уже выпускаются в массовом производстве для более чем 100 Российских и иностранных компаний.

Производство процессорных модулей для массовых партий моноблока, как и материнских плат - Россия. Поставка механических компонентов ожидается из Юго-Восточной Азии. Сборку будут выполнять на российских предприятиях.

Используются в основном в маршрутизаторах и точках доступа, сетевых коммутаторах, шлюзах безопасности, концентраторах VPN.

Главная причина, по которой данные процессоры трудно назвать «импортозамещающими» - они выпускаются на Тайване на фабрике TSMC.

II. «Эльбрус»

Работы над архитектурой «Эльбрус» начались ещё в 1986 г. в коллективе Института точной механики и вычислительной техники (ИТМ и ВТ) им. С.А. Лебедева, в котором до этого были созданы советские высокопроизводительные комплексы «Эльбрус-1» и «Эльбрус-2». Разработка вычислительного комплекса «Эльбрус-3», которая велась под руководством Б.А. Бабаяна, была завершена в 1991 г. В этом вычислительном комплексе впервые были воплощены в жизнь идеи явного управления параллелизмом операций с помощью компилятора.

Начавшиеся с 1992 г. экономические изменения в России не позволили разработчикам «Эльбруса-3» завершить наладку комплекса. В том же 1992 г. коллектив разработчиков машин семейства «Эльбрус» выделился в компанию ЗАО «МЦСТ» и начал вести работы над микропроцессорной реализацией архитектуры «Эльбрус».

Вплоть до 2007 года МЦСТ выпускала лишь микропроцессоры с архитектурой SPARC и вычислительные системы на их базе. Собственная архитектура «Эльбрус» отошла на второй план. В период с 1997 по 2007 годы были выпущены четыре SPARC-микропроцессора: МЦСТ-R100, МЦСТ-R150, МЦСТ-R500 и МЦСТ-R500S. Также увидел свет и вычислительный комплекс «Эльбрус-90микро». Несмотря на свое название, к данной архитектуре система не имела никакого отношения.

Процессоры «Эльбрус» базируются на архитектуре VLIW (Very Long Instruction Word). VLIW является развитием RISC-архитектуры и суперскалярности. Особенностью VLIW является то, что в каждой команде может содержаться до 23 элементарных операций, которые должны исполняться параллельно. При этом задача распараллеливания возлагается на компилятор, в отличие от традиционных суперскалярных архитектур, где за распараллеливание отвечают аппаратные блоки процессора. Эффективность такого метода действительно выше. Компилятор способен анализировать исходный код гораздо тщательнее, чем аппаратура RISC/CISC-процессора, и находить больше независимых операций. Поэтому в архитектуре «Эльбрус» больше параллельно работающих исполнительных устройств, чем в традиционных решениях.

Самым последним представителем данного класса процессоров, находящийся на серийном производстве является Эльбрус-4С. В таблице 1 приведены основные характеристики процессора Эльбрус-4С.

Таблица 1 - Характеристики процессора Эльбрус-4С

Тактовая частота	800 МГц
Число ядер	4
Операций в такт (на ядро)	до 23
Пиковая производительность микросхемы (64 разряда, двойная точность)	25 Гфлопс
Технологический процесс	65 нм

В режиме эмуляции платформы x86 производительность ожидаемо немного снижается (примерно на 20-30 %). При этом становятся недоступны некоторые возможности «Эльбрус-4С».

В ближайшем будущем планируется выпуск процессоров Эльбрус-8С и Эльбрус-16С.

На базе этих процессоров уже реализованы решения.

- Сервер «Эльбрус-4.4» – стоечный сервер на базе микропроцессоров «Эльбрус-4С». Он содержит четыре процессора

«Эльбрус-4С», один или два южных моста КПИ. Общая производительность сервера составляет 200 Гфлопс одинарной точности.

- Персональный компьютер АРМ Эльбрус 401-РС работает на процессоре Эльбрус-4С, оперативная память от 24 до 96 Гбайт, обладает Интегрированной видеокартой на основе СБИС SiliconMotion SM718, Жесткий диск SATA 2.0 1000 ГБ.
- Моноблок КМ4-ЭльбрусЭкран 21” 1920*1080
  • Видеокарта 2D/3D*
  • Диски: SATA 3.5” + DVD (USB 2.0, WiFi, Bluetooth, DVI, GigabitEthernet, камера,микрофон)
- На базе процессора создан НТ-ЭльбрусS – высокопроизводительный защищенный ноутбук, выполненный в ударопрочном защищенном влагостойком корпусе. Предназначен для организации работы мобильного персонала в жестких условиях.

Работают данные продукты на разработанных внутри МЦСТ:

- Программа начального старта (BIOS)
- Собственной ОС «Эльбрус» на основе ядра GNU/Linux
- Оптимизирующих компиляторах языков С, С++, Фортран, Java, средства сборки, отладки, профилирования, библиотеки

III. ГУП НПЦ ЭЛВИС

Предприятие «Элвис» создано в марте 1990 года на базе структурного подразделения научно-производственного объединения «ЭЛАС», выполнявшего в 1960-80 гг. передовые разработки в области космической электронной техники: от разработки собственных САПР до полностью законченных аппаратно-программных бортовых систем управления и обработки информации космического базирования серий «Салют», в частности, функционировавших на борту станции «МИР».

Портфельная компания РОСНАНО «ЭЛВИС-НеоТек» разработала и выпустила семантический процессор VIP-1 (Video Intelligence Processor).

VIP-1 — это принципиально новая 6-ядерная гетерогенная система на кристалле (SoC), ориентированная на стремительно растущие рынки семантического анализа изображений и компьютерного зрения (среднегодовые темпы роста этого рынка составляют более 25%).

Основные характеристики:

рабочая частота: – кодирование: 2 канала FullHD

1,2 ГГц в нормальных условиях (OverDrive)/600 МГц (VelCore-01A);	(1080p) 60 fps или 1 канал UltraFullHD (2160p) 30 fps;
1 ГГц в нормальных условиях /500 МГц (VelCore-01A);	– декодирование: 2 канала FullHD (1080p) &
– H.264: BP/MP/HP Encode and Decode;	60 fps или 1 канал UltraHD (2160p) & 30 fps.
– MPEG-4: SP/ASP Encode/Decode;	встроенное ядро графического процессора GPU
– MPEG-2: SP/MP Encode/Decode;	1080p с 4x сглаживанием; встроенный 8KB
– JPEG (MJPEG) Baseline Encode/Decode.	Техпроцесс 40 нм

Основной компонент VIP-1 — специализированный видеопроцессор, работающий со стереоизображениями и справляющийся с кодированием и декодированием видеопотоков HD и 4K со скоростью до 60 кадров в секунду. Как утверждают разработчики, процессор способен конкурировать с новейшими версиями процессоров Rockchip, MediaTek, Allwinner, Freescale, Qualcomm, выполненными по технологии 28 нанометров с 6-8 универсальными ядрами.

Кроме видеопроцессора в чип входит 2-ядерный ARM Cortex A9 с частотой 1 ГГц, ядро графического процессора, двухъядерный кластер процессора обработки сигналов и изображений и встроенное ядро навигационного приемника, поддерживающее три системы навигации — GLONASS, GPS и китайскую BeiDou.

IV. АО «ПКК Миландр»

«ПКК Миландр» - российская компания-разработчик и производитель микроэлектронной элементной базы, ориентированной на использование в изделиях с повышенными требованиями к надёжности (авиакосмическая техника, спецтехника и т. п.). Большинство изделий компании поставляются как с приёмкой «1» (приёмкой ОТК), так и с приёмкой «5» (приёмкой заказчика).

Основные виды деятельности:

- разработка и производство интегральных микросхем с проектными нормами до 0,040 мкм;
- тестирование, измерения и испытания микросхем, в том числе импортных;

- разработка и производство электронных модулей и блоков аппаратуры;
- разработка и производство счетчиков электрической энергии;
- дистрибуция и поставка электронных компонентов для радиоэлектронной аппаратуры гражданского и специального назначения.

Двухъядерный микроконтроллер с 32-разрядным RISC-ядром 16-разрядным DSP-ядром.

Особенности микроконтроллера:

- 32-битное RISC-ядро с тактовой частотой до 100 МГц;
- Блок аппаратной защиты памяти MPU;
- Рабочий температурный диапазон от -60 до +125.

На данный момент Миландр является одним из ведущих предприятий по производству микроконтроллеров и в скором будущем выведет на рынок собственные процессоры.

Материнские платы

Материнская плата «Монокуб-М»формата Mini-ITX оснащена слотом расширения PCI-Express v.1.0, гигабитным портом Ethernet, разъёмами SATA 2.0, IDE (CompactFlash), портами USB 2.0 и RS-232, видеовыходами VGA и DVI, а также входами/выходами общего назначения (GPIO). Разработчик МЦСТ.

Использование и применение

1. Байкал

Первым продуктом, построенным на «Байкал-Т1», стала отечественная система управления станками СЧПУ «Ресурс-30»

В начале 2016 года начал выпускаться ПК «Таволга терминал» на базе процессора «Байкал». Работать он будет на ОС LinuxDebian 8.

Baikal-T1 будет использоваться при создании принтеров, копировальных аппаратов, точек доступа Wi-Fi, в системах управления транспортом и других устройствах.

2. Эльбрус.

«Объединенная приборостроительная корпорация» (ОПК) создала технику для защищенной спецсвязи стран СНГ на базе «Эльбруса».

ОПК, входящая в госкорпорацию «Ростех», приступила к разработке вычислительной техники на базе нового российского 8-ядерного микропроцессора «Эльбрус-8С». Компания планирует разработать на его основе настольные рабочие станции, ноутбуки и

серверы. Все эти устройства и оборудование смогут гарантировать отсутствие шпионских закладок и придут на смену зарубежным образцам, которые эту гарантию дать не могут, сообщили в ОПК.

ФГУП НИИ «Восход» закупает серверное оборудование, построенное на отечественных процессорах «Эльбрус» и работающее на одноименной ОС, для сегментов государственной системы изготовления, оформления и контроля паспортно-визовых документов нового поколения.

Компьютеры на базе процессора Эльбрус активно используются в ПФР и внутренних ведомствах. Процессоры найдут применение в ВПК РФ.

3. ГУП НПЦ ЭЛВИС

Процессор VIP-1 можно применять в различных мобильных и мультимедийных системах — он упакован в корпус 19x19 мм и потребляет около 3 ватт. Прежде всего процессор нацелен на рынок IP-камер со встроенным интеллектом, объем которого оценивается в $10 миллиардов. Для России это первая система мирового уровня, спроектированная по 40 нанометровому техпроцессу, включая дизайн микросхемы и системное программирование.

4. Миландр

Микросхемы Миландр оптимизированы для применения в телекоммуникациях или других областях, требующих мультипроцессорной обработки. Используется в системах связи, локаторах, мобильных терминалах, базовых станциях связи, захвате данных от АЦП и управлении внешними устройствами через интерфейсные микросхемы.

На основании изложенного выше, можно сделать следующие выводы:

1. Российское производство комплектующих обладает достаточным потенциалом для успешного развития.

2. В России есть разработки, которые по своим характеристикам не уступают, а некоторые превосходят, свои западные аналоги.

3. Российское государство активно поддерживает отечественного производителя.

4. Российские технологические наработки в последнее время переходят в фазу развития массового производства.

5. В ближайшее время Российская высокотехнологичная продукция будет ориентирована на государственные нужны.

6. Российское производство медленно, но верно ориентируется на внутренний рынок и преодолевает технологическое отставание от западных компаний.

Литература

1. Постановление №109 от 17 февраля 2016 г. [Электронный ресурс] http://government.ru/media/files/5EQPfInTN3SqALKppKcX0DY
2. Постановление об установлении запрета на допуск программного обеспечения от 16 ноября 2015г. № 1236 [Электронный ресурс] http://government.ru/media/files/ac872y0wqioFnrRUeTnpGjEav
3. Постановление Правительства РФ от 17.02.2016 № 110 [Электронный ресурс] https://www.consultant.ru/document/
4. Указ Президента Российской Федерации от 31 декабря 2015 года N 683 [Электронный ресурс] http://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html
5. Государственная поддержка российских производителей электронных компонентов и радиоэлектронной аппаратуры [Электронный ресурс] http://goo.gl/mtlwAk
6. Архитектурные особенности и области применения современных российских микропроцессоров семейств Эльбрус и МЦСТ-R
7. [Электронный ресурс] http://goo.gl/5qpiqF
8. Краткое описание архитектуры Эльбрус [Электронный ресурс] http://www.elbrus.ru/arhitektura_elbrus
9. В продажу поступили ПК и серверы на базе процессоров «Эльбрус-4С» [Электронный ресурс] https://habrahabr.ru/company/ua-hosting/blog/258235/
10. Медведев поручил федеральным ведомствам гарантировать закупку российских процессоров [Электронный ресурс] http://goo.gl/k2yqxZ
11. Обзор архитектуры отечественного процессора «Эльбрус-4С» [Электронный ресурс] http://www.ferra.ru/ru/system/review/elbrus-4c-processor/
12. «ОПК» Создала технику для защищенной спецсвязи стран снг на базе «эльбруса» [Электронный ресурс] http://opkrt.ru/index.php/news/386-opk-sozdala-tekhniku-dlya-zashchish
13. Компьютеры с российским процессором появятся в Пенсионном фонде [Электронный ресурс] https://www.vedomosti.ru/technology/
14. Обзор Российских процессоров [Электронный ресурс] http://www.koshcheev.ru/2012/07/17/processory-made-in-russia/

15. Продукция Миландр [Электронный ресурс] http://milandr.ru/uploads/Products/product_231/Katalog_big.pdf
16. Российская компания ЭЛВИС-НеоТек представила 40 нм процессор VIP-1 [Электронный ресурс] https://geektimes.ru/post/

LINUX- СИСТЕМЫ В ОБРАЗОВАНИИ

Сураев Антон Александрович, студент 3 курса кафедры Информационных технологий и управляющих систем
Научный руководитель: **Исаева Галина Николаевна**, к.т.н., доцент кафедры Информационных технологий и управляющих систем

Проблема внедрения современных информационных технологий в образовательный процесс является актуальной на сегодняшний день. В данной статье рассматривается один из вариантов оптимизации локальной вычислительной сети (ЛВС) образовательного учреждения. Приводятся сравнительные характеристики программных систем, которые могут улучшить качество образовательного процесса, повысить уровень безопасности ЛВС и упростить доступ к ресурсам учреждения учащимися и сотрудниками.

Образование, ЛВС, программное обеспечение, операционная система.

LINUX SYSTEMS IN EDUCATION

Suraev Anton, 3rd year student of the Department of information technologies and control systems
Scientific adviser: **Isaeva Galina**, Candidate of Technical Sciences, Assistant Professor of the Department of information technologies and control systems

The problem of the introduction of modern information technologies in the educational process is relevant today. This article discusses one of the options to optimize the local area network (LAN) of the educational institution. The comparative characteristics of software systems that can improve the quality of the educational process increase the LAN security and simplify access to the resources and staff of the institution students.

Education, LAN, software, operating system.

Благополучие и эффективное использование ресурсов любого региона зависит, в большей степени от того, кто ими управляет. И насколько компетентны кадры, насколько они владеют современными программными и информационными технологиями, зависит качество жизни города и региона.

Наш университет является одним из главных поставщиков кадров для предприятий города Королёва и Московской области, поэтому образовательная база наших студентов должна быть всесторонняя и современная.

Особенно это касается умения освоить и использовать новые вычислительные системы и технологии. Мир не стоит на месте и технологии развиваются не по дням, а по часам. Сегодня мало владеть основами компьютерной грамотности, а надо уметь уверенно пользоваться информационным пространством всемирной сети Интернет, региональными сетями, локальной сетью нашего университета.

Локальные вычислительные сети постоянно требуют модернизации и обновления, чтобы справляться с современными потоками информации и обеспечивать интерактивный образовательный процесс в реальном времени. Но финансовый ресурс любого образовательного учреждения невелик, бюджет ограничен, поэтому модернизация на аппаратном уровне не всегда возможна. Выходом из подобной ситуации может быть модернизация системного программного обеспечения на персональных компьютерах (ПК), входящих в ЛВС [1, 2, 5, 7].

Основой системного программного обеспечения любой вычислительной системы является операционная система (ОС). И здесь заслуживают внимания две линейки операционных систем, на которых может быть построена ЛВС образовательного учреждения. Широко распространенная и всеми известная Windows-подобная ОС и, бесплатная и малораспространенная, - Linux – подобная ОС. Есть и другие современные известные системы, такие как Mac OS. Но для этой ОС требуется специальное дорогостоящее аппаратное обеспечение, что для бюджетного учреждения не всегда доступно, как упоминалось выше. На рисунке 1 приведена диаграмма, на которой показана популярность (в процентах ко всему рынку ОС в нашей стране) различных операционных систем [9].

Windows – подобные операционные системы начали свое широкое распространение с Windows 3.1. Эта линейка операционных

систем стала чуть ли не унифицированной, а к нашему времени почти незаменимой. Более 90% разработчиков программного обеспечения ориентируются именно на нее, делая разнообразные программные продукты, работающие под управлением этой ОС. Она стала самой востребованной системой для массового пользователя ПК, используемой для работы и досуга. Но большинство программных продуктов, создаваемых для данной ОС, являются платными. Как и сама Windows, собственно. Из-за этого появилось пиратство, а с ним и масса путей попадания вирусов, не считая самих взломанных программ пользователей. А так, как государственные стандарты «заставляют» покупать только лицензионные продукты, то образовательные учреждения не всегда в состоянии закупить все необходимые программы для управления сетью и контролем обучения.

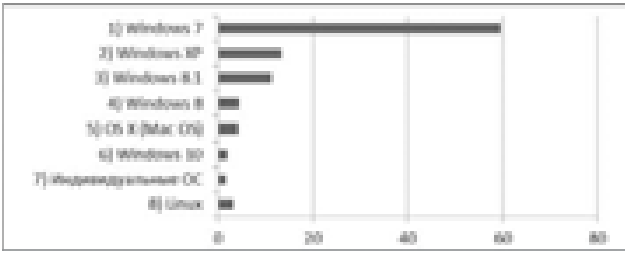


Рисунок 1 - Использование операционных систем в Российской Федерации

В связи с этим, многие организации обращают внимание на такой продукт, как Linux. Linux не является широко распространенной операционной системой, однако она имеет ряд преимуществ [6].

Во-первых – это бесплатная операционная система. Это основной плюс для бюджетных учреждений, так как все проблемы упираются в финансы.

Кроме того, в Linux присутствуют аналоги основных офисных и мультимедийных решений, что позволяет с легкостью перейти на данную ОС без малейших затруднений.

В данной операционной системе имеется возможность кастомизации (изменения) операционной системы, так как в ОС Linux изначально открытое ядро. Такое свойство операционной системы позволяет опытным пользователям настраивать ее так, чтобы было удобно работать с различными прикладными программами в данной

ОС, модифицировать интерфейсные и сервисные функции операционной системы [6].

Если сравнивать по объёмам оперативной памяти, необходимой для комфортной работы системы, то, в отличие от Windows, данная операционная система занимает меньше памяти, что благоприятно влияет на производительность каждого рабочего места (или рабочей станции) по отдельности и ЛВС в целом [3].

Стоит отметить стабильность системы, в связи с иной, чем в Windows файловой структурой, поэтому процедура дефрагментации диска не проводится так часто, как в Windows. Ещё одним плюсом является то, что операционная система Linux самостоятельно и централизованно обновляет все программные продукты, установленные на ПК, в том числе и саму ОС.

По этим характеристикам у Windows большинство программных продуктов «просит обновление»: часть обновляется автоматически, а часть ждет, пока пользователь не решит эту проблему. Таким образом, по поводу обновления ПО, Linux более стабильна чем Windows.

Если брать во внимание параметры безопасности использования этого системного ПО, то уровень безопасности данной ОС также выше, чем у альтернативной рассматриваемой ОС [6].

Таблица 1 - Отрицательные аспекты Windows и Linux

Microsoft Windows	Linux
Высокая стоимость операционной системы и программного обеспечения	Малая распространенность (3-4% пользователей)
Недостаточная оптимизация системы	Малое количество поддерживаемого программного обеспечения
Большое количество вирусов	

Таблица 2 - Положительные аспекты Windows и Linux

Microsoft Windows	Linux
Постоянная поддержка пользователей (сайт Microsoft, различные форумы и т.д.)	Бесплатный контент (в том числе, и сама операционная система)
Большое количество поддерживаемого программного обеспечения	Стабильность системы (малое количество сбоев, системных ошибок)
Распространенность	Малый расход ресурсов (физических)
	Кастомизация
	Простота в обновлении и управлении программными ресурсами

Все приведенные доводы в пользу возможности перехода к Linux-подобной операционной системе в локальной сети малобюджетного образовательного учреждения подтверждаются и

аспектами сильных и слабых сторон рассматриваемых линеек операционных систем, представленных в таблицах 1 и 2.

Чтобы показать возможность модернизации локальной вычислительной сети бюджетного образовательного учреждения, за счёт оптимизации программного обеспечения и системы в целом была смоделирована следующая ситуация (рисунок 2).

В образовательном учреждении имеется 3 этажа, в которых расположены: 1 сервер, 2 компьютерных класса по 11 компьютеров в каждом (10 для учеников, один для учителя), 27 компьютеров учителей (по 9 единиц на этаж), компьютер библиотекаря, компьютер врача, 2 компьютера секретаря и директора. В сумме выходит 42 компьютера.

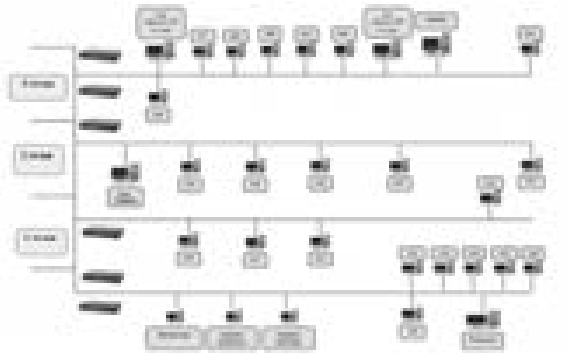


Рисунок 2 - Схема ЛВС виртуального образовательного учреждения

Создана сеть с топологией «Звезда». Между этажами и на каждом из них стоит по свитчу по 44 порта со скоростью передачи данных 100Мбит/с (по 2 на этаж). Итого - 6 шт. На севере на данный момент стоит операционная система Windows Server 2008, на ПК – Windows 7 Professional.

Переход на Linux-подобной операционной системе начинается непосредственно с персональных компьютеров всей сети. За основу можно взять операционную систему Ubuntu (построенной на ядре Linux) и установить универсальный пакет программ для образовательных учреждений Ubuntu Education Pack.11.04. Для серверного решения подойдёт дистрибутив, специализированный для семейств Ubuntu – Ubuntu Server [3].

Приведенная модель виртуального образовательного учреждения получится недорогой и функциональной, и как вариант, в

случае недостаточных ресурсов в учреждении, может быть использована для модернизации ЛВС и переходу к современному программному обеспечению.

Кроме того, если говорить о дальнейшем повышении качества обучения и образовательного процесса, то можно приобрести платный программный продукт, который, по моему мнению, улучшил бы качество управления системой обучения не только в университете, но и колледжах, входящих в наш университет. Это программный продукт Moodle [4]. Данное программное решение позволило бы реализовать возможность дистанционного обучения, контроля знаний, дополнительного развития творческой деятельности учащегося при необходимости обучения на дому. Преподавателям позволило бы использовать различные современные варианты подачи материала слушателям.

Программа обладает огромными возможностями, русской локализацией (Комплект Русский Moodle 3kl), дружественным интерфейсом для создания курсов и удобным, легким управлением и навигацией. Отрицательный аспект данного решения – это цена (около 66 000 рублей), включающая в себя: сам продукт, полную установку и локализацию под сервер заказчика, гарантию обслуживания на 1 год, консультации по поводу обслуживания и использования программного продукта [8].

Таким образом, подводя итог исследований в области повышения качества обучения в бюджетном образовательном учреждении, которое ограничено в финансовых возможностях, можно сделать выводы:

-при проведении модернизации ЛВС можно использовать свободно-распространяемое системное ПО, такое, как операционные системы линейки Linux;

-для повышения современного функционала образовательной системы необходимо применять новые информационные технологии, одной из которых является недорогой программный продукт - Комплект Русский Moodle 3kl.

Литература

1. Артюшенко, В. М. Информационные технологии и управляющие системы: монография [Текст] / В.М. Артюшенко, Т.С. Аббасова, Ю.В. Стреналюк, В.И. Привалов, В.И. Воловач, Е.П. Шевченко, В.М. Зимин, Е.С. Харламова, А.Э. Аббасов, Б.А. Кучеров

/под науч. ред. док. техн. наук, проф. В.М. Артюшенко. – М.: Издательство «Научный консультант», 2015. – 185 с.
2. Артюшенко В. М. Системный анализ в области управления и обработки информации: монография [Текст] / В.М. Артюшенко, Т.С. Аббасова, Ю.В. Стреналюк, Н.А. Васильев, И.М. Белюченко, К.Л. Самаров, В.Н. Зиновьев, С.П. Посеренин, Г.Г. Вокин, А.П. Мороз, В.С. Шайдуров, С.С. Шаврин /под науч. ред. док. техн. наук, проф. В.М. Артюшенко. – Королёв МО: «МГОТУ», 2015. – 168 с.
3. Бражук А. И.: Сетевые средства Linux - Национальный Открытый Университет «ИНТУИТ»: 2016. - 148 с.
4. Возможности системы moodle и актуальность ее применения в сфере образования Ю.В. Позняк, А.С. Гаркун, А.А. Царева Белорусский государственный университет Электронный ресурс. Режим доступа: http://elib.bsu.by/bitstream/123456789/3591/1/Vozmozn_Moodle. pdf
5. Исаева Г.Н., Пахомов Д.А. Возможности современных языков программирования высокого уровня. Стр.167-175 Современные информационные технологии [Текст] Сборник научных трудов под науч. ред. док. тех. наук, проф. В.М. Артюшенко. – М.: Издательство «Научный консультант», 2015. – 190 с.
6. Костромин В.Д., Свободная система для свободных людей (обзор истории операционной системы Linux) –М.: 2005. – 86 с.
7. Панюкова С.В. Использование информационных и коммуникационных технологий в образовании М: Издательский центр «Академия», 2010, -224 с.
8. Электронный ресурс: http: //www.opentechnology.ru/ products/ russianmoodle
9. Электронный ресурс: http://gs.statcounter.com/

КАФЕДРА МАТЕМАТИКИ И ЕСТЕСТВЕННОНАУЧНЫХ ДИСЦИПЛИН

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ОБЕСПЕЧЕНИЯ РАБОТОСПОСОБНОСТИ ЭКИПАЖЕЙ В ДЛИТЕЛЬНЫХ КОСМИЧЕСКИХ ЭКСПЕДИЦИЯХ

Дятлова Дарья Андреевна, студентка 3 курса кафедры Экономики
Научный руководитель: **Вилисов Валерий Яковлевич**, д.э.н.,
профессор кафедры Математики и естественнонаучных дисциплин

Работа посвящена современному состоянию, методам и инструментальным средствам мониторинга, оценивания и прогнозирования показателей состояния здоровья человека и его способностей выполнять профессиональные обязанности. Приведен анализ существующих гаджетов и программных средств, позволяющих отслеживать показатели здоровья персонала предприятий. Анализ существенных взаимосвязей показателей и факторов, определяющих необходимую работоспособность и производительность персонала, позволяет эффективно организовать режим труда и отдыха сотрудников.

Персонал, показатели здоровья, мониторинг, биомаркеры, предикторы, прогнозирование.

THE APPLICATION OF INFORMATION TECHNOLOGIES TO PROVIDE EFFICIENCY THE CREWS IN LONG SPACE MISSIONS

Diatlova Daria, 3rd year student of the Department of economics
Scientific adviser: **Vilisov Valery**, Doctor of Economic Sciences,
Professor of the Department of mathematics and natural sciences

The work is devoted to the current state, methods and tools of monitoring, evaluation and forecasting of indicators of the state of human health and its ability to perform professional duties. An analysis of existing gadgets and software to track indicators of health personnel of enterprises. An analysis of the substantive relationship metrics and factors that determine the necessary performance and staff productivity, allowing to organize work and rest of employees effectively.

Staff, health indicators, monitoring, biomarkers, predictors, prediction.

Введение

Космические агентства различных стран кроме текущих программ освоения ближнего и дальнего космоса проводят и перспективные исследования, направленные на отдаленную перспективу. К числу перспективных проектов относят и пилотируемые экспедиции к дальним планетам, в т.ч. к Марсу. Одна из проблем, которую предстоит решить, заключается в создании систем и технологий, помогающим космонавтам поддерживать не должном уровне состояние здоровья и работоспособность.

Даже самые богатые страны мира не могут похвастаться идеальной системой здравоохранения. Сколько бы ни вкладывалось средств в медицину, всегда ощущается нехватка квалифицированных кадров. В некоторых случаях врачи просто не успевают оказать помощь пострадавшему. К сожалению, критические состояния при хронических заболеваниях наступают не по расписанию. И если вовремя принять все медицинские меры, то пациенту можно спасти жизнь.

Для того чтобы осуществлять постоянный мониторинг состояния здоровья пациента, современная медицина нуждается в устройствах, которые снимают те или иные показатели с человеческого организма в режиме реального времени. А в случае каких-либо угрожающих изменений устройство подает сигнал пациенту, или его лечащему врачу. Процесс внедрения таких гаджетов в медицинскую практику уже успешно запущен в ряде стран [1].

Поводом для выполнения данной работы послужил выполняемый в настоящее время российско-канадско-американский проект "*CosmoCard PHM* для космонавтов" по разработке информационно-методических средств мониторинга состояния здоровья космонавтов в дальних комических экспедициях. В рамках проекта планируются космические эксперименты на международной космической станции (МКС). «МГОТУ» является участником данного проекта.

Целью настоящей работы является анализ имеющихся на сегодня гаджетов, приложений и технологий, помогающих людям отслеживать показатели их здоровья. При этом рассматриваются два аспекта:

- чисто медицинский, в рамках которого необходимо оценивать физиологические показатели человека и принимать меры при их отклонении от нормы или при соответствующем прогнозе;
- профессиональный, при котором человек является сотрудником, показатели жизнедеятельности которого должны отвечать некоторым нормативным требованиям.

Рассматриваются и некоторые методические аспекты работы с данными, поступающими в процессе мониторинга в соответствующие хранилища, цели и задачи, которые могут решаться на полученном поле данных.

Анализ состояния разработок в сфере мониторинга здоровья

Мониторинг пациентов с различными видами заболеваний представляет собой активно растущий сегмент рынка. Только в Западной Европе и США численность пациентов, страдающих от одного или нескольких хронических заболеваний и нуждающихся в услугах дистанционного мониторинга, составляет 200 млн. человек [11]. К 2020 г. аналитики прогнозируют [2], что в сетях мобильной связи будет функционировать более 60 млн. устройств мониторинга здоровья пациентов, а объем рынка в денежном выражении составит 18 млрд. долл. Наибольшим спросом будут пользоваться средства дистанционного мониторинга, предназначенные для пациентов с сердечной аритмией, диабетом и хроническими заболеваниями легких.

Одним из наиболее перспективных направлений в развитии медицинских технологий является мобильная телемедицина (mHealth). Отрасль здравоохранения представляет значительный интерес для операторов связи, поскольку здесь есть возможность предложить дополнительные электронные медицинские услуги потребителям. Операторы сотовой связи в последние годы наращивают активность в данной области. Сети нового поколения за счет более высокой пропускной способности значительно расширяют возможности передачи медицинских данных по сетям мобильной связи, что позволяет обеспечить их оперативную доставку, целостность и конфиденциальность. Кроме того, современные каналы связи позволяют организовывать прямую видеоконференцсвязь между пациентом и доктором или оператором, осуществляющим психологическое тестирование или измерение физиологических показателей.

Развитие сотовых сетей нового поколения (LTE) и всеобщее проникновение смартфонов обеспечит надежную технологическую базу для развития таких проектов. Мобильная медицина в данном случае позволяет пациентам самостоятельно использовать различные медицинские приборы для контроля своего здоровья, которые способны передавать данные метрии в медицинские центры.

Для платформ iOS и Android написаны тысячи приложений, позволяющих решать множество медицинских задач. Различные дополнительные устройства и датчики превращают обычный смартфон в медицинский прибор, позволяющий проводить достаточно точные обследования. С помощью iPhone можно снять ЭКГ, измерить давление, провести офтальмологическое обследование или оценить риск заболевания раком кожи. Причем с приемлемым уровнем погрешности. Полученные данные можно в реальном времени передать профильному специалисту и сразу же получить консультацию.

Уже сегодня владельцы смартфонов и других мобильных устройств могут установить приложения, контролирующие параметры физиологического состояния. Так, например, существует программа, которая анализирует родинки на теле человека. Для этого нужно лишь сфотографировать родинку. Такое приложение поможет вовремя обратиться к врачу и предупредить раковые заболевания на коже.

Существуют специальные приложения, с помощью которых можно проверять слух, зрение, следить за состоянием пульса, а также узнать полную информацию о любом лекарственном средстве.

Перечень некоторых из программных средств, доступных пользователям, приведен в табл. 1.

Многие научно-исследовательские институты и медицинские компании активно включились в процесс разработки устройств и приложений для смартфонов и планшетов.

Эксперты прогнозируют, что при массовом использовании медицинских гаджетов в будущем удастся существенно снизить нагрузки на медицинские учреждения. Такие устройства избавят врачей от многих рутинных и плановых осмотров, и позволят специалистам уделять время тем пациентам, кто больше остальных нуждается в медицинской помощи.

В настоящее время уже есть приборы, позволяющие кардиологу видеть в реальном времени в любом месте земного шара

электрокардиограмму пациента на своем смартфоне, наблюдать за его ритмом.

Таблица 1 – Приложения для мониторинга здоровья

Характеристика приложений	Android	iOS
Измерение частоты пульса	• Heart Rate Monitor • Instant Heart Rate • Runtastic Heart Rate	• Runtastic Heart Rate • Cardiio – пульсометр
Проверка слуха	• Проверка слуха	• Petralex Слуховой Аппарат • Проверка слуха • Слуховой помощник
Проверка зрения	• Проверка зрения (andrew.brusentsov) • Проверка зрения (healthcare4mobile)	• Проверка зрения HD • Проверка зрения вблизи
Информация о лекарственных средствах	• Лекарства и их аналоги • Справочник лекарств и болезней • MedBox – Справочник лекарств	• Лекарства бесплатно • Лекарства от А до Я Lite

Уже появились сенсоры для непрерывного измерения уровня сахара в крови. Сейчас они вживляются под кожу. Но в будущем имплантация будет не нужна т.к. достаточно будет задать допустимый диапазон уровня сахара, выше 75 и ниже 200, и контролировать, делая регулярные замеры при помощи сенсора для непрерывного измерения уровня сахара, что окажет существенную помощь диабетикам.

Арсенал разнообразной датчиковой (сенсорной) аппаратуры расширяется стремительными темпами. Причем технологии анализа все больше становятся неинвазивными – не требующими внедрения в организм.

В табл. 2 приведены некоторые из доступных сегодня приборов такого рода.

Темпы развития современных технологий позволяют вплотную подойти к реализации идеи оказания медицинских услуг, основанных на персональных особенностях каждого человека. Среди основных возможностей, предоставляемых данным подходом, можно выделить:

- эффективную диагностику и раннее выявление болезни;

Таблица 2 – Гаджеты для мониторинга здоровья и их характеристика

Прибор	Краткая характеристика
Zephyr BioPatch™ Wireless Device	Беспроводное устройство для мониторинга пациентов (ЭКГ, сердцебиение: реальное и его тренд, биопроводник, который измеряет задержку жидкости, что очень исключительно важно при мониторинге сердечной недостаточности, температура, дыхание, кислород, положение и движения тела)
Электронный пластырь-термометр	Устройство для постоянного измерения температуры человеческого тела, небольшие изменения которой способны показать, как именно работают сосуды, и помочь диагностировать заболевания сердечно-сосудистой системы.
Fitbit Force	Это элегантный браслет из легкого, почти невесомого пластика. Он разбудит вас мягкой, но настойчивой вибрацией на запястье. В течение дня он посчитает количество шагов, преодоленных ступеней, пройденных километров, потраченных калорий, а ночью – сколько часов вы проспали и как часто ворочались (качество сна). Статистика, анализ динамики и вся палитра функционала социальных сетей в комплекте.
iHealth BP5	Беспроводной монитор кровяного давления. iHealth BP5 надевается на предплечье, словно нарукавная повязка, и не имеет больше никаких дополнительных модулей. Его монитором становится соединенное с ним iOS-устройство, которое при помощи бесплатного приложения от iHealth не только выведет данные текущего измерения давления, но и покажет его расширенную статистику.
Lumoback	Монитор осанки, который умеет не только наблюдать и информировать. Его главное предназначение – периодически напоминать вам о том, что правильная осанка – дело несложное, но требующее постоянного контроля.

- выбор адекватного лечения, в том числе использование безопасных и эффективных для каждого конкретного пациента препаратов;
- более эффективную терапию, мониторинг лечения и определение прогноза.

Задачи анализа состояния здоровья

Кроме использования упомянутых средств в чисто медицинской практике, очень актуальной является задача мониторинга физиологических и психологических показателей здоровых людей, чьи профессии связаны с риском ущерба другим людям или/и риском существенных техногенных аварий. В числе таких профессий – водители автобусов, машинисты электропоездов, пилоты самолетов,

операторы АЭС, космонавты и др. Для этих категорий персонала важными являются параметры режима труда и отдыха (РТО). Известно много случаев, когда несоблюдение должного РТО случались крупные аварии, обусловленные усталостью или другими факторами, снижающими показатели работоспособности персонала.

Таким образом, важными являются задачи мониторинга и прогнозирования состояния персонала для обеспечения пребывания наиболее важных показателей на уровнях не хуже допустимых норм.

В зарубежной литературе [1-10], имеющей отношение к техническим приложениям существует направление деятельности, называемое Prognostics & Health Management (PHM), которое можно, применительно к техническому контексту, перевести как Прогнозирование и управление работоспособностью технических систем. В этой сфере наработан существенный задел по выявлению, распознаванию и прогнозированию неисправностей, что позволяет, не дожидаясь отказов и поломок, обеспечивать необходимый уровень работоспособности систем. Эти же "технократические" подходы могут быть перенесены и на сферу медицинского и психологического мониторинга персонала. Данное направление будем называть PHM персонала (PHM-P). В нем могут решаться следующие задачи:

1. мониторинг показателей;
2. поддержание показателей в заданном диапазоне (стабилизация);
3. оценка потенциальных (предельных) возможностей персонала;
4. поддержание экстремальных возможностей персонала.

Задачи 1-й и 3-й групп являются оценочными, хотя и могут содержать в своем составе тестирующие воздействия на человека, позволяющие получить необходимые оценки.

Задачи 2-й и 4-й групп помимо оценивания содержат и элементы выработки управляющих воздействий, направленных на обеспечение необходимых значений показателей.

Развернутый перечень подзадач первой и второй групп, как правило включает следующие:

- измерение показателей состояния здоровья в реальном времени с накоплением статистики на больших интервалах времени, в том числе регулярное самотестирование;
- обработка данных измерений в реальном времени специальными алгоритмами;

• интеграция данных измерений, полученных от различных датчиков и путем психологических тестов, вычисление значимых корреляций между показателями;

• вычисление предикторов и биомаркеров ухудшения здоровья и соответствующее изменение режима труда и отдыха (питания, сна и т.п.);

• выявление и отслеживание негативных тенденций с предварительным уведомлением субъекта мониторинга или менеджеров;

• вывод результатов мониторинга посредством дружественного интерфейса и их представление пользователю, не владеющему медицинскими знаниями и навыками.

Важными элементами, обеспечивающими эффективность решения этого перечня подзадач, являются *биомаркеры* и *предикторы*.

Биомаркеры – это такие показатели, которые можно объективно измерить, и которые могут служить в качестве индикатора физиологических и патологических биологических процессов или фармакологических ответов на терапевтические вмешательства. К ним относятся, например, значения веса, давления крови, частота пульса, показатели анализов крови, УЗИ, МРТ и т.п.

Биомаркером может быть вещество, введенное или обнаруженное в организме, что может указывать на конкретное болезненное состояние или присутствие чужеродных организмов (например, наличие специфических антител может указывать на конкретную инфекцию.

В настоящее время уже используются тысячи биомаркеров для оценки состояния здоровья и их перечень постоянно растет.

В зависимости от целей исследования субъекта различают следующие основные типы биомаркеров:

• предупредительные - используются для выявления склонности к возникновению того или иного заболевания;

• верификационные - подтверждают заболевания на субклинической стадии;

• диагностические - использующиеся для идентификации определенного заболевания;

• биомаркеры состояния - используются для определения стадии заболевания;

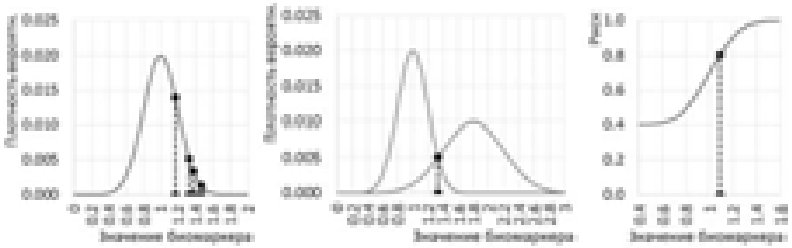
• прогностические - используются для оценки прогноза развития заболевания, его возможного исхода и оценки эффективности лечения;

• фармакодинамические - используются для выявления определенного фармакологического ответа, необходимого, например, для оптимизации дозировок лекарств.

Предиктором называют биомаркер, позволяющий предсказать благоприятный или неблагоприятный исход заболевания или эффективность лечения.

Методы обработки и представления данных мониторинга здоровья

Логика использования биомаркеров в статике (в отдельные не связанные между собой моменты времени) приведена на рис.1



а) б) в)

Рисунок 1 – Значения биомаркеров в норме и не в норме: а) допустимые уровни доверительной вероятности; б) дискриминационные пределы нормы и ненормы; в) порог риска

Однако, часто на практике при мониторинге показателей отдельного человека или узкой группы людей возникает задача отслеживания показателей в динамике, их приближение или удаление от критических границ. Это может позволить прогнозировать на некоторый момент в будущем значение показателя и, возможно, предотвратить его переход в критическую зону.

Область прикладной статистики, в которой рассматриваются математические аспекты обработки данных биомаркеров и подготовка вариантов выводов, называется биоинформатикой. В ее арсенале средств разнообразные методы и модели, в частности:

- статистическое оценивание;
- распознавание образов;
- кластерный анализ;

- многомерный регрессионный анализ;
- последовательное оценивание (в том числе байесовское) и др.

Важная роль в деле обеспечения точности распознавания состояния человека и в прогнозировании его изменений отводится:

1. комплексным биомаркерам, т.е. взаимозависимостям, обеспечивающим синергетический эффект (например, влияние психологического состояния на физиологические показатели и т.п.);
2. учет влияния на значение показателя дополнительных факторов (возраст, тренированность, состояние внешней среды и т.п.).

Таким образом, в терминах прикладной статистики взаимосвязь показателей и факторов можно представить разными способами, в частности, в виде:

- многомерной регрессионной модели (множественной регрессии);
- задачи распознавания образов;
- задачи кластеризации и др.

Анализ данных мониторинга здоровья

В продолжительных космических экспедициях одной из важных задач, определяющих работоспособность экипажа, является поддержание физической формы. Уровень тренированности определяется, в том числе, таким показателем, как время восстановления частоты сердечных сокращений (ВВЧСС) после нагрузок. У тренированных людей ВВЧСС меньше, чем у нетренированных. Диапазон значений ЧСС у тренированных людей может варьироваться от 50 до 240 ударов в минуту в зависимости от нагрузки. Прибором, позволяющим оценить текущее значение ВВЧСС могут быть велоэргометры, беговые дорожки и другое специальное оборудование, позволяющее задавать необходимые тестовые нагрузки и измерять текущие показания ЧСС, а по ним вычислять с помощью стандартных или специализированных программных средств оценки ВВЧСС.

Современное оборудование, используемое для мониторинга физиологических показателей, часто позволяет записывать измеряемые данные на носители, отправлять их по радиоканалам (Bluetooth, WiFi и др.) или пересылать по сети интернет по заданному адресу.

В зависимости от нагрузки и степени тренированности графики изменения ЧСС при восстановлении имеют, например, вид, приведенный на рис. 2.

Для каждого из таких графиков может быть вычислена оценка единственного показателя, отражающего скорость прихода в норму ЧСС. И именно этот показатель может служить одним из биомаркеров уровня тренированности человека. По его значениям можно назначать поддерживающие физические упражнения.

Процесс восстановления ЧСС обычно можно представить экспоненциальной зависимостью вида:

$$f(t) = a + (d - a)e^{-\text{ит}} + \text{е}, \qquad (1)$$

где a – значение ЧСС в норме; d – значение ЧСС сразу после снятия нагрузки; и – коэффициент скорости успокоения ЧСС; е – случайная составляющая измерений. По измерениям текущих значений целевого показателя ЧСС $f(t)$ можно вычислить оценку коэффициента и, например, методом наименьших квадратов [11-13] с помощью специализированных или универсальных программных средств.

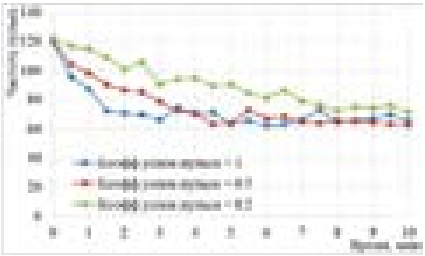


Рисунок 2 – Измерения процесса восстановления ЧСС после снятия нагрузки для разных уровней тренированности

Мониторинг коэффициента и может служить основанием для коррекции уровня тренированности человека т.к. от нее зависит работоспособность и устойчивость к воздействиям окружающей среды.

В спортивной практике кроме ЧСС измеряют и ряд других биомаркеров, в частности, частоту и глубину дыхания и др. Число возможных биомаркеров, значения которых будут измеряться в продолжительных космических экспедициях, может быть достаточно большим и разнообразным. Так текущая физическая активность может быть измерена с помощью миниатюрных акселерометров

(например, трехосевых микромеханических датчиков ускорения [13-15]), вшитых в одежду в разных местах – на руках, ногах, голове и др. Эти датчики смогут по радиоканалам передавать данные для регистрации и обработки. Статистический анализ этих данных (например, дисперсионный, корреляционный, кластерный и др.) может показать, какие части тела получают спонтанную (в процессе текущей деятельности) или специальную нагрузку.

Подобные биомаркеры (факторы, входные переменные) в процессе непрерывного мониторинга должны увязываться с некоторыми целевыми показателями (выходными переменными), от них зависящими или с ними существенно коррелированными. Целевые показатели могут отражать уровень работоспособности, вероятность ошибки, способность сосредоточиться, устойчивость к заболеваниям (сила иммунитета) и т.п.

В процессе мониторинга по текущим данным могут быть построены зависимости показателей (L) от вектора факторов ($\bar{x} = [x_1, x_2, \cdots, x_n]^T$) в виде линейных или нелинейных регрессионных зависимостей $L = f(\bar{b}, \bar{x})$, где $\bar{b}$ –вектор параметров.

Если эту зависимость строить в линейной форме и в нормированных переменных, то большие значения коэффициентов b_i будут свидетельствовать о том, что соответствующий им фактор (биомаркер) x_i является предиктором, т.е. существенно предсказывает изменение показателя. А значит, в таком случае, по значению предиктора можно принимать управляющие (корректирующие) меры, не зная самого значения показателя.

Выводы

С учетом представленного в работе анализа возможна, например, следующая технология мониторинга, анализа и управления здоровьем группы людей в определенной профессиональной сфере, в частности в длительных космических экспедициях.

1. Для построения действенных методов прогнозирования состояния субъекта, исполняющего свои определенные профессиональные обязанности, необходимо собрать на реальной контрольной группе достаточный объем статистических данных, отражающих норму и/или патологию (ненорму).

2. На поле реальных данных исследуемой предметной области выявить наиболее значимые биомаркеры, предикторы, а также наиболее эффективные их комплексы.

3. Исследовать зависимости значимых биомаркеров и/или предикторов (в том числе и комплексных) от факторов внешней и внутренней среды, существенно влияющих на их прогностические свойства для обеспечения максимальной точности оценивания и прогнозирования.

4. Исследовать и определить характеристики точности оценивания и прогнозирования показателей изменения состояния субъектов исследуемой группы.

5. Исследовать степень возможной персонифицируемости моделей и методик анализа состояний конкретного субъекта.

Литература

1. Popov, A. PHM for Astronauts – A New Application / A.Popov, W. Fink, A. Hess // Annual Conference of the Prognostics and Health Management Society 2013. – pp. 1-8.

2. Вараксин, А.Н. Статистические модели с коррелированными предикторами в экологии и медицине / А.Н. Вараксин, В.Г. Панов, Ю.И. Казмер. – Екатеринбург: Изд-во Урал. ун-та. 2011. – 92 с.

3. Вилисов, В.Я. Адаптивная транспортная логистическая модель / В.Я. Вилисов, С.Е. Сабо // Информационно-технологический вестник. - 2014. - № 2. - С. 40-45.

4. Вилисов, В.Я. Адаптивный выбор управленческих решений. Модели исследования операций как средство хранения знаний ЛПР [Текст] / В.Я. Вилисов. - Саарбрюккен (Германия): LAP LAMBERT Academic Publishing. - 2011. - 376 с.

5. Вилисов, В.Я. Адаптивный подход к распределению ограниченных материальных ресурсов в производственных системах [Текст] / В.Я. Вилисов // Менеджмент в России и за рубежом. - 2007. - №5. - С. 10-19.

6. Вилисов, В.Я. Анализ динамики обучения робота в условиях нестационарности критериев модель / В.Я. Вилисов // Информационно-технологический вестник. - 2014. - № 2. - С. 34-39.

7. Вилисов, В.Я. Анализ эффективности обучения робота в условиях целевой нестационарности [Текст] / В.Я. Вилисов // Вибрационные технологии, мехатроника и управляемые машины. Сборник научных статей по материалам XI Международной научно-технической конференции: в 2 частях. - 2014. - Часть 2. - С. 282-287.

8. Вилисов, В.Я. Марковская модель обучения робота целесообразному поведению / В.Я. Вилисов // Информационно-технологический вестник. - 2015. - № 4. - С. 11-18.

9. Вилисов, В.Я. Транспортная модель, аппроксимирующая предпочтения ЛПР [Текст] / В.Я. Вилисов // Прикладная информатика. - 2010. - № 6 (30). - С. 101-110.
10. Вилисов, В.Я. Управление переключениями тарифных планов сотовой связи [Текст] / В.Я. Вилисов // Управление большими системами. - Выпуск 40. - М.: ИПУ РАН. - 2012. - С. 221-237.
11. Мирошниченко, И.И. Биомаркеры в современной медико-биологической практике // И.И. Мирошниченко, С.Н. Птицына / Биомедицинская химия, 2009 том 55, вып. 4, с. 425-440.
12. Пастухова, Ю.И. Модель волатильности валютного рынка [Текст] / Ю.И. Пастухова, Г.И. Муджири, А.Б. Яцкевич // Сборник статей Международной научно-практической конференции. Уфа, 2015. С. 36-38.
13. Самаров, К.Л. Финансовая математика: учебное пособие [Текст] / К.Л. Самаров. - Москва: Альфа-М. - 2005. - 77 с.
14. Сидоренкова, И.В. Конфликты критериев при отборе инвестиционных проектов: экономико-математический анализ [Текст] / И.В. Сидоренкова // Вопросы региональной экономики. - 2014. - Т.19. - №2. - С. 78-83.
15. Сидоренкова, И.В. Оптимизация позиций участников форфейтной операции [Текст] / И.В. Сидоренкова // Вопросы региональной экономики. - 2015. - Т.22. - №1. - С. 82-86.
16. Яцкевич, А.Б. Экспертные методы в инвестиционных конкурсных процедурах [Текст] / А.Б. Яцкевич, О.Н. Борисова // «Экономические аспекты развития российской индустрии в условиях глобализации 2/2015». - Труды международной научно-практической конференции. - М: Университет машиностроения, 2015 г. - С. 79-81.

ЖЕСТКИЕ И МЯГКИЕ МАТЕМАТИЧЕСКИЕ МОДЕЛИ В ЭКОЛОГИИ

Карпова Наталья Михайловна, студентка 3 курса кафедры Информационных технологий и управляющих систем
Научный руководитель: **Сидоренкова Ирина Владимировна**, старший преподаватель кафедры Математики и естественнонаучных дисциплин

В работе поставлена задача определения критического значения квоты вылова байкальской нерпы. Для решения задачи была использована логистическая модель роста. Рассмотрены условия

сохранения устойчивого объема популяции при различных параметрах добычи нерпы.

Модель роста, популяция, устойчивость.

HARD AND SOFT MATHEMATICAL MODELS IN ECOLOGY

Karpova Natalia, 3rd year student of the Department of information technology and control systems
Scientific adviser: **Sidorenkova Irina**, Senior Lecturer of the Department of mathematics and natural sciences

In the task of determining the critical value of the catch quotas of the Baikal seal. Logistic growth model was used to solve the problem. The conditions for the conservation and sustainable population size at different settings seal prey.

Growth model, population, sustainability.

Введение. Байкальская нерпа (Pusa Siberika – лат.) – единственный в мире вид тюленя, живущий в пресной воде. Байкальская нерпа является эндемиком Байкала. Упоминание о ней есть в отчетах первых землепроходцев, пришедших сюда в первой половине XVII в. Научное описание впервые сделано во время работы 2-й Камчатской, или Великой Северной, экспедиции, руководимой В. Берингом. Охота на байкальскую нерпу велась с древности и проводится сейчас. Для коренного населения это неотъемлемая часть местной культуры природопользования. Наряду с узаконенной охотой по-прежнему происходит браконьерство. Особенно жестоко ведется охота на детенышей нерпы в возрасте до нескольких месяцев, несмотря на то, что это запрещено законом. У нерпы естественных врагов, кроме человека, нет. В настоящее время по данным Лимнологического института озера Байкал, а также организации Гринпис, популяция нерпы находится в угнетенном состоянии и стареет. Сложная и богатая экосистема озера очень уязвима, испытывает тяжелые последствия нерационального лова и охоты.

Постановка задачи. Используя статистические данные о численности популяции байкальской нерпы, определить критическое значение квоты вылова.

Решение задачи. Простейшая модель роста – это известная модель Мальтуса:

$$\dot{m} = km, \qquad (1)$$

Где, m(t) – масса популяции, а коэффициент k - характеристика среды обитания. Она приводит к экспоненциальному росту популяции с течением времени. Эта жесткая модель не реализуется на практике (по крайней мере, в течение продолжительного периода). При больших m конкуренция за ресурсы приводит к уменьшению k, и жесткая модель Мальтуса должна быть заменена мягкой моделью:

$$\dot{m} = k(m)m, \qquad (2)$$

простейшим примером которой служит ***логистическая*** модель:

$$\dot{m} = b(a-m)m. \quad (3)$$

Эту модель и будем использовать для решения поставленной задачи. Коэффициент a характеризует емкость среды обитания, а коэффициент b – прирост популяции. Выбором системы единиц m и t можно добиться равенства коэффициентов a и b единице, т.е. прийти к уравнению:

$$\dot{m} = m - m^2. \qquad (4)$$

Однако полученные для этого уравнения выводы останутся справедливыми и при любых значениях коэффициентов a и b (с точностью до числовых значений констант) и даже для широкого класса моделей с различными убывающими функциями $k(m)$.

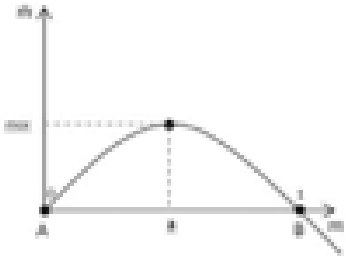


Рисунок 1 - Зависимость скорости роста популяции $\dot{m}$ от массы m

На рис. 1 точки A и B – стационарные (скорость равна 0).

Дифференциальное уравнение имеет решение вида $t = -\frac{1}{ab}\ln\left|\frac{a}{m} - 1\right| + c$, зависимость *m(t)* может быть построена графически.

Модель предсказывает, что с течением времени устанавливается стационарный режим B, который устойчив: большая популяция уменьшается, меньшая увеличивается. На практике должны наблюдаться затухающие колебания около прямой y = B.

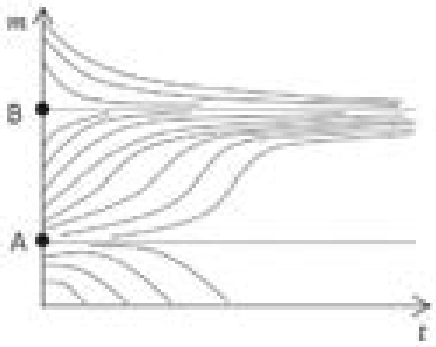


Рисунок 2 - Зависимость массы популяции от времени при разных начальных условиях

Посмотрим теперь, как сказывается на судьбе популяции внешнее воздействие (охота, рыболовство и т.д.) с интенсивностью ***v***:

$$\dot{m} = m - m^2 - v\,.$$

Расчеты показывают, что ответ резко меняется при некотором критическом значении квоты ***v***. Для жесткой модели это v =1/4.

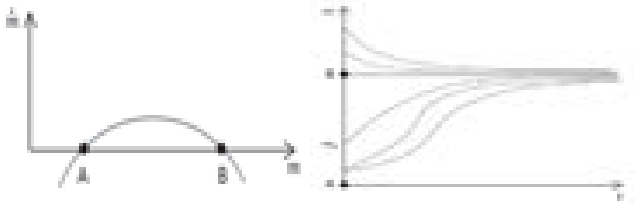


Рисунок 3 - Изменение массы популяции при *v* < ¼

На рис. 3 квота ***v*** мала, состояние B устойчиво, популяция меньше, чем необлавливаемая, но она легко восстанавливается при малых отклонения m от равновесного значения B. Состояние A неустойчиво: если вследствие каких-либо причин (браконьерства или мора) размер популяции упадет хоть немного ниже уровня A, то в

дальнейшем популяция хоть и медленно, если отличие от A невелико) будет уничтожено полностью за конечное время.

Если квота ν больше критической, то популяция уничтожается за конечное время, как бы велика она не была в начальный момент.

Опасность уничтожения согласно логистической модели появляется тогда, когда неустойчивое состояние A приближается к устойчивому состоянию B.

Из сказанного видно, что выбор значения параметра ν является чрезвычайно важным моментом управления эксплуатации популяцией m.

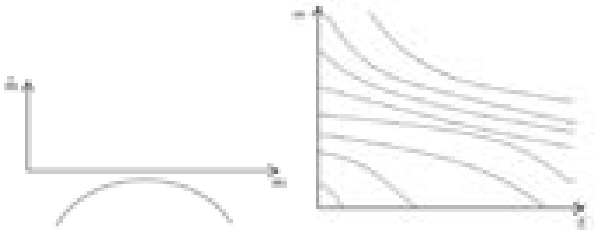


Рисунок 4 - Изменение массы популяции при $\nu > ¼$

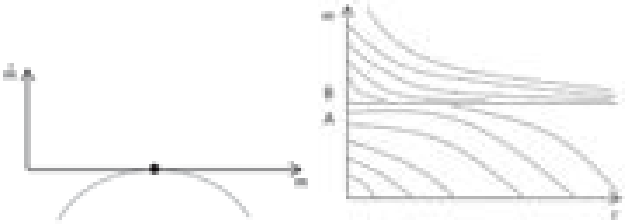


Рисунок 5 - Изменение массы популяции при $\nu = ¼$

Оптимизация приводит к выбору именно критического значения c, при котором эксплуатируемая популяция еще не уничтожается, а доход достигает максимума. На рис. 5 видно, что произойдет при таком «оптимальном» выборе. При любом начальном значении m >1/2, с течением времени эволюционная кривая выйдет на стационарный режим A = B = 1/2, который неустойчив. Небольшое случайное уменьшение m приведет к полному уничтожению популяции за конечное время.

По данным статистики наблюдений за популяцией байкальской нерпы 1970 – 2015гг., значение коэффициента b установлено равным 0,00094. Емкость озера Байкал определена на уровне 120 000 особей.

Источники статистических данных:

-Государственный доклад Министерства природных ресурсов и экологии «О состоянии озера Байкал и мерах по его охране» 2003-2015гг.;

-Отчет экспедиции Гринпис 2000-2001гг.;

-Данные Лимнологического института Сибирского отделения РАН;

-Данные Востсибрыбцентра.

Критическое значение квоты определяется из условия $\dot{m} > 0$: ***v = 3 380***.

Выводы

1. Официальная квота не превышает полученного значения показателя, за исключением периода 1977-1981гг. (см. рис. 6), когда проводился не имевший аналогов «научно-производственный эксперимент по оценке состояния популяции нерпы в условиях увеличенного промыслового изъятия». Однако, по оценкам экспертов, незаконный вылов нерпы превышает разрешенный в 3-5 раза. Популяция находится в угнетенном состоянии, к тому же средний возраст популяции растет вследствие вылова в первую очередь детенышей до года.

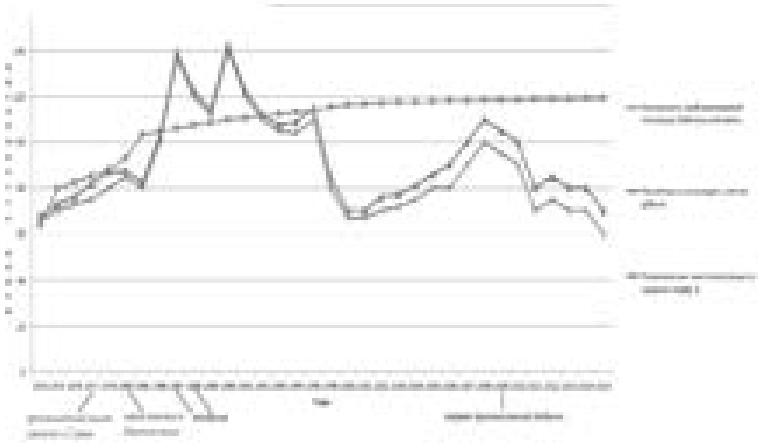


Рисунок 6 - Численность популяции байкальской нерпы

2. Международная Конвенция СИТЕС, участником которой является и Россия, относит тюленей к видам, находящимся под угрозой исчезновения, торговля которыми может оказать на их существование неблагоприятное влияние. Добыча тюленей должна

быть разрешена только в исключительных обстоятельствах. Конвенция регулирует вопросы международной торговли этими животными, и подобные нормы включены в нее не просто так. Преамбула Конвенции гласит, что «*Народы и государства являются и должны быть наилучшими хранителями их собственных дикой фауны и флоры*».

Литература

1. Арнольд, В.И. Мягкие и жесткие математические модели. – М.: МЦНМО. – 2004. – 32 с.
2. Вилисов, В.Я. Особенности многокритериального выбора инвестиционных проектов [Текст] / В.Я. Вилисов, И.В. Сидоренкова // Перспективы, организационные формы и эффективность развития сотрудничества ВУЗов стран Таможенного союза и СНГ, Сборник научных трудов Международной научно-практической конференции. - 2013. - С. 319-327.
3. Ивашев-Мусатов, О. С. Начала математического анализа. - М. : Наука. - 1988. - 288 с.
4. Никонова, Ю.Ю. О плотности распределения страховых выплат [Текст] / Ю.Ю. Никонова, Ю.И. Пастухова // Обозрение прикладной и промышленной математики. - 2008. - Т.15. - №1. - С. 162-163.
5. Пастухова, Ю.И. Модель волатильности валютного рынка [Текст] / Ю.И. Пастухова, Г.И. Муджири, А.Б. Яцкевич // Сборник статей Международной научно-практической конференции. Уфа, 2015. С. 36-38.
6. Пастухова, Ю.И. Об одной задаче принятия решений в рекламном бизнесе [Текст] / Ю.И. Пастухова, А.А. Дмитриева // Обозрение прикладной и промышленной математики. - 2007. - Т.14. - № 6. - С. 1130-1131.
7. Самаров, К.Л. Финансовая математика: учебное пособие [Текст] / К.Л. Самаров. - Москва: Альфа-М. - 2005. - 77 с.
8. Сидоренкова, И.В. Конфликты критериев при отборе инвестиционных проектов: экономико-математический анализ [Текст] / И.В. Сидоренкова // Вопросы региональной экономики. - 2014. - Т.19. - №2. - С. 78-83.
9. Сидоренкова, И.В. Методы теории игр в исследовании рисков, связанных с лизинговой деятельностью [Текст] / И.В. Сидоренкова // Экономика и предпринимательство. - 2012. - №6 (29). - С. 413-416.

10. Сидоренкова, И.В. Оптимизация позиций участников форфейтной операции [Текст] / И.В. Сидоренкова // Вопросы региональной экономики. - 2015. - Т.22. - №1. - С. 82-86.
11. Сидоренкова, И.В. Совершенствование механизма отбора инновационных проектов в ракетостроении [Текст] / И.В. Сидоренкова // Инновационные аспекты социально-экономического развития региона, Сборник статей по материалам участников V ежегодной научной конференции (аспирантов ФТА). - 2014. - С. 500-508.
12. Сидоренкова, И.В. Совершенствование механизма отбора инновационных проектов в ракетостроении [Текст] / И.В. Сидоренкова // Инновационные технологии в современном образовании, Сборник трудов по материалам II Международной научно-практической интернет-конференции. - 2015. - С. 321-327.
13. Сидоренкова, И.В. Форфейтные операции: экономико-математический анализ [Текст] / И.В. Сидоренкова // Вопросы региональной экономики. - 2014. - Т.20. - №3. - С. 75-79.
14. Сидоренкова, И.В. Экономико-математический анализ и особенности международного лизинга [Текст] / И.В. Сидоренкова // Перспективы, организационные формы и эффективность развития сотрудничества ВУЗов стран Таможенного союза и СНГ, Сборник научных трудов Международной научно-практической конференции. - 2013. - С. 394-399.
15. Яцкевич, А.Б. Экспертные методы в инвестиционных конкурсных процедурах [Текст] / А.Б. Яцкевич, О.Н. Борисова // «Экономические аспекты развития российской индустрии в условиях глобализации 2/2015». - Труды международной научно-практической конференции. - М: Университет машиностроения, 2015 г. - С. 79-81.

ПРИМЕНЕНИЕ ЗАДАЧИ О НАЗНАЧЕНИИ ДЛЯ ПОДДЕРЖКИ ПРИНЯТИЯ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ

Кокорев Сергей Андреевич, студент 3 курса кафедры Информационных технологий и управляющих систем
Научный руководитель**: Бугай Ирина Владимировна**, к.т.н., доцент кафедры Математики и естественнонаучных дисциплин

В работе поставлена и решена задача распределения работ между людьми так, чтобы суммарное время, затраченное ими на работу, было минимальным. Задача решена для некой фирмы,

получившей заказ на разработку 6 программных продуктов. В ходе решения было определенно оптимальное распределение работы между программистами. Для решения задачи за основу был взят венгерский метод, написана программа на С++ для оптимизации процесса.

Венгерский метод, оптимизация процесса, С++.

APPLICATION OF THE PROBLEM OF APPOINTMENT TO SUPPORT MANAGEMENT DECISION-MAKING

Kokorev Sergey, 3rd year student Department of information technology and control systems
Scientific adviser: **Bugay Irina**, Candidate of Technical Sciences, Associate Professor of the Department of mathematics and natural sciences

In work the task of distribution of works between people is set and solved so that the total time spent by them for work was minimum. The task is solved for the certain firm which has received the order for development of 6 software products. During the decision there was definitely optimum distribution of work between programmers. For the solution of a task the Hungarian method has been taken as a basis, the program on C++ for process optimization is also written.

The Hungarian method, process optimization, C ++.

Введение

В процессе выполнения проектных работ часто возникает задача определения наилучших (оптимальных в некотором смысле) структуры или значений параметров объектов и/или комплексов работ [3, 4, 6, 9].

В настоящее время данная задача является крайне актуальной, так как каждое предприятие стремится обеспечить максимальную производительность и минимальные издержки [1, 2, 5, 7, 8].

Постановка и решение задачи

Фирма получила заказ на разработку 6 программных продуктов. Для выполнения этих заказов решено привлечь шесть наиболее опытных программистов. Каждый из них должен разработать одну программу.

Каждый программист имеет различные способности, навыки и затрачивает различное время на выполнение заказа.

Каждый программист дал собственную оценку времени (в днях), которое ему потребуется для разработки программ. Оценки приведены в таблице 1.

Таблица 1 – Производительность программистов

№ программы	1	2	3	4	5	6
Павлов	3	4	11	2	1	2
Иванов	14	12	4	5	1	1
Петров	15	16	5	7	7	1
Сидоров	2	8	2	8	6	3
Кузькин	4	5	8	9	3	2
Постников	7	5	2	1	3	2

Требуется: Распределить работу между программистами так, чтобы суммарное время, затраченное ими на разработку всех программ, было минимальным.

Для решения задачи Венгерским методом была разработана программа на языке С++. В результате использования программы был получен следующий результат (оптимальное решения задачи).

Для написания всех программ требуется 13 дней (рис. 1)

Назначения проведены:

Первую программу пишет: Кузькин

Вторую- Павлов

Третью- Сидоров

Четвертую- Постников

Пятую- Иванов

Шестую- Петров

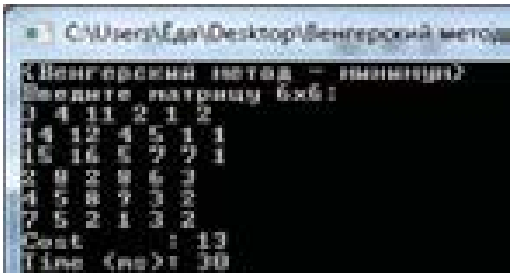


Рисунок 1 – Экран решения задачи с помощью программы на С++

Далее с помощью надстройки MS Excel "Поиска Решений" была проверена работы программы. Полученное решение полностью совпало с решением задачи с помощью программы на C++:

Программа:
***13 дней**
Назначения проведены:
Первую программу пишет: Кузькин
Вторую- Павлов
Третью- Сидоров
Четвертую- Постников
Пятую- Иванов
Шестую- Петров
Поиск Решений:
***13 дней**
Назначения проведены:
Первую программу пишет: Кузькин
Вторую- Павлов
Третью- Сидоров
Четвертую- Постников
Пятую- Иванов
Шестую- Петров

Поскольку оценки производительности программистов не являются абсолютно точными, то на практике важно знать степень устойчивости решения к вариации элементов матрицы производительностей программистов. Для исследования такого влияния была поставлена и решена задача для интервальных оценок производительностей в следующем виде.

Задача. Пусть оценка времени, необходимого программистам для выполнения каждой из работ, задана интервалами (см. таблицу 2).

Таблица 2 – Интервальные производительности программистов

	1	2	3	4	5	6
Павлов	[2,5;3,5]	[3,5;4,5]	[10,5;11,5]	[1,5;2,5]	[0,5;1,5]	[1,5;2,5]
Иванов	[13,5;14,5]	[11,5;12,5]	[3,5;4,5]	[4,5;5,5]	[0,5;1,5]	[0,5;1,5]
Петров	[14,5;15,5]	[15,5;16,5]	[4,5;5,5]	[6,5;7,5]	[6,5;7,5]	[0,5;1,5]
Сидоров	[1,5;2,5]	[7,5;8,5]	[1,5;2,5]	[7,5;8,5]	[5,5;6,5]	[2,5;3,5]
Кузькин	[3,5;4,5]	[4,5;5,5]	[7,5;8,5]	[8,5;9,5]	[2,5;3,5]	[1,5;2,5]
Постников	[6,5;7,5]	[4,5;5,5]	[1,5;2,5]	[0,5;1,5]	[2,5;3,5]	[1,5;2,5]

Определить: влияет ли на назначение программистов и минимизацию общего времени выполнения работ изменение условий задачи?

На рис. 2 можно наблюдать общее время выполнения заказа, в зависимости от вариаций производительности выполнения работ (табл. 3).

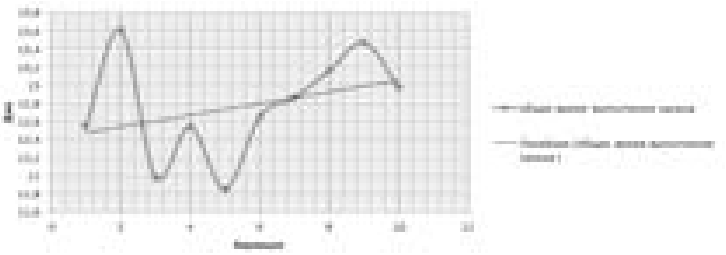


Рисунок 2 - Общее время выполнения заказа при интервальных оценках производительности

Таблица 3 – Варианты решения задачи для интервальных производительностей программистов

	Вариации производительности									
	1	2	3	4	5	6	7	8	9	10
Павлов	2	4	1	4	2	5	4	2	1	4
Иванов	5	5	5	5	5	3	5	5	5	5
Петров	6	6	6	6	6	6	6	6	6	6
Сидоров	3	1	3	1	3	1	1	3	3	1
Кузькин	1	2	2	2	1	2	2	1	2	2
Постников	4	3	4	3	4	4	3	4	4	3

Часто на практике время не является единственным целевым показателем оптимальности решения. Рассмотрим в качестве второго показателя – стоимость выполнения работ.

Задача: Пусть каждому программисту, которому будет поручено выполнить заказ, фирма может предложить оплату в размере 1тыс. руб. в день. При этом издержки составят 13 000 рублей. Решение задачи по стоимостному показателю будет следующим:

Первую программу пишет: Кузькин
Вторую- Павлов
Третью- Сидоров
Четвертую- Постников
Пятую- Иванов
Шестую- Петров

В случае, если не все программисты согласились с предложенными условиями оплаты в связи с различной их квалификацией, ставка была изменена, в результате чего издержки составили 19 000 рублей. При этом решение будет следующим:

Первую программу пишет: Сидоров
Вторую- Кузькин
Третью- Постников
Четвертую- Павлов
Пятую- Иванов
Шестую- Петров

Для двух целевых показателей одновременно задача примет вид:

Задача: Распределить работу между программистами так, чтобы суммарное время, затраченное ими на разработку всех программ, было минимальным, а также суммарная стоимость выполнения всего заказа была бы минимальной.

Таблица 4 – Варианты и значения показателей

	Вариации производительности									
	1	2	3	4	5	6	7	8	9	10
Павлов	2	4	1	4	2	5	4	2	1	4
Иванов	5	5	5	5	5	3	5	5	5	5
Петров	6	6	6	6	6	6	6	6	6	6
Сидоров	3	1	3	1	3	1	1	3	3	1
Кузькин	1	2	2	2	1	2	2	1	2	2
Постников	4	3	4	3	4	4	3	4	4	3
суммарное время выполнения работ, дни	12.55	13.61	11.98	12.54	11.85	12.65	12.86	13.16	13.47	12.98
стоимость выполнения работ, руб.	18320	19465	17360	18050	17175	20325	18705	18705	20555	19590

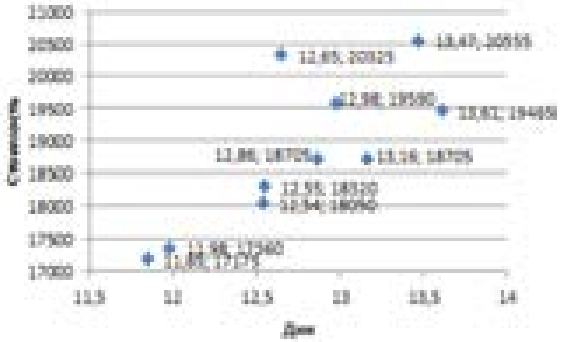


Рисунок 3 – Варианты решения задачи по двум критериям

Выводы

1. Построенная на языке С++ программа решения задачи о назначениях Венгерским методом показала свою работоспособность т.к. позволяет получать оптимальные решения, аналогичные другим программам, в частности, MS Excel.

2. Выбор оптимального решения на основе одновременного использования двух критериев оптимизации позволил для рассматриваемых наборов данных, используя принцип доминирования Парето, получить единственное решение задачи о назначениях, которое позволяет обеспечить минимальные сроки выполнения заказов (11.85 дней) при минимальных издержках (17175 руб.).

Литература

1. Баранчикова, О. И. Моделирование параметров движения остатков средств на едином счете Федерального казначейства [Текст] / О.И. Баранчикова, Д.С. Демина, Ю.С. Пастухова // Инновационные технологии в науке и образовании: Материалы III Междунар. науч.-практ. конф. (Чебоксары, 23 окт. 2015 г.). – Чебоксары: Интерактив плюс. - 2015. – № 3. – С. 179–181.

2. Вилисов, В.Я. Адаптивный выбор управленческих решений. Модели исследования операций как средство хранения знаний ЛПР [Текст] / В.Я. Вилисов. - Саарбрюкен (Германия): LAP LAMBERT Academic Publishing. - 2011. - 376 с.

3. Никонова, Ю.Ю. О плотности распределения страховых выплат [Текст] / Ю.Ю. Никонова, Ю.И. Пастухова // Обозрение прикладной и промышленной математики. - 2008. - Т.15. - №1. - С. 162-163

4. Пастухова, Ю.И. Модель волатильности валютного рынка [Текст] / Ю.И. Пастухова, Г.И. Муджири, А.Б. Яцкевич // Сборник статей Международной научно-практической конференции. Уфа, 2015. С. 36-38.

5. Пастухова, Ю.И. Об одной задаче принятия решений в рекламном бизнесе [Текст] / Ю.И. Пастухова, А.А. Дмитриева // Обозрение прикладной и промышленной математики. - 2007. - Т.14. - № 6. - С. 1130-1131.

6. Самаров, К.Л. Финансовая математика: учебное пособие [Текст] / К.Л. Самаров. - Москва: Альфа-М. - 2005. - 77 с.

7. Сидоренкова, И.В. Конфликты критериев при отборе инвестиционных проектов: экономико-математический анализ

[Текст] / И.В. Сидоренкова // Вопросы региональной экономики. - 2014. - Т.19. - №2. - С. 78-83.
8. Сидоренкова, И.В. Оптимизация позиций участников форфейтной операции [Текст] / И.В. Сидоренкова // Вопросы региональной экономики. - 2015. - Т.22. - №1. - С. 82-86.
9. Яцкевич, А.Б. Экспертные методы в инвестиционных конкурсных процедурах [Текст] / А.Б. Яцкевич, О.Н. Борисова // «Экономические аспекты развития российской индустрии в условиях глобализации 2/2015». - Труды международной научно-практической конференции. - М: Университет машиностроения, 2015 г. - С. 79-81.

АНАЛИЗ ВЛИЯНИЯ СЛУЧАЙНЫХ ФАКТОРОВ НА ПОКАЗАТЕЛИ РАБОТЫ ГИРОСКОПИЧЕСКИХ ПРИБОРОВ

Кудрявцева Надежда Алексеевна, Мулькова Ольга Сергеевна,
студентки 3 курса кафедры Экономики
Научный руководитель: **Вилисов Валерий Яковлевич**, д.э.н.,
профессор кафедры Математики и естественнонаучных дисциплин

В работе проведен анализ случайных факторов различных типов, влияющих на показатели качества работы гироскопических приборов. Приведены сравнительные оценки точности гироприборов, построенных на разных физических принципах. Для оценивания воздействия различных видов возмущений и их удобного представления используется специализированная программа AlaVar, реализующая алгоритм вычисления вариации Аллана. Различные виды имитированных случайных возмущений рассмотрены по отдельности и в виде их комбинаций. Проведенный анализ позволит более точно выявлять типы случайных факторов при выходных и входных испытаниях гироприборов в производственных условиях.

Случайные факторы, гироприборы, точность, вариация Аллана, имитационное моделирование.

ANALYSIS OF THE INFLUENCE OF RANDOM FACTORS ON THE INDICATORS OF GYROSCOPIC INSTRUMENTS

Kudryavtseva Nadezhda, Mulkova Olga, 3rd year students of the department of economics
Scientific adviser: **Vilisov Valery**, Doctor of Economic Sciences,
Professor of the Department of mathematics and natural sciences

The analysis of different types of random factors affecting the performance quality of the gyroscopic instruments. The comparative assessment of the accuracy of gyroscopic devices built on different physical principles. To assess the effects of various disturbances and convenient presentation AlaVar used specialized software that implements an algorithm for calculating Allan variance. Various kinds of random disturbances limited considered individually or as a combination thereof. The analysis will more accurately identify the type of random factors in the output and input tests gyroscopic devices in a production environment.

Random factors, gyroscopic devices, accuracy, variation Allan simulation.

Введение

Гироскопические приборы (гироприборы) в настоящее время очень широко используются в самых различных устройствах в широком спектре прикладных областей [1-4, 7, 9, 10, 16].

При выходном контроле гироприборов, помимо определения фактических характеристик, существует важная задача выявления (идентификации) тех или иных типов погрешностей (шумов) т.к. каждый из них имеет свою природу. Зная состав шума, можно выявить его природу и при возможности устранить воздействие негативных факторов, обеспечив максимальную потенциально достижимую точность.

В практике анализа случайных составляющих погрешностей гироприборов широкое распространение получили программные инструментальные средства, использующие в своей основе вариацию Аллана [10], и в частности, программа AlaVar 5.2 [9, 16] и многочисленные ее аналоги. Они позволяют представить статистику испытаний конкретного образца в виде σ-τ диаграммы. При этом для классических вариантов шумов внешний вид диаграммы известен [9, 10, 16], однако, на практике могут возникать самые разнообразные смеси по составу шумов, в том числе и неклассические, а также ранее неизвестные.

Поэтому актуальной является задача исследования отображения различных смесей шумов на (σ-τ)-диаграмме, что можно выполнить на основе имитационного моделирования. Эта задача и решается в данной работе.

Виды гироприборов

В различных прикладных системах, использующих гироприборы, основанные на различных физических принципах,

обладающих различными массогабаритными, точностными и иными характеристиками. Приведем некоторые наиболее важные из признаков классификации гироприборов.

По типу измеряемых показателей:

- указатели направления (гирокомпасы);
- датчики угловой скорости;
- датчики ускорения (акселерометры).

Наиболее важным из всех классификационных признаков является их физический принцип действия, по которому выделяют:

- механические:
  - роторные;
  - микромеханические.
- оптические:
  - лазерные;
  - волоконно-оптические.

Приведем особенности этих вариантов.

Разные конструкции ГП имеют свои потенциально достижимые пределы точности измерений. В табл. 1 приведены [9, 10] интервалы варьирования точности измерения угла поворота (ухода в единицу времени) относительно рабочей оси чувствительности ГП.

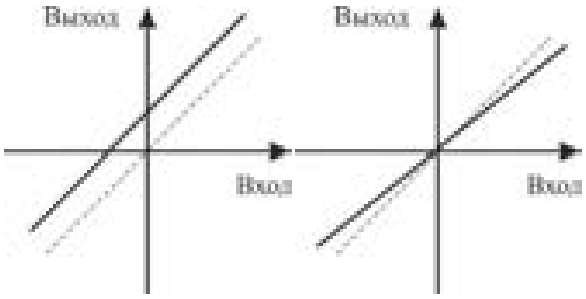
Разновидности погрешностей

Погрешности (шумы) ГП могут иметь весьма разнообразную природу.

Таблица 1 – Пределы точности типов гироприборов

№ п/п	Тип гироприбора	Пределы точности (уход), град/час	
		минимальная (от)	максимальная (до)
1	Электростатические	$5*10^{-6}$	$2*10^{-4}$
2	На магнитных подвесах	$2*10^{-4}$	$2*10^{-3}$
3	Поплавковые интегрирующие	$7*10^{-4}$	$2*10^{-2}$
4	На воздушном подвесе	$3*10^{-3}$	$7*10^{-2}$
5	Волновые твердотельные	$2*10^{-2}$	1
6	Лазерные	$3*10^{-3}$	1
7	Волоконно-оптические	$3*10^{-3}$	1
8	Динамически настраиваемые	$5*10^{-2}$	5
9	Механические	$7*10^{-2}$	5
10	Микромеханические	5	100

Основные проявления погрешностей, возникающих в ГП приведены на рис. 1, где "Вход" – это фактическое значение, например, угла поворота И, а "Выход" – это измеренное значение и.



а *б*

Рисунок 1 - Погрешности гироскопов: а – смещение нуля; б – погрешность коэффициента преобразования

Погрешности (шумы) гироприборов имеют несколько представлений:

1. источники шумов, в числе которых могут быть, например:
   a. особенности конструкции ГП;
   b. производственные факторы (дефекты материалов и комплектующих, качество технологии изготовления);
   c. факторы эксплуатации (внешней среды).
2. проявление воздействия шумов в искажении показаний ГП;
3. математическое описание (представление) шумов.

Каждое из этих представлений используется для разных целей.

В процессе разработки ГП обычно задаются его паспортные характеристики, в числе которых предельная точность (см. табл.1).

Постановка задачи

При анализе шумов ГП, как правило, решают следующие задачи:

1. выявление, по возможности, всех разновидностей шумов, которые возникают в конкретном экземпляре (или в партии) ГП для:
   a. устранения источников и причин шумов, и при возможности - следствий (собственно погрешностей);
   b. компенсация погрешностей, например, введением поправочных коэффициентов и специальных алгоритмов обработки, при невозможности устранения причины, а значит и самих погрешностей в измерениях;

2. установление причинно-следственной связи между разновидностями шумов и их источниками (причинами).

В работе рассмотрена одна из подзадач второй задачи – выявление типов частных (элементарных) шумов, составляющих поток погрешностей измерений по данным испытаний ГП.

Использование вариации Аллана для анализа погрешностей ГП

Вариация Аллана – это статистика второго порядка (некоторый аналог выборочной дисперсии), применяемая для анализа временных последовательностей и содержащихся в них случайных составляющих. Этот инструмент в настоящее время применяется при анализе случайных составляющих в различных системах, в том числе в ГП.

Основная расчетная формула:

$$\text{у}^2(nT_0) = \frac{1}{2(M-2n)(nT_0)^2} \sum_{m=1}^{M-2n} (\text{и}_{m+2n} - 2\text{и}_{m+n} + \text{и}_m)^2, \quad (1)$$

где M – размер выборки; T_0 – интервал времени между наблюдениями; n – номер наблюдения ($n = 1,2, \dots, n_{max} \leq (M-1)/2$); и_i – значение измерения на i-ом шаге.

Графически схема вычисления вариации Аллана по выборке приведена на рис. 2:

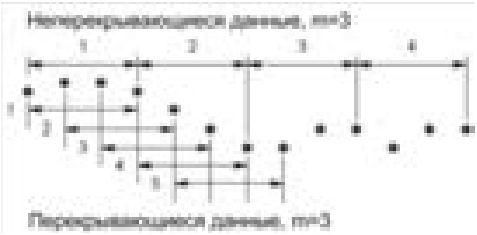


Рисунок 2 – Схема вычисления вариации Аллана

Чаще на практике используется не вариация Алана, а отклонение Аллана (*Allan Deviation* (*AD*)) $\text{у}(nT_0)$ как корень квадратный из вариации Аллана. Затем строится график отклонения Аллана, причем по оси абсцисс откладывается десятичный логарифм среднего времени $\text{ф} = nT_0$, а по оси ординат – десятичный логарифм отклонения Аллана $\text{у}(nT_0)$. Особенность применения вариации Аллана для анализа типов шумов заключается в том, что некоторые

конкретные типы шумов имеют определенный вид на диаграмме в осях (у − ф) (см. рис. 3).

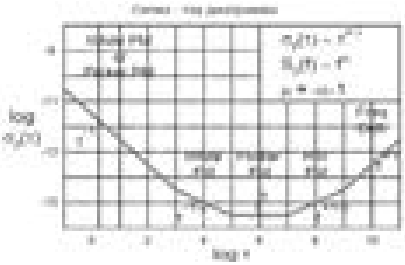


Рисунок 3 – Типичный вид графика отклонения Аллана для комбинированного шума

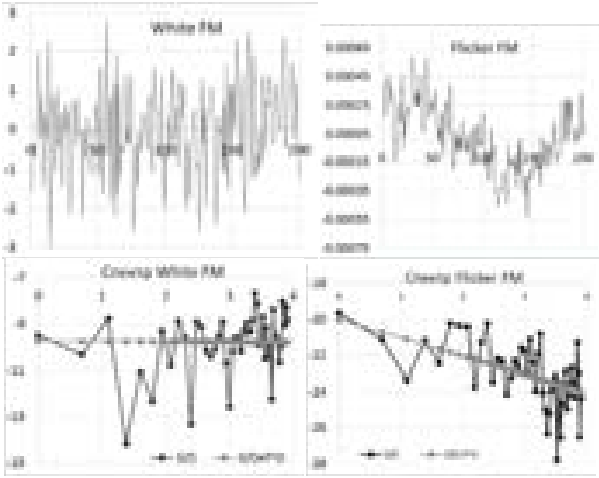
На этом рисунке указаны участки, наклон которых отражает наличие в погрешности конкретного экземпляра ГП того или иного вида шума, в частности: белый шум с фазовой модуляцией (White PM) или фликкер-шуму с фазовой модуляцией (Flicker PM); белый шум с частотной модуляцией (White FM); фликкер-шум с частотной модуляцией (Flicker FM); шум в виде случайных блужданий частотной модуляции (Random Walk FM); уход частоты (Frequency Drift);

Анализ смесей типов погрешности ГП и их отображение на плоскости (у − ф)

На основе имитационного моделирования [5, 6, 8, 11-15] проанализированы различные виды частных шумов с последующим формированием их аддитивных смесей (комбинаций) различного состава и в различных долях мощности (амплитуды).

В качестве инструментальных вычислительных средств были использованы, кроме универсальных - MS Excel, такие специализированные программы как AlaVar 5.2 [9, 16], позволяющая по временному ряду наблюдений строить диаграмму отклонения Аллана в осях (у − ф), а также программа-генератор AlaNoise 3.0 [16], позволяющая формировать временные ряды, соответствующие типичным для ГП частным шумам.

Были сформированы семь частных шумов, имеющих различную спектральную плотность ($S(щ) = щ^{б}$), наиболее часто рассматриваемых в гироскопии [3]:White PM ($б = 2$), Flicker PM ($б = 1$), White FM ($б = 0$), Flicker FM ($б = -1$), Random Walk FM ($б = -2$), Flicker Walk FM ($б = -3$), Ramdom Run FM ($б = -4$). Два из них приведены на рис. 4.



а). б).

Рисунок 4 – Частные шумы в выходном сигнале гироскопов и их отклонения Аллана: а – белый шум; б – случайные блуждания

Формирование аддитивных смесей частных шумов в различных амплитудных долях позволяет подобрать такой комбинированный шум, который максимально соответствует наблюдаемым в конкретном экземпляре (или в серии) ГП. На рис. 5 приведены два из множества полученных в процессе анализа графиков отклонения Аллана.

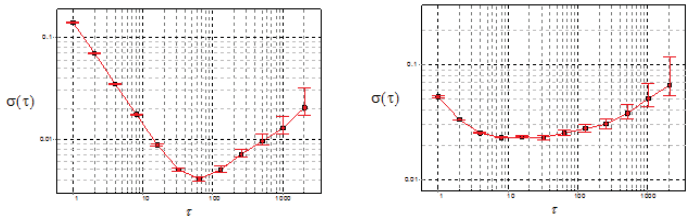


Рисунок 5 – Диаграммы отклонений Аллана для комбинированных шумов

Путем смешивания различных частных шумов можно обеспечить максимальную степень приближения смеси к фактической диаграммы Аллана. Это позволит считать наличие идентифицированных шумов в составе фактически наблюдаемой смеси.

Выводы

1. Гироприборы различных типов находят все более широкое применение в самых различных прикладных областях. Основным их показателем качества является точность показаний, которая определяется как производственными, так и эксплуатационными факторами. Одной из особенностей гироприборов является то, что ошибка в показаниях может накапливаться со временем.

2. На производстве при выходных испытаниях гироприборов важно выявить тип и источник погрешностей для устранения их производственных причин или учета и компенсации погрешностей. Имитация различных типов погрешностей и их смесей позволила сформировать каталог типовых вариантов отображения их вариаций Аллана. Это позволяет более эффективно проводить мониторинг и идентификацию негативных производственных факторов и существенно упрощает задачу распознавания источников погрешностей, что способствует повышению качества выпускаемых гироприборов.

Литература

1. Вилисов, В.Я. Адаптивная транспортная логистическая модель / В.Я. Вилисов, С.Е. Сабо // Информационно-технологический вестник. - 2014. - № 2. - С. 40-45.

2. Вилисов, В.Я. Адаптивный выбор управленческих решений. Модели исследования операций как средство хранения знаний ЛПР [Текст] / В.Я. Вилисов. - Саарбрюккен (Германия) : LAP LAMBERT Academic Publishing. - 2011. - 376 с.

3. Вилисов, В.Я. Адаптивный подход к распределению ограниченных материальных ресурсов в производственных системах [Текст] / В.Я. Вилисов // Менеджмент в России и за рубежом. - 2007. - №5. - С. 10-19.

4. Вилисов, В.Я. Анализ динамики обучения робота в условиях нестационарности критериев модель / В.Я. Вилисов // Информационно-технологический вестник. - 2014. - № 2. - С. 34-39.

5. Вилисов, В.Я. Анализ эффективности обучения робота в условиях целевой нестационарности [Текст] / В.Я. Вилисов // Вибрационные технологии, мехатроника и управляемые машины. Сборник научных статей по материалам XI Международной научно-технической конференции: в 2 частях. - 2014. - Часть 2. - С. 282-287.

6. Вилисов, В.Я. Марковская модель обучения робота целесообразному поведению / В.Я. Вилисов // Информационно-технологический вестник. - 2015. - № 4. - С. 11-18.
7. Вилисов, В.Я. Транспортная модель, аппроксимирующая предпочтения ЛПР [Текст] / В.Я. Вилисов // Прикладная информатика. - 2010. - № 6 (30). - С. 101-110.
8. Вилисов, В.Я. Управление переключениями тарифных планов сотовой связи [Текст] / В.Я. Вилисов // Управление большими системами. - Выпуск 40. - М.: ИПУ РАН. - 2012. - С. 221-237.
9. Кробка, Н.И. Дифференциальные методы идентификации шумов гироскопов // Гироскопия и навигация. - 2011. - № 1(72) . - С. 59-77.
10. Матвеев, В.В. Анализ погрешностей микромеханических гироскопов методом вариации Аллана / В.В. Матвеев, М.Г. Погорелов // Известия ТулГУ. - Технические науки. - 2015. - Вып. 3. – С. 123-135.
11. Пастухова, Ю.И. Модель волатильности валютного рынка [Текст] / Ю.И. Пастухова, Г.И. Муджири, А.Б. Яцкевич // Сборник статей Международной научно-практической конференции. Уфа, 2015. С. 36-38.
12. Самаров, К.Л. Финансовая математика: учебное пособие [Текст] / К.Л. Самаров. - Москва: Альфа-М. - 2005. - 77 с.
13. Сидоренкова, И.В. Конфликты критериев при отборе инвестиционных проектов: экономико-математический анализ [Текст] / И.В. Сидоренкова // Вопросы региональной экономики. - 2014. - Т.19. - №2. - С. 78-83.
14. Сидоренкова, И.В. Оптимизация позиций участников форфейтной операции [Текст] / И.В. Сидоренкова // Вопросы региональной экономики. - 2015. - Т.22. - №1. - С. 82-86.
15. Яцкевич, А.Б. Экспертные методы в инвестиционных конкурсных процедурах [Текст] / А.Б. Яцкевич, О.Н. Борисова // «Экономические аспекты развития российской индустрии в условиях глобализации 2/2015». - Труды международной научно-практической конференции. - М: Университет машиностроения, 2015 г. - С. 79-81.
16. Сайт разработчика программ AlaVar 5.2 и AlaNoise 3.0 [Электронный ресурс]. – URL - http://www.alamath.com.

ВЫБОР ЭКОНОМИЧЕСКИ ОПТИМАЛЬНЫХ ОБЪЕМОВ ИСПЫТАНИЙ ПРИ ВЫХОДНОМ КОНТРОЛЕ ГИРОСКОПИЧЕСКИХ ПРИБОРОВ

Кудрявцева Надежда Алексеевна, Мулькова Ольга Сергеевна,
студентки 3 курса кафедры Экономики
Научный руководитель: **Вилисов Валерий Яковлевич**, д.э.н.,
профессор кафедры Математики и естественнонаучных дисциплин

В работе проведен обзор использования гироскопических приборов в различных сферах приложения. Рассмотрены основные составляющие затрат на производство и испытания гироприборов их структура и взаимосвязь в цепочках взаимодействия от производителя до конечного пользователя. Разработана методика определения экономически оптимального объема выходных испытаний гироприборов при их производстве. Приведены численные расчеты некоторых вариантов.

Гироприборы, точность, выходные испытания, издержки.

SELECTING THE ECONOMICALLY OPTIMAL VOLUME OF TESTS AT INCOMING INSPECTION GYROSCOPIC INSTRUMENTS

Kudryavtseva Nadezhda, Mulkova Olga, 3rd year students of the Department of economics
Scientific adviser: **Vilisov Valery**, Doctor of Economic Sciences,
Professor of the Department of mathematics and natural sciences

In this paper a review of the use of gyroscopic instruments in various fields of application. The main components of the cost of production and testing of gyroscopic devices, their structure and relationship of cooperation in chains from the producer to the end user. A method for determining the economically optimal amount of output test gyroscopic devices in their production. Numerical calculations of some embodiments.

Gyroscopic devices, precision, output test, costs.

Введение

В настоящее время существует широкий спектр бесплатформенных гироприборов (ГП), основанных на различных

физических принципах [9, 10]. Важнейшим показателем ГП является точность показаний в различных условиях.

В процессе создания гироприборов на их показатели могут оказывать воздействие различные производственные факторы, приводящие к погрешностям показаний [1,7, 12-14]. Выходной контроль на производстве призван подтвердить соответствие показателей конкретного экземпляра прибора его паспортным значениям [4, 2, 11]. Как правило, все проверки требуют значительных временных затрат, причем, большей точности соответствуют более продолжительные проверки.

С другой стороны, при выходном тестировании ГП возникает вопрос разумной достаточности [3, 5, 6, 8, 15] объема проверок, обусловленного величиной ожидаемого ущерба при отказе ГП при его эксплуатации. Поэтому актуальной является задача выбора объема испытаний, оптимизирующего суммарные издержки, обусловленные затратами на них и ожидаемой неустойкой в случае отказа ГП при его эксплуатации. Эта задача и решается в данной работе.

Типовая схема производства и использования гироприборов

ГП имеют две группы показателей [9, 10], отражающих их основные потребительские свойства: точность и надежность.

Для подтверждения паспортных значений точности и надежности необходимы испытания на дорогостоящем специальном стендовом оборудовании. При этом степень достоверности измеренных показателей пропорциональна продолжительности испытаний.

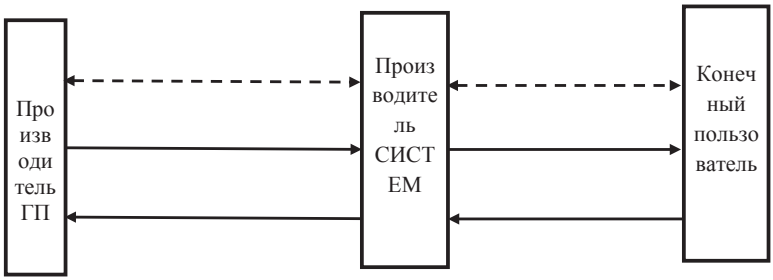


Рисунок 1 - Взаимодействие сторон

Если затраты на испытания приводят к увеличению издержек, то более точные значения показателей позволяют снизить вероятные издержки от отказа ГП при эксплуатации (т.к. ненадежные ГП не будут направлены в эксплуатацию или доработаны).

Для оценки издержек, связанных с производством и поставкой ГП заказчикам, принята схема (см. рис.1) их использования после изготовления и поставки, включающую производителя, потребителя и конечного пользователя.

Структура издержек

Себестоимость производства ГП складывается из всех стандартных издержек любого производства [11, 12]: постоянные издержки; переменные издержки (стоимость материалов, комплектующих, зарплаты и т.п.). При этом в составе переменных издержек помимо производственной их части есть характерная для ГП доля, обусловленная их выходными испытаниями (издержки испытаний ГП - S_v).

Издержки потребителя, использующего ГП в составе своей системы, в случае отказа, зависят от того насколько ГП функционально значим для системы. Если отказ ГП не приводит к полному отказу системы, а лишь несколько уменьшает ее функциональность, то коэффициент значимости ГП небольшой. Отказом ГП можно считать пребывание величины погрешности вне заданного диапазона.

С помощью этого коэффициента можно описывать одну из составляющих ущерба, который несет конечный пользователь в случае отказа ГП, а значит и изготовитель системы (в пределах гарантийного срока, закрепленного в контракте), который, в свою очередь может требовать неустойку от изготовителя. Например, если ГП, установленный на борту беспилотного летательного аппарата (БПЛА), является единственным источником его навигационных параметров, то отказ ГП может привести к полной утере БПЛА, а возможно и к дополнительным потерям, связанным с невыполнением поставленных ему задач.

В работе принято, что коэффициент значимости (k_z) может принимать значения от 0 до 1. При этом, если отказ элемента (ГП) никак не влияет на выполнение системой функций, то этому случаю соответствует его значение $k_z = 0$. Если отказ элемента приводит к полной потере работоспособности системы, то в этом случае $k_z = 1$.

Полную величину ущерба, связанного с отказом системы обозначим S_u, тогда доля ущерба, обусловленную отказом ГП определим как:

$$S_z = k_z S_u \qquad (1)$$

Для некоторых групп прикладных систем в табл. 1 приведены примерные диапазоны возможных значений k_z.

Таблица 1 - Диапазоны варьирования коэффициента значимости для некоторых видов прикладных систем

Прикладная система	Ср. цена, $	Коэффициент значимости ГП в системе										
		0	**0.1**	**0.2**	**0.3**	**0.4**	**0.5**	**0.6**	**0.7**	**0.8**	**0.9**	**1**
Телефоны, игрушки, бытовые приборы, …	1											
Оборудование, приборы, …	100											
Самолеты, ракеты, БПЛА, суда, …	10000											

Исходя из этого, например, для приложений ГП в бытовых приборах, производитель ГП может получить претензию (если это оговорено в контракте) в объеме $S_z = 0.1Ч10000\$ = 1000\$$. Однако, если вероятность отказа ГП (P_0) отлична от единицы, то в среднем для каждого экземпляра ГП (из однородной партии) ущерб составит:

$$S(P_o) = P_0 S_z \qquad (2)$$

Так, в продолжение предыдущего примера, если вероятность отказа ГП, например, $P_0 = 0.05$, то средний ожидаемый ущерб составит $S(P_o) = 0.05Ч1000\$ = 50\$$. Однако, оценка вероятности отказа конкретного ГП до его испытаний известна не точно, а лишь в виде интервальной оценки с заданной доверительной вероятностью: $P_0 \in [P_{min}; P_{max}]$. Типовой процесс уточнения величины P_0 в процессе испытаний ГП приведен на рис. 2.

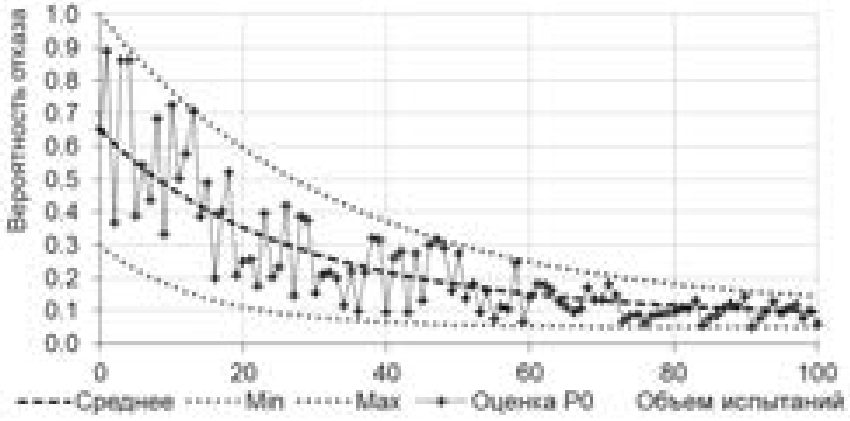


Рисунок 2 - Уточнение оценки P_0 в процессе испытаний ГП

По мере проведения испытаний доверительный интервал ("трубка") оценки сужается. Трубка оценки вероятности может быть представлена и в шкале (по оси ординат) величины ущерба. Так для приведенного выше примера значению $P_0 = 1$ будет соответствовать величина ущерба $S_z = 100\$$. А это значит, что по мере проведения испытаний величина ожидаемого ущерба в среднем (по множеству однородных ГП) монотонно снижается.

Выбор оптимальных объема испытаний ГП

По мере увеличения продолжительности испытаний ГП накопленная стоимость издержек, связанных с проведением испытаний, растет (как правило, линейно). Две тенденции, отражающие два вида затрат (ожидаемый ущерб и затраты на испытания) можно объединить в общей целевой функции $S(t)$, представленной на рис. 3. Тогда, если известны все упомянутые параметры составляющих суммарных затрат, то может быть определено оптимальное значение продолжительности испытаний ГП. На рис. 3 оптимальная продолжительность испытаний $t_{opt} = 53$ час, этому значению будет соответствовать объем суммарных затрат $S(t_{opt}) = 32.88\ \$$.

Если для испытуемой партии ГП параметры среднего ожидаемого ущерба не известны, то по мере проведения испытаний можно строить последовательно уточняемую оценку среднего ущерба, имея в виду, что суммарная целевая функция может быть аппроксимирована следующим выражение:

$$S(t) = a + (d - a)e^{-ct} + kt \qquad (3)$$

Здесь a – нижнее асимптотическое значение, к которому сходится оценка среднего ущерба; d – начальное значение среднего ущерба (при $t = 0$), которое может быть определено из априорных данных, например из прошлых испытаний ГП данной партии или на основании данных конструкторской документации; c – коэффициент сходимости среднего ущерба к установившемуся значению; k – стоимость одного час испытаний ГП.

Оптимальное значение продолжительности испытаний можно найти, продифференцировав выражение $S(t)$ и приравняв производную к нулю, после чего:

$$t_{opt} = -\frac{1}{c}\ln\frac{k}{c(d-a)} \qquad (4)$$

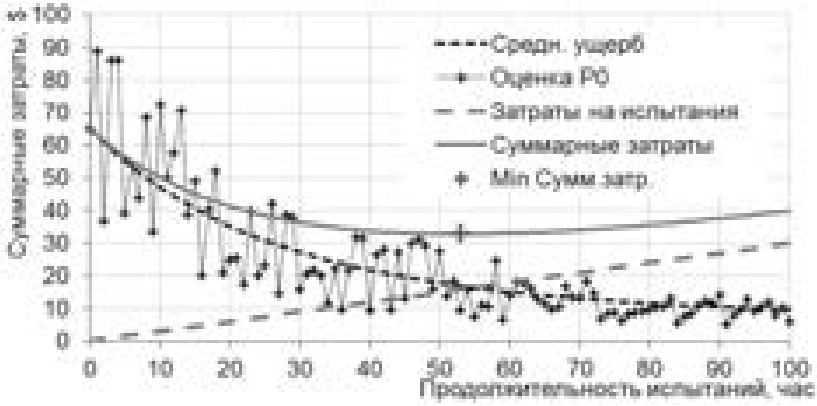


Рисунок 3 - Суммарные затраты $S(t)$ испытаний ГП

Выводы

1. Основным показателем качества работы гироприборов является точность показаний, которая определяется различными производственными и эксплуатационными факторами. Для выявления фактических значений используются выходные испытания, продолжительность которых с одной стороны пропорциональна степени достоверности оценки погрешности, а с другой увеличивает себестоимость прибора.

2. Предложена методика определения оптимальной продолжительности выходных испытаний гироприборов в зависимости от степени их функциональной значимости в составе системы. Выполнены модельные расчеты для некоторых типовых вариантов применения гироприборов.

Литература

1. Вилисов, В.Я. Адаптивная транспортная логистическая модель / В.Я. Вилисов, С.Е. Сабо // Информационно-технологический вестник. - 2014. - № 2. - С. 40-45.

2. Вилисов, В.Я. Адаптивный выбор управленческих решений. Модели исследования операций как средство хранения знаний ЛПР [Текст] / В.Я. Вилисов. - Саарбрюккен (Германия) : LAP LAMBERT Academic Publishing. - 2011. - 376 с.

3. Вилисов, В.Я. Адаптивный подход к распределению ограниченных материальных ресурсов в производственных системах [Текст] / В.Я. Вилисов // Менеджмент в России и за рубежом. - 2007. - №5. - С. 10-19.

4. Вилисов, В.Я. Анализ динамики обучения робота в условиях нестационарности критериев модель / В.Я. Вилисов // Информационно-технологический вестник. - 2014. - № 2. - С. 34-39.
5. Вилисов, В.Я. Анализ эффективности обучения робота в условиях целевой нестационарности [Текст] / В.Я. Вилисов // Вибрационные технологии, мехатроника и управляемые машины. Сборник научных статей по материалам XI Международной научно-технической конференции: в 2 частях. - 2014. - Часть 2. - С. 282-287.
6. Вилисов, В.Я. Марковская модель обучения робота целесообразному поведению / В.Я. Вилисов // Информационно-технологический вестник. - 2015. - № 4. - С. 11-18.
7. Вилисов, В.Я. Транспортная модель, аппроксимирующая предпочтения ЛПР [Текст] / В.Я. Вилисов // Прикладная информатика. - 2010. - № 6 (30). - С. 101-110.
8. Вилисов, В.Я. Управление переключениями тарифных планов сотовой связи [Текст] / В.Я. Вилисов // Управление большими системами. - Выпуск 40. - М.: ИПУ РАН. - 2012. - С. 221-237.
9. Кробка Н.И. Дифференциальные методы идентификации шумов гироскопов // Гироскопия и навигация. - 2011. - № 1(72) . - С. 59-77.
10. Кутовой Д.А. Оценка основных характеристик бесплатформенного инерциального блока с использованием вариации Аллана / Д. А. Кутовой, П. В. Ситников, А. А. Федотов, В. Л. Якимов. - Вестник Самарского ГАУ № 1(43) 2014 г. – С.201-209.
11. Пастухова, Ю.И. Модель волатильности валютного рынка [Текст] / Ю.И. Пастухова, Г.И. Муджири, А.Б. Яцкевич // Сборник статей Международной научно-практической конференции. Уфа, 2015. С. 36-38.
12. Самаров, К.Л. Финансовая математика: учебное пособие [Текст] / К.Л. Самаров. - Москва: Альфа-М. - 2005. - 77 с.
13. Сидоренкова, И.В. Конфликты критериев при отборе инвестиционных проектов: экономико-математический анализ [Текст] / И.В. Сидоренкова // Вопросы региональной экономики. - 2014. - Т.19. - №2. - С. 78-83.
14. Сидоренкова, И.В. Оптимизация позиций участников форфейтной операции [Текст] / И.В. Сидоренкова // Вопросы региональной экономики. - 2015. - Т.22. - №1. - С. 82-86.
15. Яцкевич, А.Б. Экспертные методы в инвестиционных конкурсных процедурах [Текст] / А.Б. Яцкевич, О.Н. Борисова // «Экономические аспекты развития российской индустрии в условиях

глобализации 2/2015». - Труды международной научно-практической конференции. - М: Университет машиностроения, 2015 г. - С. 79-81.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ ПОКАЗАТЕЛЕЙ РАЗВИТИЯ МУНИЦИПАЛЬНЫХ ОБРАЗОВАНИЙ СЕВЕРО-ВОСТОКА МОСКОВСКОЙ ОБЛАСТИ И РЕГИОНОВ РФ

Хальченко Ольга Андреевна, студентка 3 курса кафедры Бухгалтерского и финансового учета
Научный руководитель: **Пастухова Юлия Ивановна**, к.ф.-м.н., доцент кафедры Математики и естественнонаучных дисциплин

В работе поставлена задача и предложена методика анализа официальных показателей, которые позволяют судить о реальной социально-экономической ситуации в Московской области Российской федерации, а также отдельных регионов страны. Задача решена для данных о статистических показателях социально-экономическом состоянии отдельных городов и регионов, опубликованных в официальных источниках. Решение проблемы направленно на разработку доступных способов анализа официальных показателей, которые позволяют по возможности судить о реальной социально-экономической ситуации в регионе.

Статистический анализ, социально-экономические показатели, регионы.

COMPARATIVE ANALYSIS OF SOCIO-ECONOMIC INDICATORS OF MUNICIPALITIES NORTH-EAST OF MOSCOW REGION AND RUSSIAN REGIONS

Halchenko Olga, 3rd year student of the Department of accounting and financial accounting
Scientific adviser: **Pastukhova Yulia,** Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of mathematics and natural sciences

In the task, and a method of analysis of official figures which provide a glimpse of the real socio-economic situation in the Moscow region of the Russian Federation, as well as certain regions of the country. The problem is solved for the data on the statistical indicators of socio-economic status of the individual cities and regions, published in the official sources. The

solution is directed to the development of the available methods of analysis of official figures that allow for the possibility to judge about the real socio-economic situation in the region.

Statistical analysis of socio-economic indicators, the regions.

Введение. Федеральная служба государственной статистики и другие источники [13, 15, 16] опубликовали данные официальной статистики различных показателей за 2014 г. по субъектам РФ и за 2015 г. по городам северо-востока Московской области. Числовые показатели социально-экономического состояния значительно варьируются в предоставляемых статистических данных из различных официальных источников. Поэтому анализ официальных данных, тем более в условиях действующего кризиса, является первоочередной задачей.

Постановка и решение задачи. Для анализа было выбрано 10 городов или городских поселений, среди которых: Королёв, Ивантеевка, Сергеев-посад, Мытищи, Хотьково, Монино, Фрязино, Щелково, Софрино, Черноголовка. Анализировались статистические данные за семь месяцев 2015 года [13].

Средняя зарплата по городу Королёву существенно ниже показателей других городов. Это обуславливается тем, что Королёв является наукоградом, в котором большую часть работающего населения составляют преимущественно научно-технические кадры, зарплата которых не является высокой.

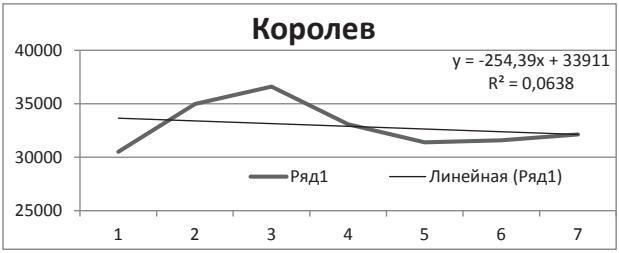


Рисунок 1 - Изменение среднего уровня заработной платы с июня по декабрь 2015 г. по городу Королёв

Для каждого города была построена диаграмма изменения среднего уровня зарплаты по месяцам [1, 2, 14]. Для каждого из рядов динамики определен линейный тренд [7, 8]. Коэффициент наклона k прямой линии тренда указывает [7, 8, 11] на среднюю скорость изменения средней заработной платы. Следует отметить, что для

большинства городов отмечаются значительные колебания этого показателя за последние семь месяцев прошедшего года, на что указывают низкие коэффициенты детерминации, за исключением города Мытищи, где наблюдается устойчивый рост.

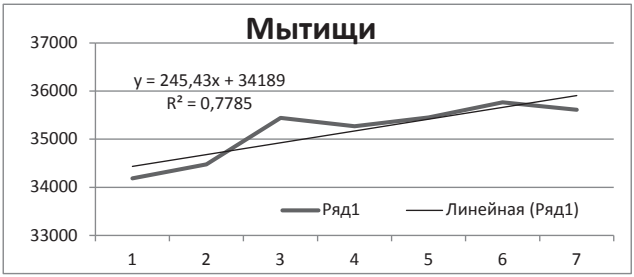


Рисунок 2 - Изменение среднего уровня заработной платы с июня по декабрь 2015 г. по городу Мытищи

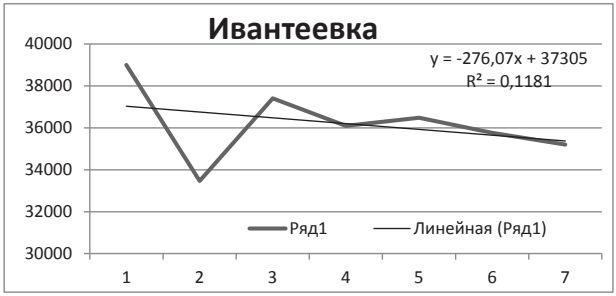


Рисунок 3 - Изменение среднего уровня заработной платы с июня по декабрь 2015 г. по городу Ивантеевка

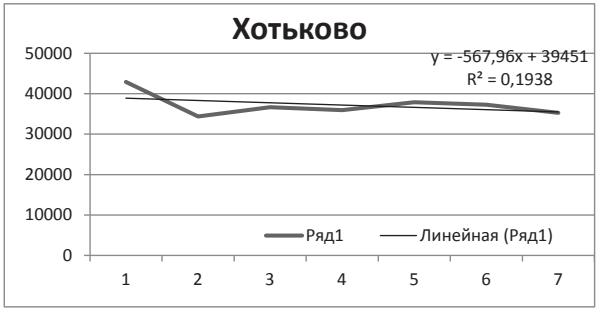


Рисунок 4 - Изменение среднего уровня заработной платы с июня по декабрь 2015 г. по городу Хотьково

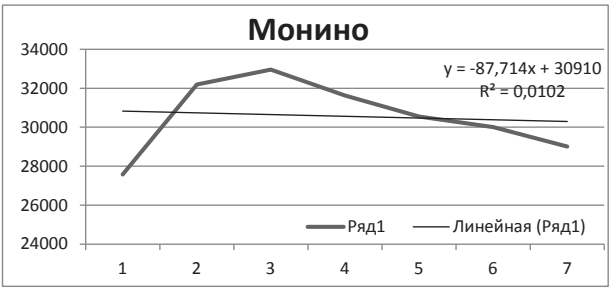


Рисунок 5 - Изменение среднего уровня заработной платы с июня по декабрь 2015 г. по городу Монино

Рисунок 6 - Изменение среднего уровня заработной платы с июня по декабрь 2015 г. по городу Щелково

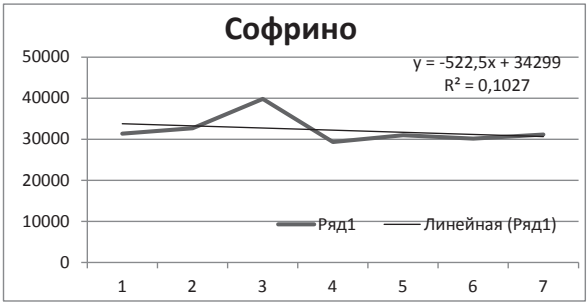


Рисунок 7 - Изменение среднего уровня заработной платы с июня по декабрь 2015 г. по городу Софрино

Рисунок 8 - Изменение среднего уровня заработной платы с июня по декабрь 2015 г. по городу Черноголовка

Как известно, положительное значение углового коэффициента указывают на преимущественное возрастание средних зарплат, а отрицательное – на преимущественное убывание. Можно сделать вывод, что рост зарплаты проходит четко прослеживается в городах Мытищах и Фрязино. Более высокий коэффициент по Фрязино обусловлен резким падением в предшествующие месяцы и последующим ростом.

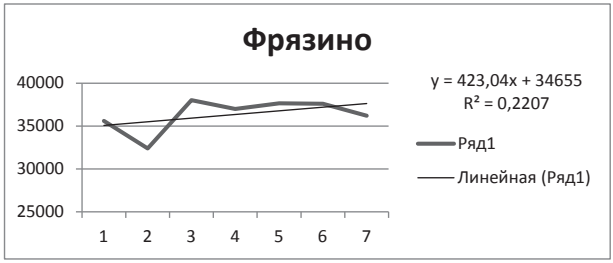


Рисунок 9 - Изменение среднего уровня заработной платы с июня по декабрь 2015 г. по городу Фрязино

На втором этапе исследования была составлена корреляционная матрица. На ее основе проводился анализ парных зависимостей.

Анализ корреляционной таблицы [5, 6] позволяет сделать вывод о том, что динамика изменения средней заработной платы в г. Королёве очень схожа с динамикой, наблюдаемой в городах Сергеев-Посад, Монино и Софрино; в основном противоположна динамике населенных пунктов Хотьково, Черноголовки, Ивантеевки и не обнаруживает связи с динамикой городов Мытищи, Фрязино и Щелково. Сопоставление указанных фактов, а также сравнение промышленной структуры, позволит специалистам сделать более точные выводы и прогнозы [12].

Таблица 1 – Сравнительный анализ углового коэффициента, коэффициента детерминации, наименьшей, наибольшей и средней заработной платы по городам северо-востока Московской области

Населенный пункт	**k**	R^2	Наименьшее значение з/п за период	Наибольшее значение з/п за период	Средняя з/п за период
Ивантеевка	276,07	0,118	33464 (июль)	39000 (июнь)	36201
Королёв (н.град)	254,39	0,0638	30500 (июнь)	36000 (август)	32839
Сергеев-Посад	96,179	0,02	29396 (июнь)	34057 (август)	31269
Мытищи	245,43	0,7785	34184 (июнь)	35766 (ноябрь)	35171
Хотьково	567,96	0,1938	34386 (июль)	42903 (июнь)	31179
Монино	87,714	0,0102	27571 (июнь)	32960 (август)	30559
Фрязино (н.град)	423,04	0,2207	32387 (июль)	38017 (август)	36347
Щелково	234,18	0,1142	32519 (июль)	36404 (июнь)	34792
Софрино	-522,5	0,1027	29311 (сентябрь)	39835 (август)	32209
Черноголовка (н.град)	-406	0,1925	35447 (июль)	41798 (июнь)	37644

Следует отметить, что наиболее близкие показатели связи процессов изменения заработной платы наблюдаются в достаточно отдаленных друг от друга городах: Монино-Королёв (0,8794), Хотьково-Ивантеевка (0,8692), Черноголовка-Ивантеевка (0,8983), Хотьково-Черноголовка (0,9415), исключение составляют лишь Ивантеевка-Щелково (0,9037). Соответствующие коэффициенты корреляции значимы.

Приведенные выше динамики в основном противоположны основном противоположна динамике населенных пунктов Хотьково, Черноголовки, Ивантеевки.

Несмотря на обнаруженные существенные различия в динамике изменения средней заработной платы, множественные коэффициенты корреляции, т.е. показатели связи одного муниципалитета с остальными по средней зарплате очень велики. Этим, скорее всего, можно объяснить тот факт, что попытка применить корреляционный анализ к 10 субъектам (Московской, Тверской, Калужской, Ленинградской, Костромской, Волгоградской, Омской, Томской, Кемеровской, Иркутской) [16] не позволяет сделать каких-либо четкие выводов, кроме того, что прослеживается практически одинаковая тенденция. Самая тесная корреляция [9, 10] наблюдается

между областями: Московской и Тверской (0,98772), Волгоградская и Московская (0,990413), Костромской и Калужской (0,987786).

Таблица 2 – Проверка значимости значений корреляции корреляционной матрицы

Города	Наблюдаемое значение сстатистики t	$t_{табл}$=2,7764 Вывод
Монино-Королёв	3,6944	значим
Хотьково-Ивантеевка	3,516	значим
Черноголовка-Ивантеевка	4,0899	значим
Хотьково-Черноголовка	5,5899	значим
Ивантеевка-Щелково	4,2269	значим

Похожая ситуации наблюдается и при анализе доходов населения. Для анализа были выбраны те же 10 областей. [16] Как и в случае с заработной платой, все указанные регионы обнаруживают почти одинаковую тенденцию в изменении среднедушевых доходов населения. Однако сильнее всего это наблюдается в Ленинградской и Московской (0,9795), Калужской и Тверской (0,97202), Иркутской и Тверской (0,9780002) областях.

Анализ динамики прожиточного минимума по регионам РФ (те же 10 областей) также не дает четкой картины. Выбранные субъекты показывают практически одинаковую связь между собой (данные сделаны на основе составленной корреляционной таблицы). Однако наиболее сильная связь прослеживается между областями: Московской и Калужской (0,9908), Московской и Костромской (0,9975), Костромской и Калужской (0,9895), Кемеровской и Омской (0,9857).

Большая группа экспертов указывает на наличие факта снижения уровня заработной платы в системе здравоохранения и сфере образования.

Мнения экспертов, участвовавших в опросе Центра «Народная экспертиза», находят свое подтверждение и в данных, опубликованных Росстатом за девять месяцев 2015 г. (доступно на данный момент). Детальный анализ официальной статистики показывает, что действительно в ряде регионов имеет место снижение заработной платы врачей, среднего и младшего медперсонала, а также педагогических работников. При этом снижение отмечено как в абсолютном выражении, так и относительно средней зарплаты бюджетников в регионе или отрасли.

Выводы

1. Анализ показал, что необходим детальный анализ динамики зарплаты в небольших муниципальных образованиях, расположенных на незначительном расстоянии. Важную информацию при этом может дать сравнение динамики в различных населенных пунктах.

2. Результаты дальнейших исследований могут свидетельствовать о самодостаточности или зависимости рынка труда соседних городов, выявлять направления движения потоков трудовых ресурсов.

3. При дальнейших исследованиях важно учитывать структуру населения, имеющийся рынок труда, междугородные транспортные сети.

Литература

1. Вилисов, В.Я. Адаптивный подход к распределению ограниченных материальных ресурсов в производственных системах / В.Я. Вилисов // Менеджмент в России и за рубежом. - 2007. - №5. - С. 10-19.

2. Вилисов, В.Я. Инструменты внутреннего контроля / В.Я. Вилисов, И.Е. Суков. - М.: РИОР, ИНФРА-М. - 2016. - 262 с. - DOI: 10.12737/11472

3. Вилисов, В.Я. Инфраструктура инноваций и малые предприятия: состояние, оценки, моделирование / В.Я. Вилисов, А.В. Вилисова. - М.: ИЦ РИОР, НИЦ ИНФРА-М. - 2015. -228 с. - DOI: 10.12737/4320

4. Вилисов, В.Я. Особенности многокритериального выбора инвестиционных проектов [Текст] / В.Я. Вилисов, И.В. Сидоренкова // Перспективы, организационные формы и эффективность развития сотрудничества ВУЗов стран Таможенного союза и СНГ, Сборник научных трудов Международной научно-практической конференции. - 2013. - С. 319-327.

5. Вилисов, В.Я. Управленческая среда инновационной системы предприятия // Материалы симпозиума «Стратегическое планирование и развитие предприятий». - М. ЦЭМИ РАН, 2011. - С. 34-36.

6. Вилисов, В.Я. Адаптивный выбор управленческих решений. Модели исследования операций как средство хранения знаний ЛПР [Текст] / В.Я. Вилисов. - Саарбрюкен (Германия): LAP LAMBERT Academic Publishing. - 2011. - 376 с.

7. Пастухова, Ю.И. Модель волатильности валютного рынка [Текст] / Ю.И. Пастухова, Г.И. Муджири, А.Б. Яцкевич // Сборник статей Международной научно-практической конференции. Уфа, 2015. С. 36-38.
8. Переяславский, В.И. Рынок услуг, маркетинг и паевые инвестиционные фонды [Текст] / В.И. Переяславский // Маркетинг услуг. - 2014. - №4. - С. 322-327.
9. Самаров, К.Л. Финансовая математика: учебное пособие [Текст] / К.Л. Самаров. - Москва: Альфа-М. - 2005. - 77 с.
10. Сидоренкова, И.В. Оптимизация позиций участников форфейтной операции [Текст] / И.В. Сидоренкова // Вопросы региональной экономики. - 2015. - Т.22. - №1. - С. 82-86.
11. Сидоренкова, И.В. Конфликты критериев при отборе инвестиционных проектов: экономико-математический анализ [Текст] / И.В. Сидоренкова // Вопросы региональной экономики. - 2014. - Т.19. - №2. - С. 78-83.
12. Яцкевич, А.Б. Экспертные методы в инвестиционных конкурсных процедурах [Текст] / А.Б. Яцкевич, О.Н. Борисова // «Экономические аспекты развития российской индустрии в условиях глобализации 2/2015». - Труды международной научно-практической конференции. - М: Университет машиностроения, 2015 г. - С. 79-81.
13. Система поиска вакансий и резюме [Электронный ресурс]. – URL - http://www.trud.com/
14. Общероссийский народный фронт [Электронный ресурс]. – URL - http://onf.ru/
15. Правовая поддержка организаций [Электронный ресурс]. – URL - http://www.elcode.ru/ -
16. Федеральная служба государственной статистики [Электронный ресурс]. – URL - http://www.gks.ru/

КАФЕДРА УПРАВЛЕНИЯ КАЧЕСТВОМ И СТАНДАРТИЗАЦИИ

ОЦЕНКА ВЛИЯНИЯ ТАРЫ НА КАЧЕСТВО И СПРОС МОЛОЧНОЙ ПРОДУКЦИИ

Бабкин Дмитрий Сергеевич, студент 3 курса кафедры Управления качеством и стандартизации
Научный руководитель: **Исаев Владимир Геннадьевич,** к.т.н., доцент, заведующий кафедрой Управления качеством и стандартизации

В работе рассмотрено влияние упаковки и информации на ней на качество и спрос молочной продукции. Проведены опросы населения для определения мнения потребителя и его предпочтений. На основании этих данных были составлены рекомендации.

Качество, упаковка, молоко.

RESEARCH OF THE TAR'S INFLUENCE ON THE QUALITY ON THE DEMAND OF DAIRY PRODUCTS

Babkin Dmitry, 3rd year student of the Department of quality management and standardization
Scientific adviser: **Isaev Vladimir,** Candidate of Technical Sciences, Associate Professor, Head of the Department of quality management and standardization

The study reviews the impact of the packing and the information on it on the quality and demand of dairy products. Population surveys were done to determine the opinion of the consumer and his preferences. Relying on that data recommendations were compiled.

Quality, packing , milk.

Молочные продукты в настоящее время являются одними из основных продуктов потребляемых населением Российской Федерации. Поэтому целью исследования являлось изучение потребительских приоритетов населения при покупке молока.

Для достижения поставленной цели решались следующие задачи

1) определение критериев важности при выборе молока;

2) определение коэффициента удовлетворенности потребителей;

3) Сравнение основных продуктов представленных на рынке молока;

4) разработка рекомендаций для потребителя при покупке молока.

Был проведен опрос 100 респондентов, по специально разработанной анкете. Анкета составлялась с учетом того, что продукция должна удовлетворять современным требованиям по качеству к продукту [1, 2]. Основными вопросами в анкете являлись

- Насколько важен для Вас вид тары
- Насколько важна для Вас жирность молока
- Насколько важна для вас маркировка на упаковке
- Насколько важен для вас срок годности молока

Для обработки результатов анкетирования использовался метод описательной статистики, который представляет собой обработку эмпирических данных, их систематизацию, наглядное представление в форме графиков и таблиц, а также их количественное описание посредством основных статистических показателей [1, 2]. Так же были использованы коэффициенты удовлетворенности и важности.

Коэффициент удовлетворенности определялся как сумма средних значений удовлетворенности по влияющим на качество и доступность обслуживания факторам, взвешенных с учетом значимости этих факторов для обеспечения качества и доступности.

Расчет коэффициента удовлетворенности проводился по формуле 1

$$K_y = \frac{\sum_{\Phi=1}^{n} (У_\Phi \times B_\Phi)}{\sum_{\Phi=1}^{n} B_\Phi}, \quad (1)$$

где

- ***Ку*** - коэффициент удовлетворенности, баллов;
- ***Уф*** - среднее значение удовлетворенности по фактору ***ф***, баллов;
- ***Вф*** - среднее значение важности фактора ***ф*** для обеспечения удовлетворенности клиентов качеством услуг, баллов;
- ***ф*** - значимый для обеспечения качества услуг фактор (ф = 1- n).

Для вычисления значения коэффициента удовлетворенности в процентах использовалась формула 2:

$$K_{y(\%)} = \frac{K_y \times 100\%}{5}, \quad (2)$$

где

- ***Ку(%)*** - коэффициент удовлетворенности, %;
- ***Ку*** - коэффициент удовлетворенности, баллов;
- ***5*** - максимальное количество баллов в используемой для сбора первичных данных оценочной шкале (для сбора первичных данных о важности и удовлетворенности по выделенным факторам оценки в данном исследовании применялась пятибалльная шкала).

Результаты анкетирования представлены на рисунках 1-3.

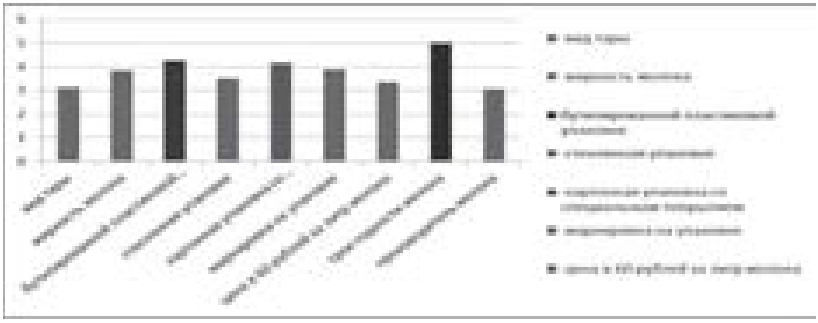


Рисунок 1 - Общий коэффициент важности

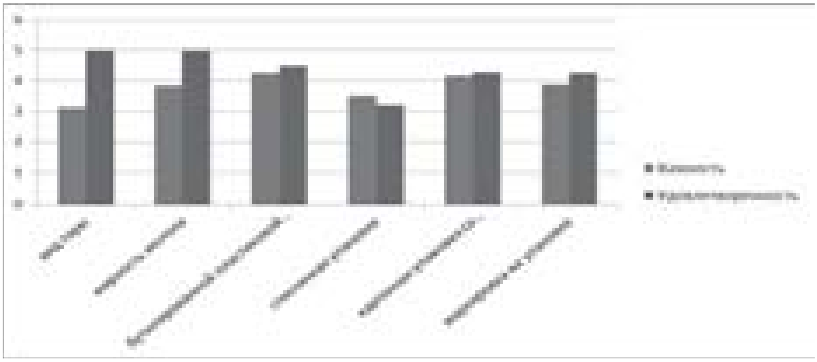


Рисунок 2 - Сравнение коэффициента важности и удовлетворенности

Продукт 1

- Объем – 1 л
- Жирность – 3,2%
- Цена за литр – 138р
- Упаковка - стеклянная
- Ку% - 56,8%
- Основные проблемы продукта вызвавшие низкий процент коэффициента удовлетворенности: Упаковка, Цена.

Продукт 2

- Объем – 1 л
- Жирность – 3,2%
- Цена за литр – 64,55р
- Упаковка – Тетра пак
- Ку% - 86,2%

Продукт 3

- Объем – 1 л
- Жирность – 3,2%
- Цена за литр – 67р
- Упаковка – Тетра пак
- Ку% - 92%

Продукт 4

- Объем – 1 л
- Жирность – 3,2%
- Цена за литр – 62р
- Упаковка – Бутилированное
- Ку% - 76,4%

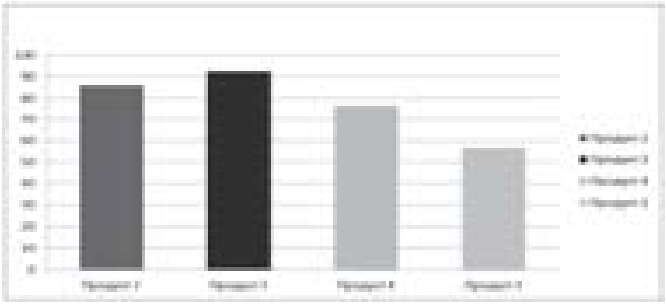


Рисунок 3 - Сравнение коэффициентов удовлетворённости

Анализ полученных данных позволил сформулировать следующие выводы

1) Важнейшими факторами, влияющими на удовлетворённость потребителя, являются упаковка и цена продукта.

2) Согласно коэффициенту важности наиболее важным фактором для потребителя является срок годности продукта. Менее важным оказался вид тары, но при этом потребитель не удовлетворен стеклянной упаковкой.

Рекомендации:

1) Цена в 60 рублей является приемлемой для потребителя, нужно стараться не очень сильно отходить от этой цены.

2) Наиболее важными факторами для потребителя при выборе молока являются: цена, жирность, вид тары, маркировка на упаковке. Следует обращать пристальное внимание на эти факторы.

3) Так же следует обратить внимание на то, что потребитель не очень удовлетворён стеклянной упаковкой, вследствие чего надо что-то поменять в упаковке или отказаться от нее в пользу более популярной.

4) Нужно проводить такие мониторинги мнения потребителя постоянно, для достижения наиболее полного удовлетворения потребностей потребителя и их предвосхищения.

Литература

1. Антипова Т.Н., Асташева Н.П., Горленко О.А., Исаев В.Г., Копылов О.А., Коновалова В.А., Жидкова Е.А., Строителев В.Н., Суслов А.Г. Управление инновациями и качеством. Москва. ФТА, 2013.

2. Асташева, Н.П., Жидкова, Е.А., Исаев, В.Г., Озерский, М.Д., Строителев, В.Н. Критерии выбора и принятия решений [Текст] / Н.П. Асташева, Е.А. Жидкова, В.Г. Исаев, М.Д. Озерский, В.Н. Строителев : монография / под ред. Т.Е. Старцевой. – М.О. г. Королёв: Изд-во «Канцлер». 2015.

ВЛИЯНИЕ ИМПОРТОЗАМЕЩЕНИЯ НА КАЧЕСТВО ОТЕЧЕСТВЕННОЙ ПРОДУКЦИИ

Вершинин Александр Алексеевич, студент 3 курса кафедры Экономики, **Мамонтова Екатерина Вадимовна**, студент 3 курса кафедры Управления качеством и стандартизации
Научный руководитель: **Исаев Владимир Геннадьевич**, к.т.н., доцент, заведующий кафедрой Управления качеством и стандартизации

В России активно работает политика импортозамещения. При этом полки магазинов также забиты продовольственными товарами. Поэтому необходимо проследить изменение качества отечественной продукции, последствия данной политики и все косвенные изменения методом анализа анкетных данных.

Импортозамещение, качество отечественных товаров, импорт, экспорт

THE IMPACT OF IMPORT SUBSTITUTION ON THE QUALITY OF DOMESTIC PRODUCTS

Vershinin Alexander, 3rd year student of the Department of economics, **Mamontova Ekaterina**, 3rd year student of the Department of quality management and standardization
Scientific adviser: **Isaev Vladimir,** Candidate of Technical Sciences, Associate Professor, Head of the Department of quality management and standardization

Russia has been active policy of import substitution products. However store shelves are also filled to capacity by food products. So it's need to attend for changes of quality domestic products, import substitution consequences and all indirect changes by self-administered questionnaire's method.

Import substitution, the quality of domestic goods, imports, exports.

Вот уже два года, как российским производителям выдан карт-бланш: благодаря продуктовым контрсанкциям в отношении продукции из стран ЕС, у них появился шанс завоевать весь рынок. Однако как выяснила газета «Совершенно секретно», делается это в основном за счет ухудшения качества товаров. Также опасаться фальсификатов необходимо при покупке продуктов, не попавших под запреты. В таких условиях нельзя надеяться на «невидимую руку рынка». Необходима вполне «ежовая рукавица» государства.

Выступая перед Федеральным собранием, Владимир Владимирович Путин еще раз напомнил о необходимой политике импортозамещения. По его мнению: «Сегодня приоритетная задача – повышение качества российских товаров. Это непременное условие роста их конкурентоспособности, а значит, успешного продвижения на внутреннем и внешнем рынках».

В 2015 году по сравнению с 2014 годом произошло уменьшение экспорта с 345,84 млрд. долларов США до 263,4 млрд. долларов США, Данные изменения произошли в результате падения цен на нефть до уровня 40$, т.к. экономика России является сырьевой и 65% доходов идет с продажи нефти. Импорт уменьшился с 188,22 млрд. долларов США до 135,8 млрд. долларов США в связи с введением эмбарго на ряд иностранных товаров, но при этом чистый экспорт остался положительным, при этом уменьшился с 155,62 млрд. долларов США до 127,6 млрд. долларов США. Данные изменения

побуждают производить нам самим в связи с сокращением источников для внутреннего рынка. Таким образом, задача России заключается в том, чтобы рос экспорт и падал импорт, а также в изменении структуры экспорта, чтобы вместо сырья продавать готовую продукцию.

Импортозамещаемость – неизбежный атрибут современной региональной экономики, при этом ее уровень и структура должны соответствовать темпам социально-экономического развития территории и уровню внешнеэкономических рисков [2, с.82].

Стоит отметить, что импортозамещение необходимо рассматривать с двух точек зрения: появление «нового» железного занавеса и уменьшение конкурентов, что может спровоцировать волну некачественных товаров, огромного количества фальсификата. С другой стороны, благодаря политики импортозамещения, создается более благоприятная обстановка для отечественных производителей товаров.

Применяя политику импортозамещения, следует учитывать и то, что в связи с существующими ограничениями по имеющимся ресурсам или технологиям ни одна страна мира не сможет полностью отказаться от импортной продукции, а на начальном этапе производимые товары внутри страны могут быть более низкого качества, чем ввозимые [1, с.57].

При этом у импортозамещения есть положительные и отрицательные моменты. В отрицательных моментах можно выделить следующее:

- Отсутствие импортной продукции.
- Появление большого количества фальсификата.
- Отсутствует оперативная информация о выпускаемой продукции.

В положительных же моментах стоит отметить:

- Увеличение объемов производства и сбыта.
- Усовершенствование отечественной техники и технологий.
- Усовершенствование нормативной базы.

Некоторые недобросовестные производители действуют по простому способу импортозамещения. Изготавливая свою продукцию, они используют дешевые заменители ингредиентов. Данный способ быстрее и проще, чем вкладывать деньги в строительство новых мощностей, покупку сельхозугодий, закупку сырья, набор и обучение персонала. Если верить статистике, Россия

сумела заменить запретный пармезан собственными сырами – их производство выросло на 37 %. При этом молока российские буренки дали на 2 % меньше, а импорт молока упал на 40 %.

Но если посмотреть на импорт в Россию пальмового масла, то он за это же время вырос на 27%. Недавно Союз потребителей «Росконтроль» провел мониторинг по выявлению фальсифицированной молочной продукции. Результаты оказались шокирующими: из проверенных более 40 образцов сливочного масла и сыра в 70% торговых марок выявлена замена молочного жира растительным. В частности – пальмовым маслом. К счастью, не все производители так поступают.

Чтобы в этом убедиться, мы решили провести свой анализ. Для анализа мы рассматривали рынок пищевой продукции, а именно сыры и мясо, сыры входят в тройку лидеров по фальсификации, а мясо и мясные продукты, взятых производителей, являются одними из лидеров продаж. Помимо этого мы решили проанализировать изменение качества товаров на полках сетевых магазинов на примере: «Пятерочка», «Дикси», «Магнит». Мы предлагали людям заполнить анкету, которая представлена на рисунке 1.

В данном опросе приняло участие 64 человека. Мы ранжировали на 5 возрастных групп:

- До 18 лет.
- От 18 до 25 лет.
- От 25 до 45 лет.
- От 45 до 60 лет.
- Более 60 лет.

Но необходимо отсеять участников, попавшие в группу 1 и 5, т.к. люди в этой группе выбирают скорее дешевый, нежели качественный товар, в связи с недостаточной социальной поддержкой данных категорий.

А также была произведена ранжировка по уровню доходов в месяц на 5 групп:

- Низкое (МРОТ).
- Ниже среднего (От МРОТ до 15 тыс. руб.).
- Среднее (15 – 30 тыс. руб.).
- Выше среднего (30 – 45 тыс. руб.).
- Высокое (Более 45 тыс. руб.).

Также был проведен анализ трех магазинов «Пятерочка», «Дикси», «Магнит».

Анкета

Вопросы	Ответы
В какой вы возрастной категории?	1. До 18 лет 2. От 18 до 21 лет 3. От 21 до 45 лет 4. От 45 до 60 лет 5. Более 60 лет
Ваше материальное положение, т.р в месяц?	1. Низкий (МРОТ) 2. Ниже среднего (От МРОТ до 13 тыс. руб) 3. Средний (13 – 30 тыс. руб) 4. Выше среднего (30 – 45 тыс. руб) 5. Высокий (Более 45 тыс. руб)
Как часто вы ходите в магазин делать большие покупки?	1. Один раз в месяц 2. Два раза в месяц 3. Один раз в неделю 4. Два раза в неделю 5. Каждый день
Сказалось ли на вашей потребительской корзине покупок импортозамещение?	1. Да 2. Нет 3. Не обратил на внимание
Заметили ли вы изменения в качестве товара?	1. Да, оно стало хуже 2. Да, оно стало лучше 3. Нет, оно не изменилось
Стараетесь ли вы покупать отечественные товары?	1. Да, покупаю для того, чтобы поддержать отечественного производителя 2. Да, покупаю, потому что считаю, что оно лучшего качества 3. Нет, считаю его не конкурентоспособным 4. Иное
Довольны ли вы качеством товаров на полках магазинов?	1. Да, полностью устраивает 2. Нет, полностью не устраивает 3. Трудновато сказать
Что для вас главное при выборе и покупке товара? (выберите 2 пункта)	1. Качество 2. Цена 3. Марка, бренд, производитель 4. Советы друзей, коллег 5. Реклама 6. Популярность 7. Иное

Рисунок 1 – Анкета для потребителей

По результатам опросов, данные оказались приятно удивительными. В магазине «Дикси» заметили улучшение 48% процентов опрошенных, 38% не заметили изменений и лишь 14% заметили ухудшение качества. Данные представлены на рисунке 2. В магазине «Пятерочка», не заметивших изменений и заметивших улучшение качества было одинаково по 39%, заметивших ухудшение 22%. Данные представлены на рисунке 3. И в магазине «Магнит» 53% отметили улучшение качества продукции, 19% увидели ухудшение качества товаров на полках и 28% не заметили изменений. Данные представлены на рисунке 4.

Также респонденты отвечали на ряд вопросов, по которым можно сделать вывод, что продуктовая корзина 69% опрошенных не подверглась изменению, 18% изменили ее, а 13% не заметили разницы.

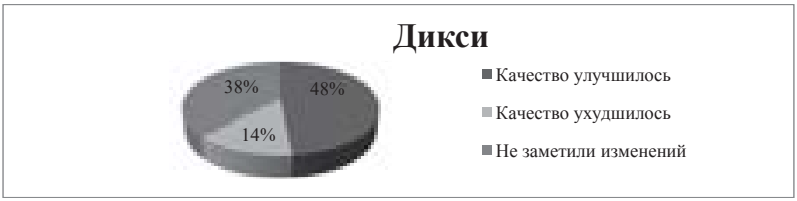


Рисунок 2 – Качество на полках магазина «Дикси»

Рисунок 3 – Качество на полках магазина «Пятерочка»

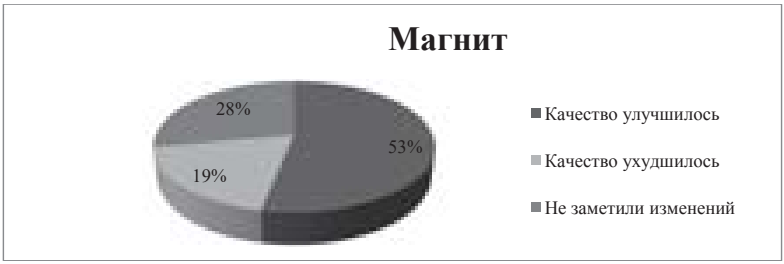


Рисунок 4 – Качество на полках магазина «Магнит»

Данные представлены на диаграмме 4. Было выявлено, что 17% покупателей приобретают отечественный товар, чтобы поддержать отечественного производителя, 16% приобретаю отечественный по причине высокого качества товара, при этом 25% не считают его конкурентоспособным и не приобретают его, и 42% опрошенных не придают значения производителю. Данные представлены на рисунке 6.

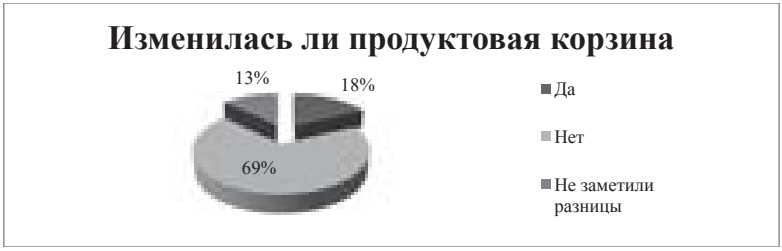


Рисунок 5 – Изменения в продуктовой корзине покупателей

Рисунок 6 – Отношение к покупке отечественных товаров

Рисунок 7 – Приоритеты покупателей при приобретении товаров

Помимо этого, мы предложили 5 критериев, которые выбирали респонденты в качестве первостепенного для себя при покупке. Можно сделать вывод, что для потребителей на первом месте стоит «цена» (30% опрошенных), второе место занимает «качество» (20%), третье «советы друзей, коллег» (16%), далее с результатом 15% идет «марка и бренд» товара, 12% и 7% соответственно получили «иное» и «реклама». Данные представлены на рисунке 7.

Также был проведен сравнительный анализ 6 видов продуктов: сыр фирмы «Город сыра» голландский 48%, сыр фирмы «Город сыра» российский 45%, сыр фирмы «Красная цена» 50%, фарш фирмы «Эколь» говяжий, филе грудки цыплят-бройлеров «Первая свежесть» и говядина тушеная «Гродфуд». Оценка производилась по четырем параметрам, вес каждого параметра единица. В опросе приняло участие 60 человек, по 10 человек на каждый вид продукта. Пример анкеты, которую заполняли опрашиваемые, представлен на рисунке 8. Для анализа данные о натуральности брались с сайта roscontrol.ru из-за отсутствия собственной лаборатории. Вкусовые ощущения, а также внешний вид оценивали респонденты, а баллы на цену начислялись по формуле 1:

$$Б = \frac{ЦТср}{ЦПср} * 100, \quad (1)$$

Б – баллы, начисляемые в результате опроса;

ЦТср – цена товара, средняя по магазинам, руб;

ЦПср – цена продукта (всех сыров данного вида), средняя по магазинам, руб.

Для примера: Цена сыра N вида «Российский» за 1 кг составляется 240 рублей, средняя цена по сырам вида «российский» за 1 кг 500 рублей. Тогда получаем 240/500*100=48 баллов.

Первым был оценен сыр фирмы «Город сыра» голландский, 48%, по нашему опросу он получил средние 77 балла (Натуральность 90, Вкусовые ощущения 76, Внешний вид 80, Цена 62), при этом оценка Росконтроля 76 баллов (Безопасность 80, Натуральность 90, Полезность 48, Дегустация 85) из 100, что говорит о примерном совпадении результатов, следовательно, правильной оценки.

Далее оценивался сыр фирмы «Город сыра» российский 45%, по нашему опросу он получил 71 балл (Натуральность 70, Вкусовые ощущения 73, Внешний вид 80, Цена 62), при оценке Росконтроля в 66 балла (Безопасность 70, Натуральность 70, Полезность 45, Дегустация 78). Результаты выше среднего, что говорит о неплохом качестве товара.

Для проверки гипотезы, что дешевый продукт не означает некачественный, мы оценили сыр фирмы «Красная цена», 50%. По результатам он получил 64 балла (Натуральность 70, Вкусовые ощущения 54, Внешний вид 49, Цена 83), при 58 баллах (Безопасность 50, Натуральность 70, Полезность 45, Дегустация 68) Росконтроля, это означает, что дешево – это не значит некачественно.

Говяжий фарш «Эколь» получил 64 балла (Безопасность 80, Натуральность 54, Полезность 64, Дегустация 57) по сравнению с 48 баллами (Безопасность 31, Натуральность 80, Полезность 40). Полученный итог сильно разнится, это может быть связанно с тем, что Росконтроль оценил по 3, а не 4 критериям.

Куриные грудки фирмы «Первая свежесть» получил 64 балла (Безопасность 85, Натуральность 79, Полезность 76, Дегустация 68) по сравнению с 52 баллами (Безопасность 77, Натуральность 85, Полезность 47) Росконтроля, возможно, данные сильно разнятся также из-за количества критериев оценки товара.

Тушеная говядина фирмы «Гродфуд» получил такую же оценку в нашем тесте, что и у Росконтроля, 65 баллов (Безопасность 75, Натуральность 62, Полезность 59, Дегустация 64) – наш тест,

(Безопасность 72, Натуральность 75, Полезность 33, Дегустация 78) – тест Росконтроля. Данные говорят об объективной оценке данного товара.

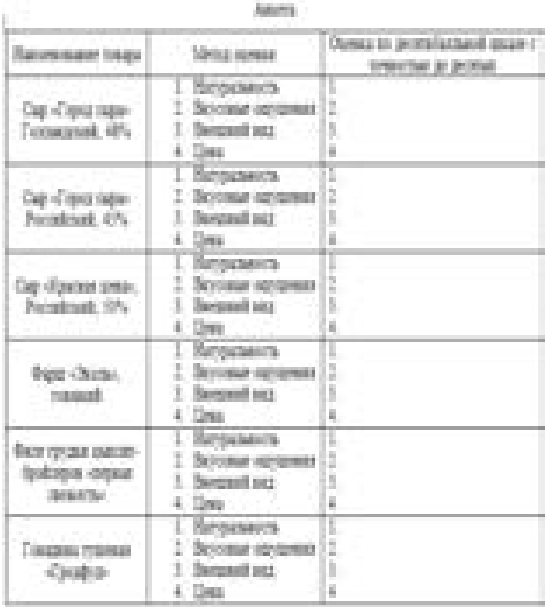


Рисунок 8 – Анкета по конкретным видам продукции

Подводя итоги по качеству отечественного товара, можно сформулировать следующие выводы:

1. Качество отечественных товаров находится на надлежащем уровне;
2. Отечественный товар пользуется популярностью у россиян;
3. Политика импортозамещения не сильно повлияла на потребительские корзины граждан, что говорит о ее эффективной работе и правильном замещении продукции.

В целом достигнуты не плохие результаты, но необходимо добавить несколько рекомендаций для улучшения функционирования данной политики, а именно:

- Шире использовать российские премии по качеству, например, «Сто лучших товаров», «Экологически чистый продукт» и т.д.;
- Оперативно пресекать появление контрафактной продукции, увеличив или ужесточив наказание за производство фальсификата;
- Проверять качество товара на всех стадиях жизненного цикла

производства, чтобы избежать появление некачественного товара, тем самым уменьшить количество брака продукции, что повлечет за собой уменьшение себестоимости товара и снижение рыночной цены на товар;

- Открыть доступ к банку «Продукции России» для всех желающих, чтобы каждый смог выбирать качественный и удовлетворяющий его потребностям товар;
- Актуализировать Постановление Правительства РФ от 01.12.2009 №982 (ред. от 03.09.2015) «Об утверждении единого перечня продукции, подлежащей обязательной сертификации, единого перечня продукции, подтверждение соответствия которой осуществляется в форме принятия декларации о соответствии»;
- Проводить мероприятия в СМИ по обучению потребителей по вопросам обеспечения качества.

Литература

1. Вопросы региональной экономики №3(24) 2015
2. Вопросы региональной экономики №4(21) 2014
2. [Электронный ресурс]. Режим доступа: http://voprosik.net/kak-importozameshhenie-vliyaet-na-kachestvo-tovarov/ (дата обращения 01.02.2016)
3. [Электронный ресурс]. Режим доступа: http://rueconomics.ru/122012-importozameshhenie-v-deystvii-v-rf-stali-bolshe-doveryat-kachestvu-otechestvennyih-produktov (дата обращения 04.02.2016)
4. [Электронный ресурс]. Режим доступа: http://rg.ru/2014/12/04/importozameshchenie-anons.html (дата обращения 31.01.2016)
5. [Электронный ресурс]. Режим доступа: http://bloknot.ru/rossiya/putin-ob-importozameshhenii-my-absolyutno-vse-mozhem-sdelat-sami-100220.html (дата обращения 26.01.2016)

ИЗУЧЕНИЕ ВНЕДРЕНИЯ НОВЫХ ТЕХНОЛОГИЙ В КРАЕВЕДЧЕСКИЕ МУЗЕИ

Джабарова Лейла Маратовна, студентка 3 курса кафедры Управления качеством и стандартизации
Научный руководитель: **Исаев Владимир Геннадьевич,** к.т.н., доцент, заведующий кафедрой Управления качеством и стандартизации

В работе рассмотрено влияние организации изменений путем внедрении инноваций в краеведческие музеи. Проведены опросы населения для определения мнения потребителя и его предпочтений. На основании этих данных были составлены рекомендации для улучшения качества музеев.

Качество, инновации, музеи.

RESEARCH OF INTRODUCTIONS NEW TECHNOLOGIES IN MUSEUM

Dzhabarova Leila, 3rd year student of the Department of quality management and standardization
Scientific adviser: **Isaev Vladimir,** Candidate of Technical Sciences, Associate Professor of the Department of the Quality management and standardization

In work influence of the organization of changes implementation considered innovations in museum. Population surveys were done to determine the opinion of the consumer and his preferences. Relying on that data, recommendations for the improvement quality of museum constituted.

Quality, innovation, museum.

В настоящее время нормативных документов, касательно данной темы, не существует. Однако, многие политики постепенно затрагивают эту проблему в своих выступлениях. Так же министр культуры Правительства Московской области Галина Ратникова выслушав вопрос о создании виртуальных музеев ответила так: « Для нас интернет сейчас не ново и конечно это вполне неплохая идея, которую мы хотим осуществить уже не первый год. Вы конечно же должны понимать, что это достаточно дорогостоящий проект и

поэтому это долговременный процесс….но я хочу сказать что ДА этот проект вполне осуществим и да мы будем его реализовывать . Конечно не могу обещать ,что в следующем году все музеи будут иметь свой персональный виртуальный музей ,но большинство крупных музеев Московской области вы сможете посетить сидя перед экранов компьютера и при этом находясь за тысячу километров от интересующего их места. Например, в городе Королёве существует муниципальный музей космического машиностроения доступен не всем жителям, а сотрудникам и студентом предприятий.

Поэтому целесообразно для начала составить методы внедрений инноваций и указать точные предложения по улучшению качества работы музеев. Для достижения этой цели были поставлены следующие задачи:

1. краеведческая кухня с указанием особенности кухни данной местности (травы грибы, разновидности одного блюда);
2. создание книги рецептов, в которую посетитель мог предложить вписать рецепт блюда, которое было бы связано с этим краем;
3. создание виртуальных музеев;

Для решения этих задач была разработана соответствующая анкета и проведен опрос населения. В анкете были заданы следующие вопросы:

1. Укажите, пожалуйста, ваш возраст.
2. Укажите ваш пол.
3. Вид деятельности.
4. Важно ли для вас расположение музея.
5. Хотели бы вы помочь в изменении музеев (если да то чем именно).
6. Обращаете ли вы внимание на рекламу о выставках в музее вашего города.

Для того чтобы выявить степень согласованности мнений жителей (респондентов) мы использовали коэффициент конкордации. Коэффициент конкордации – коэффициент ранговой корреляции для группы, состоящей из ***m*** респондентов.

Коэффициент конкордации является мерой согласованности мнений респондентов по нескольким факторам с учётом их важности.

Результаты опроса представлены на рисунках 1-3. В ходе исследования было опрошено 120 респондентов. Из них - 42% женщины и 58% мужчины. Средний возраст опрошенных 24 года

минимальный возраст 14 лет максимальный 92 года. Состав респондентов представлен на рисунке 1.

Анализ данных, представленных на рисунках 1-3, показал следующее:

Рисунок 1 - Контингент опрошенных

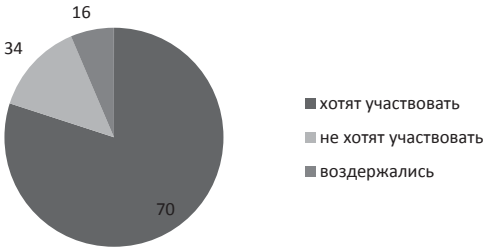


Рисунок 2 - Количество опрошенных и их желание

На рисунке 2 показано насколько люди интересуются музеями и хотят принять участие в изменении музеев. Анализ этих данных показывает, что музей является проблемой для многих и они хотели бы изменить его при условии, что это будет не только как временный проект (игрушка), а серьезный проект.

Рисунок 3 - Актуальность данной темы, по мнению опрошенных

На рисунке 3 мы видим, что на ключевой вопрос: Является ли данная тема актуальной? Большинство респондентов считает, что это не самое важное, но на это все же стоит обратить внимание. На основании полученных данных можно сделать вывод, что музеи теряют свою популярность поскольку людям живущим в 21 веке хочется узнавать старину не только слушая вызубренные тексты, но и видеть насколько это было важно людям того времени.

Следует отметить, что проведённые исследования не учитывали стоимость данных изменений, возрастные пристрастия потребителей, особенности вида деятельности и т.д.

На основе проведенного исследования можно сформулировать следующие выводы и рекомендации:

1. Появление разнообразных, в том числе и виртуальных, музеев, а также развитие новых направлений и форм музейной деятельности происходит во многом стихийно, без осознания глубинного единства и связи между их разноплановыми проявлениями. Ситуация, когда практика обгоняет теорию, может считаться нормальной только до определенного предела. Современному музееведению необходимо понимание общих закономерностей возникновения и трансформации музейной потребности и осмысление новой роли музея в обществе и культуре. Это обусловлено, с одной стороны, этапом становления музееведения как самостоятельной дисциплины, а с другой, насущными практическими задачами. При создании концепций современных музеев не достаточно учитывать только историческую и культурную значимость музеефицируемых объектов. Необходимо понимание социальных и культурно-исторических закономерностей эволюции музейной потребности, а также основ функционирования музея как социокультурного феномена.

2. Максимальную актуальность экспозиций (инсталляций) самих по себе, средств их экспонирования и организации пространства. Три года назад я работала над дипломным проектом по музейной теме, столкнувшись с общей кризисной ситуацией жанра в глобальном музейном пространстве. Одной из главных идей была максимальная открытость-доступность музея, отсутствие преград (каких бы то ни было). "Город - музей", "Музей как имидж-технология", "Руками трогать!", "Музей - место встречи, приятного время-провождения" и пр. Конечно, это проблемно, для музеев, демонстрирующих ценные (даже ветхие) с исторической точки зрения экспонаты, однако здесь и открывается место, для размышления над технологиями самого по себе экспонирования.

Литература

1. Антипова Т.Н., Асташева Н.П., Горленко О.А., Исаев В.Г., Копылов О.А., Коновалова В.А., Жидкова Е.А., Строителев В.Н., Суслов А.Г. Управление инновациями и качеством. Москва ФТА, 2013-300с.

2. Размустова Т.О. По дороге к возрождению// Известия культуры России.—1990— № 8. Музейное дело России. М., 2003;
3. Сундиева А.А. Краеведческие музеи на пороге нового века.//Современное состояние и перспективы развития краеведения в регионах России: Материалы Всероссийской научно-практической конференции 10-11 декабря 1998.— М., 1999.— С. 89—94.

ИННОВАЦИОННЫЕ РЕШЕНИЯ ОРГАНИЗАЦИИ ПАССАЖИРСКИХ ПЕРЕВОЗОК

Зернов Иван Романович, студент 4 курса кафедры Управления качеством и стандартизации
Научный руководитель: **Костылёв Андрей Геннадиевич,** к.т.н., доцент кафедры Управления качеством и стандартизации

Для современной России значение транспорта велико, поскольку именно транспорт объединяет множество регионов страны в единое государство. В связи с этим транспорт является одним из важнейших государство образующих факторов. Степень удовлетворения потребности населения в передвижении влияет как на экономику региона, так и на социальные взаимодействия, поэтому большое значение имеет качество пассажирских перевозок.

Качество пассажирских перевозок, анализ пассажиропотока по времени суток, методы исследования пассажиропотока.

INNOVATIVE SOLUTIONS OF THE ORGANIZATION OF PASSENGER TRANSPORTATION

Zernov Ivan, student 4 courses of the Department of management of quality and standardization
Scientific adviser: **Kostylyov Andrey,** Candidate of Technical Sciences, Assistant Professor of the Department of management of quality and standardization

For modern Russia relevance of transport is great as transport unites a set of regions of the country in the uniform state. In this regard transport is one of the major of the state forming factors. Degree of satisfaction of need of the population for movement influences both region economy, and social interactions therefore quality of passenger traffic is of great importance.

Quality of passenger transportation, the analysis of a passenger transportation on time of day, methods of research of a passenger transportation.

Требования к качеству пассажирских перевозок

На существующем этапе развития организации пассажирских перевозок можно выделить свойства, характеризующие качество услуги в целом, которые представлены в таблице 1 [3].

Таблица 1 – Свойства, характеризующие качество пассажирских перевозок

Свойство	Требования	Показатели
Доступность	насыщенность транспортом городской территории	плотность маршрутной сети, частота движения на маршрутах
	информативность	уровень информационного обслуживания пассажиров
	доступные тарифы	социальная приемлемость и стабильность тарифов
Результативность	экономия затрат времени	затраты времени на поездку, коэффициент затрат
	экономия сил пассажиров	уровень транспортной усталости пассажиров
Надежность	регулярность сообщения	коэффициенты регулярности, среднеквадратичные отклонения от расписания
	гарантированность уровня обслуживания	вероятность отказа пассажиру в поездке
	безопасность поездки	динамичность показателя безопасности движения
Удобство	наполнение автобуса пассажирами	коэффициент использования вместимости
	комфортабельность	соответствие нормативам комфортабельности

Пути повышения качества пассажирских перевозок

1. Рациональное распределение транспортных средств по маршрутам путем постоянного систематического анализа пассажиропотоков;

2. Улучшение оборудования автобусных маршрутов, транспортных средств и технических сооружений, направленное на лучшее обслуживание пассажиров, повышение безопасности движения и повышение объема автобусных перевозок;

3. Улучшение условий организации труда автобусных компаний, направленное на повышение производительности труда, безопасности движения и лучшее обслуживание пассажиров.

4. Повышение качества обслуживания пассажиров в часы пиковой нагрузки, путем рационального распределения транспортных средств по маршруту.

5. Рациональное размещение автотранспортных предприятий, их филиалов и организации обслуживания маршрутов двумя автобусными парками, с целью снижения нулевых пробегов [1].

Методы анализа пассажиропотока по времени суток

Для выявления пассажиропотоков, распределения их по маршрутам, сбора данных об изменениях пассажиропотоков во времени суток проводят исследования. Существующие методы исследования разделяются по ряду признаков. По длительности охватываемого периода исследования бывают систематические (в течение всего периода движения) и разовые (кратковременные по той или иной причине). По ширине охвата транспортной сети разделяют на сплошные (одновременно по всей транспортной сети) и выборочные (по отдельным районам движения). По виду методы обследования могут быть анкетными, отчетно-статистическими, натурными и автоматизированными.

Анализ пассажиропотока по времени суток состоит в краткосрочном прогнозировании пассажиропотока, что позволяет с большой вероятностью рассчитать загруженность маршрута на ближайшее время и впоследствии корректировать количество транспортных средств на маршруте.

Создание алгоритма краткосрочного прогнозирования пассажиропотока сопряжена с учетом огромного количества факторов, которые могут образовываться как по причине причинно-следственных связей, так и по причине неопределенности. Последние усложняют задачу и, в этом случае, необходимо использовать в комплексе вероятностно-статистические методы для получения конкретных решений [2].

Заключение

В настоящее время наиболее актуальны вопросы совершенствования технологических, организационных и управленческих процессов. Так как даже если бы удалось заменить большую часть транспортных средств и создать современную систему их технического обслуживания и ремонта, то при нынешнем уровне перевозок, системе финансирования с трудом можно будет получить значительный и устойчивый эффект. При этом удорожание

фондов приведет только к росту себестоимости перевозок, что может негативно отразится при формировании стоимости проезда.

Решение технологических, организационных и управленческих вопросов требует значительно меньших затрат и может быть проведено в сжатые сроки, в то время как развитие инфраструктуры и техническое переоборудование требуют огромных инвестиций.

Литература

1. Гудков В.А. и др. Технология, организация и управление пассажирскими автомобильными перевозками М. Транспорт, 1997 г. 254 с
2. Загорский И. О. Эффективность организации регулярных перевозок пассажирским автомобильным транспортом / И. О. Загорский, П. П. Володькин. – Хабаровск : Изд-во Тихоокеан. гос. ун-та, 2012. – 154 с.
3. Организация дорожного движения: учебник для вузов / Г.И. Клинковштейн, М.Б. Афанасьев. - М.: Транспорт, 2001

ВХОДНОЙ КОНТРОЛЬ КАЧЕСТВА НА ПРЕДПРИЯТИИ РАКЕТНО-КОСМИЧЕСКОЙ ОТРАСЛИ

Касимова Анна Дмитриевна, магистрант 1 курса кафедры Управления качеством и стандартизации
Научный руководитель: **Шайдуров Валерий Сергеевич**, д.х.н., профессор базовой кафедры Управления качеством в области новых материалов и технологий

В статье рассмотрен один из элементов системы менеджмента качества – входной контроль качества. Проведен анализ состояния системы входного контроля качества продукции на предприятиях ракетно – космической отрасли в настоящее время, выявлены основные недостатки. Разработаны предложения по совершенствованию системы входного контроля качества, которые позволят исключить возможности проникновения в производство продукции с отступлениями от требований к качеству.

Система входного контроля качества, совершенствование системы входного контроля.

INCOMING INSPECTION QUALITY IN THE SPACE INDUSTRY

Kasimova Anna, 1rd year undergraduate student of the Department quality management and standardization
Scientific adviser: **Shaidurov Valery**, Doctor of Chemical Sciences, professor base of the Department of quality management of in the field of new materials and technologies

The article describes one of the quality management system elements - incoming inspection quality. The analysis of incoming inspection quality system in the space industry at the moment, the main shortcomings identified. Developed proposals for improving incoming inspection quality system that will eliminate the possibility of penetration into production with deviations from quality requirements.

Incoming inspection system quality, improving the system of incoming inspection quality.

Постоянная конкуренция на мировом рынке космических услуг диктует ракетно-космической промышленности острую необходимость в поставках качественной продукции.

В условиях жесткой конкуренции на рынке, изготовитель стремится добиться стабильного качества своей продукции, используя все инструменты, выработанные мировой практикой. Одним из них является система менеджмента качества (СМК), комплексно охватывающая все аспекты деятельности предприятия и получившая широчайшее распространение и признание во всем мире. СМК является частью общей функции управления предприятием, связанной с формированием и реализацией целей политики в области качества [3].

Важным элементом системы менеджмента качества является входной контроль качества сырья и материалов.

Входной контроль (верификация) проводится с целью проверки соответствия качества закупленной продукции требованиям промышленной безопасности, нормативно-технической и эксплуатационной документации и предупреждения запуска в эксплуатацию продукции ненадлежащего качества [2].

В настоящее время особенно актуальным является проблема организации входного контроля качества продукции. Однако, на отдельных предприятиях данному виду контроля уделяют недостаточно внимания, что приводит к проблемам в процессе

изготовления и выпуска продукции.

В космической технике крайне востребованы композиционные материалы (КМ). КМ состоят из связующего и армирующего наполнителя. Качество КМ находится в непосредственной зависимости от качества исходного сырья [6].

Статистический анализ данных в течение последних пяти лет, показал, что количество рекламаций по выпущенным изделиям из композиционных материалов ежегодно растет на 2-3%.

Основными недостатками организации входного контроля на предприятиях ракетно-космической промышленности являются:

- недостаточная численность персонала, приводящие к нарушению ритмичности производства и реализации продукции, невыполнению отдельных работ по контролю качества, появлению бесконтрольных участков производства;
- недостоверность результатов контроля, низкая требовательность и субъективизм в оценке качества продукции;
- слабая техническая вооруженность и несовершенство метрологического обеспечения;
- несовершенство методик измерений, дублирование и параллелизм в работе по оценке качества;
- относительно низкая заработная плата работников служб контроля качества;
- несовершенство системы премирования персонала контрольных служб, приводящая к незаинтересованности в полном и своевременном выявлении брака;
- недостаточная компетентность персонала в вопросах контроля качества.

Применительно к рассматриваемым проблемам, построим причинно-следственную диаграмму или диаграмму Исикавы, которая служит для графического изображения взаимосвязи показателя качества со всеми возможными причинами (рисунок 1).

Указанные обстоятельства предопределили необходимость выработки ряда мер (нормативно-правовых, организационных и методических), направленных на обеспечение организации входного контроля качества.

Для организации входного контроля продукции на предприятиях ракетно-космической промышленности, действуют следующие стандарты [3, 4, 6]:

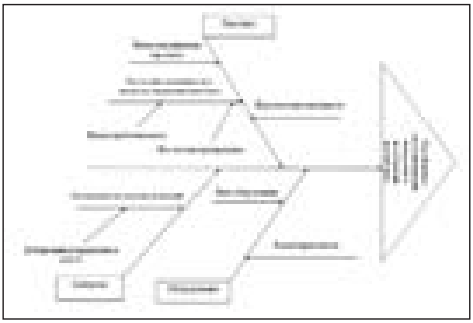


Рисунок 1 – Причинно-следственная диаграмма

- ГОСТ РВ 0015-308-2011 «Система разработки и постановки на производство военной техники. Входной контроль изделий. Основные положения».
- ГОСТ 24297-2013 «Верификация закупленной продукции. Организация проведения и методы контроля».
- ГОСТ Р 52745-2007 «Контроль качества материалов и полуфабрикатов, используемых при изготовлении изделий авиационной, космической, оборонной техники и техники двойного применения. На предприятиях - поставщиках. Общие требования».

Для обеспечения выполнения требований ГОСТ 24297 с учетом типа и особенностей выпускаемой продукции разрабатываются стандарты предприятия (СТП). СТП устанавливает порядок организации, проведение и оформление результатов входного контроля изделий, поступающих на предприятие.

Входной контроль может быть сплошным или выборочным [2].

Сплошной входной контроль проводят:

- По требованию представителя заказчика.
- При освоении новых видов ракетно-космической техники.
- При наличии требований в нормативной документации.

Выборочный входной контроль устанавливают:

- При получении материалов, изделий в количествах, позволяющих применение статистических методов контроля.
- При невозможности без разрушения провести контроль поступившей продукции.
- При условии экономической нецелесообразности сплошного контроля.

Для обеспечения высокого качества выпускаемых изделий важную роль играет совершенствование системы входного контроля

исходного сырья, которое позволяет исключить возможности проникновения в производство данного сырья с отступлениями от требований к качеству, которые указаны в договоре.

Совершенствование системы входного контроля осуществляется по следующим направлениям [5]:

- Совершенствование технологии контроля.
- Совершенствование средств контроля.
- Повышение квалификации персонала.
- Совершенствование документального обеспечения системы входного контроля

Для реализации перечисленных направлений, на ракетно-космическом предприятии необходимо осуществить следующие задачи:

- Создание мероприятий по предупреждению брака в производстве.
- Статистическое регулирование утвержденных технологических процессов.
- Внедрение японской философии «Кайдзен», которая фокусируется на непрерывном совершенствовании процессов производства, разработки, вспомогательных бизнес-процессов и управления, а также всех аспектов жизни.
- Применение системы 5S - инструмента бережливого производства на рабочих местах сотрудников.
- Внедрение системы ключевых показателей эффективности и результативности персонала отдела входного контроля, которые помогут данному подразделению в достижении стратегических и тактических целей.
- Создание эффективной системы материальной и нематериальной мотивации сотрудников для того, чтобы повысить заинтересованность в работе, которая отразится на повышении производительности труда.
- Повышение кадрового потенциала подразделений технического контроля, которое подразумевает выявление трудового потенциала подразделения, профессиональное образование работников, управление движением персонала, формирование кадрового резерва.

Реализация указанных направлений и задач позволит осуществлять своевременное выявление и предупреждение

отклонений от установленных требований, выявить и устранить причины снижения качества выпускаемой продукции.

Литература

1. ГОСТ РВ 0015-308-2011 Система разработки и постановки на производство военной техники. Входной контроль изделий. Основные положения.
2. ГОСТ 24297-2013 Верификация закупленной продукции. Организация проведения и методы контроля.
3. ГОСТ Р ИСО 9001-2015 Системы менеджмента качества. Требования.
4. ГОСТ Р 52745-2007 «Контроль качества материалов и полуфабрикатов, используемых при изготовлении изделий авиационной, космической, оборонной техники и техники двойного применения. На предприятиях - поставщиках. Общие требования».
5. Гумеров А. В. Совершенствование системы входного контроля качества промышленного предприятия [Текст] // Актуальные вопросы экономических наук: материалы междунар. науч. конф. — Уфа: Лето, 2011. С88-90.
6. Миронов Ю.М., Нелюб В.А., Бородулин А.С., Чуднов И.В., Буянов И.А., Александров И.А., Муранов А.Н. Исследование качества поверхностей углеродных волокон. - Электронный научно-технический ж. Инженерный вестник. - №11, ноябрь 2012.

ВЫБОР ПОСТАВЩИКА ЛИПКОЙ ЛЕНТЫ И АНАЛИЗ КРИТЕРИЕВ ЕГО ВЫБОРА

Ханжина Екатерина Евгеньевна, студентка 4 курса кафедры Управления качеством и стандартизации, **Касаткин Иван Павлович,** магистрант 1 курса кафедры Управления качеством и стандартизации
Научный руководитель: **Воейко Ольга Александровна**, к.т.н., доцент кафедры Управления качеством и стандартизации

Одной из основных проблем в управлении закупками ресурсов является выбор поставщика. Важность ее объясняется не только тем, что на современном рынке функционирует большое количество поставщиков схожих ресурсов, а и, главным образом тем, что поставщик должен быть надежным партнером предприятия в реализации его стратегий.

Квалиметрия, критерий, оценка, коэффициент, значимость, согласованность, выбор поставщика.

THE CHOICE OF A SUPPLIER OF PRODUCTS AND AN ANALYSIS OF THE CRITERIA OF ITS SELECTION

Khanzhina Catherine, 4rd year student of the Department of quality management and standardization, **Kasatkin Ivan,** 1 undergraduate course of the Department of quality management and standardization
Scientific adviser: **Voeiko Olga,** Candidate of Technical Sciences, Associate Professor of the Department of quality management and standardization

One of the main problems in the management of procurement resources is the choice of supplier. The importance of this is explained not only by the fact that the market operates a large number of suppliers have similar resources, but mainly that the Supplier should be a reliable partner of the enterprise in the implementation of its strategy.

Qualimetry, criterion, estimate, factor, relevance, coherence, choice supplier, the choice of supplier.

При осуществлении закупок одной из важнейших задач является выбор поставщика. Он включает поиск источников снабжения и оценку возможности своевременной поставки и предоставления необходимых услуг до и после продажи [3].

Ввиду невозможности получения прямой количественной оценки поставщиков для разработки методики ее проведения принято использовать принципы квалиметрии.

Квалиметрия выделяет несколько методов определения показателей качества. В основном применяются экспертные методы оценки.

При проведении квалиметрической оценки поставщиков продукции необходимо сформировать номенклатуру из нескольких критериев, после их анализа рассчитать коэффициент весомости для каждого критерия, с помощью которых и будет выбираться поставщик [1].

Выбор и оценка критериев

Для выбора поставщика липкой ленты используем 5 критериев состоящих из единичных показателей:

1. Репутация фирмы поставщика;

2. Цена продукции;
3. Уровень поставки (срок поставок партии);
4. Уровень обслуживания (скорость оформления заказа);
5. Качество продукции (наличие сертификата соответствия).

Пятый критерий является релейным, он не нуждается в ранжировании, так как имеет только два значения, да и нет.

Для квалиметрической оценки и выбора поставщиков необходимо провести опрос и заполнить матрицу оценок.

Первым шагом определяется согласованность мнений экспертов (в экспертную группу вошли 3 эксперта).

Таблица 1 – Матрица рангов

№п/п	Критерий	Экспертная группа		
		Э1	Э2	Э3
1	Репутация фирмы поставщика (x1)	2	2	1
2	Цена продукции (x2)	1	1	1
3	Уровень поставки (x3)	3	4	4
4	Уровень обслуживания (x4)	4	3	3

Так как в матрице имеются связанные ранги (одинаковый ранговый номер) в оценках эксперта Э3, производится переформирование (таблица 2):

Таблица 2 – Переформирование рангов Э3

Номера мест в упорядоченном ряду	1	2	3	4
Расположение факторов по оценке экспертов	1(x1)	1 (x2)	3 (x4)	4 (x3)
Новые ранги	1,5	1,5	3	4

На основе переформирования рангов строится новая матрица рангов (таблица 3):

Таблица 3 – Переформированная матрица рангов

Эксперты / Факторы	Э1	Э2	Э3	Сумма рангов	Ср. ранг	Δ	$Д^2$
x1	2	2	1,5	5,5	7,5	-2	4
x2	1	1	1,5	3,5		-4	16
x3	3	4	4	11		3,5	12,25
x4	4	3	3	10		2,5	6,25
Σ	10	10	10	30		S=38,5	

Δ вычисляется по формуле (1):

$$\Delta = \sum_{j=0}^{m} x_{ij} - \frac{\sum_{i=0}^{n}\sum_{=0}^{m} x_{ij}}{n}, \qquad (1)$$

Проверка правильности составления матрицы на основе исчисления контрольной суммы производится с использование формулы (2):

$$\sum_{i=0}^{n} \boldsymbol{x_{ij}} = \frac{(\mathbf{1}+\boldsymbol{n})\text{Ч}\boldsymbol{n}}{\mathbf{2}}, \qquad (2)$$

$$\sum_{i=0}^{n} x_{ij} = \frac{(1+4)4}{2} = 10$$

Сумма по столбцам матрицам равны между собой и контрольной суммой (10), матрица составлена верно.

Далее проводится анализ значимости критериев отбора поставщиков (таблица 4):

Таблица 4 - Расположение критериев по значимости

Критерии	x2	x1	x4	x3
Сумма рангов	3,5	5,5	10	11

На следующем этапе оценивается степень согласованности мнений всех экспертов с использованием коэффициента конкордации Кендела.

Коэффициент конкордации принимает значения от 0 до 1. Причем он равен 1 при максимальной согласованности и равен 0 при максимальной несогласованности. При значениях W от 0,30-0,70 уровень согласованности считают удовлетворительным, а при значениях более 0,7 высокая, если коэффициент менее 0,3 то степень согласованности не удовлетворительная.

Формула коэффициента конкордации, для случая, когда имеются связанные ранги (3)[2]:

$$\boldsymbol{W} = \frac{\mathbf{S}}{\frac{\mathbf{1}}{\mathbf{12}}\mathbf{m^2}(\mathbf{n^3}-\mathbf{n}) - \mathbf{m}\sum_{\mathbf{j=0}}^{\mathbf{m}}\mathbf{T_i}}, \qquad (3)$$

где $T_i = \frac{1}{12}\sum_{i=0}^{L_i}(t_l^3 - t_l)$, L_i число (видов повторяющихся элементов) в оценках i-го эксперта, t_l-количество элементов в l-ой связке для i-го эксперта (количество повторяющихся элементов).

S=38,5 (табл. 3), n=4 (количество критериев), m=3 (количество экспертов),

$T_3 = \frac{1}{12}\text{Ч}(2^3 - 2) = 0{,}5$(в оценках 3-го эксперта одна связка, повторяется ранг «1,5» 2раза).

Если нет связанных рангов, то T_i равно 0. Тогда:

$$\sum_{i=0}^{m} T_i = 0{,}5$$

Коэффициент конкордации Кендела равен:

$$W = \frac{38{,}5}{\frac{1}{12}Ч3^2Ч(4^3 - 4) - 3Ч0{,}5} = 0{,}89$$

W=0,89 говорит о наличии высокой степени согласованности мнений экспертов.

Следующим этапом оценивается значимость коэффициента конкордации, для этой цели используется критерий согласия Пирсона (хи-квадрат).

Значение χ^2 вычисляется по формуле (5):

$$\chi^2 = \frac{\mathbf{S}}{\frac{\mathbf{1}}{\mathbf{12}}\mathbf{mn(n+1)} + \frac{\mathbf{1}}{\mathbf{n-1}}\sum_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{T_i}}, \quad (5)$$

В нашем случае значение χ^2 равно:

$$\chi^2 = \frac{38{,}5}{\frac{1}{12}Ч3Ч4(4+1) - \frac{1}{4-1}Ч0{,}5} = 7{,}9$$

Вычисленный χ^2 =7,9 сравнивается с табличным значением для числа степеней свободы (К=n-1=4-1=3) и при заданном уровне значимости (α=0,05).

Так как χ^2 расчетный 7,9 > χ^2 табличного = 7,81473, то W=0,89-величина не случайная, а потому полученные результаты имеют смысл и могут использоваться в дальнейшей работе.

Следующий этап - подготовка решения экспертной комиссии. На основе получения суммы рангов можно вычислить показатели весомости рассмотренных параметров. Матрица опроса преобразуется в матрицу преобразованных рангов по формуле (6):

$$\mathbf{S_{ij}} = \mathbf{x_{max}} - \mathbf{x_{ij}}, \quad (6)$$

x_{max} = 4.

Результаты заносятся в таблицу:

Таблица 5 – Матрица преобразованных рангов

Эксперты / № п.п.	1	2	3	∑	Коэффициент весомости, ω	Обобщенный ранг
x1	2	2	3	7	≈0,368	2
x2	3	3	3	9	≈0,474	1
x3	1	0	0	1	≈0,0526	4
x4	0	1	1	2	≈0,105	3
∑				19	1	

Расчет показателей для оценки поставщика липких лент

Рассмотрим количественные критерии: Репутация фирмы поставщика; Цена продукции; Уровень поставки; Уровень обслуживания.

Рассматриваемые критерии имеют различные единицы измерения, требуется нормализация критериев, под которой понимается такая последовательность процедур, с помощью которой все критерии приводятся к единому, безразмерному масштабу измерения.

Для приведения к общему виду все значения используемые критерии должны быть обработаны. В соответствии с принципом квалиметрии, для каждого показателя определяется эталонное значение, максимальное или минимальное, в зависимости от влияния показателей на общую оценку.

Нормализованный коэффициент вычисляется по формулам (7, 8):

$$в_{ij} = \frac{a_{ij}}{a_j^+}(7) в_{ij} = \frac{a_i^-}{aij}\ , \quad (8)$$

Гдеa_j^+ (a_j^-) −максимальное (минимальное) значение рассматриваемого критерия; a_{ij}- локальный критерий.

В последующем, для удобства поставщики будут пронумерованы следующим образом:

1. «Нова Ролл»
2. «МПК СД»
3.Торговый дом «Технолента»

Таблица 6 – Расчет нормализованного коэффициента «Репутация поставщика»

	№ п-ка	Локальный критерий a_{ij}, год	a_i^+	Нормализованный коэффициент
Опыт на рынке	1	22	22	1
	2	10		0,45
	3	1		0,045

Таблица 7 – Расчет нормализованного коэффициента «Цена продукции»

	№ п-ка	Локальный критерий a_{ij}, тыс. руб.	a_i^-	Нормализованный коэффициент
Цена на рынке	1	30	28	0,93
	2	28		1
	3	40		0,7

Таблица 8 – Расчет нормализованного коэффициента «Уровень поставки»

	№ п-ка	Локальный критерий a_{ij}, дней	a_i^-	Нормализованный коэффициент
Срок поставок партии	1	5	5	1
	2	7		0,71
	3	10		0,5

Таблица 9 – Расчет нормализованного коэффициента «Уровень обслуживания»

	№ п-ка	Локальный критерий a_{ij}, дней	a_i^-	Нормализованный коэффициент
Скорость оформления заказа	1	1	1	1
	2	1		1
	3	2		0,5

Рассмотрим релейный критерий – «Качество продукции» (наличие сертификата соответствия).

Таблица 10 – «Критерий «Качество продукции»»

	№ поставщика	Коэффициент
Наличие сертификата соответствия	1	Да
	2	Да
	3	Да

Далее все рассчитанные данные заносятся в общую таблицу для дальнейшего анализа и выбора поставщика (таблица 11):

Таблица 11 - Показатели для оценки и выбора поставщика

№ п.п	Критерий	№ поставщика			Коэффициент весомости, ω
		1	2	3	
1	Репутация фирмы поставщика	1	0,45	0,045	≈0,368
2	Цена продукции	0,93	1	0,7	≈0,474
3	Уровень поставки	1	0,71	0,5	≈0,0526
4	Уровень обслуживания	1	1	0,5	≈0,105
5	Качество продукции	да	да	да	

Далее все данные заносятся в таблицу с учетом весовых коэффициентов и суммируются (таблица 12):

Таблица 12 – Выбор поставщика

№ п.п.	Критерий	№ поставщика		
		1	2	3
1	Репутация фирмы поставщика	0,368	0,166	0,017
2	Цена продукции	0,441	0,474	0,332
3	Уровень поставки	0,053	0,037	0,026
4	Уровень обслуживания	0,105	0,105	0,053
5	Качество продукции	да	да	да
	Σ	**0,967**	0,782	0,428

Согласно произведенному расчету наилучшим поставщиком липкой ленты является Поставщик №1, а именно компания «Нова Ролл».

В настоящее время существует множество потенциальных поставщиков требуемых ресурсов, поэтому необходимо выбрать те из них, которые могли бы с наибольшим эффектом обеспечить успешную деятельность предприятия.

Литература

1. Анцев В. Ю., Игнатенко Е. Ю., Пасько Н. И.Журнал Известия Тульского государственного университета. Технические науки, Выпуск № 1 / 2012
2. Конкордация Кендела machinelearning.ru/ (Дата обращения: 10.03.2016)
3. Понятие, цели и задачи логистики do.gendocs.ru/ (Дата обращения: 03.03.2016)

ЗАОЧНОЕ ОБУЧЕНИЕ В ТЕХНОЛОГИЧЕСКОМ УНИВЕРСИТЕТЕ

Чернышёва Ольга Александровна, магистрант 1 курса кафедры Управления Качеством и стандартизации
Научный руководитель: **Асташева Надежда Павловна**, д.б.н., профессор кафедры Управления качеством и стандартизации

В работе рассмотрены проблемы заочного обучения в Технологическом Университете. Проанализирована динамика численности студентов в стране и бакалавров заочного факультета университета. Подчеркнуто, что в основе заочного образования лежит принцип совмещения обучения и работы, который дает студентам возможность соотносить теорию с практикой, дополняя одно другим. Выявлены основные противоречия системы заочного обучения в Технологическом университете.

Высшее образование, очно-заочное обучение, подготовка специалистов, инновационные методы.

DISTANCE LEARNING AT UNIVERSITY OF TECHNOLOGY

Chernysheva Olga, 1 undergraduate course of the Department of quality management and standardization
Scientific adviser: **Astasheva Nadezhda**, Doctor of Biological Sciences, Professor of the Department of quality management and standardization

The research considers the problems of distance learning at the Technological University. It analyses dynamics of the number of students in the country and bachelors of the correspondence department of the University. It defined the basis of correspondence education is the principle of combining training and work. It gives students the opportunity to correlate theory and practice complementing each other. Also the main contradictions of distance learning system at the Technological University are identified.

Higher education, part-time training, training, innovative methods.

Стремительное развитие жизни предопределяет подготовку специалистов, имеющих высшее образование. Вопрос качества обучения студентов заочного отделения поднимался во многих работах, посвященных современному образованию. Ряд исследователей обращают внимание на особенности, которые имеет заочное обучение. Данная система ориентирована на выполнение важных социальных задач общества: осуществление социальной справедливости, возможность получения знаний, профессиональному, личностному и культурному росту.

Обучение — это целенаправленный процесс формирования и развития у людей знаний, навыков и умений с учетом требований современной жизни и деятельности. Обучение обеспечивает преемственность поколений, полноценное функционирование общества и соответствующий уровень развития личности. Считается, что обучение это процесс, а образование - итог, результат. Главными механизмами освоения содержания в процессе обучения является целенаправленно организованная в специальных формах взаимодействия совместная деятельность студентов и преподавателей, их содержательное познавательное общение [1].

Заочная форма обучения была открыта первоначально как одна из дополнительных форм образования с целью обеспечения гарантии социального равенства прав на образование различных слоев общества. Постепенно заочная форма при своем развитии приобрела статус равноправный стационарной и сформировалась как самостоятельная образовательная система. Именно благодаря заочной форме обучения, после второй мировой войны наша страна смогла осуществить массовую подготовку специалистов с высшим образованием и выйти на лидирующие позиции в мире. Заочное обучение при соответствующих условиях может обеспечить доступность качественного высшего образования широким слоям населения независимо от места проживания и условий работы, гибко реагировать на запросы рынка труда, полнее использовать педагогический, научный, кадровый потенциал вузов, экономить финансовые средства [2].

Система заочного обучения ориентирована на широкий круг людей, поскольку позволяет им получать высшее образование, не отрываясь от работы.

В Технологическом университете действует особый механизм очно-заочного обучения, который позволяет получать знания в короткие сроки. Студентам предоставляется возможность обучаться один раз в неделю в выходной без отрыва от производства. Учебными планами предусмотрены лекционные и практические занятия, после которых студенту необходимо сдать зачет или экзамен.

В динамике количества студентов в РФ всех форм обучения наблюдается снижение количества студентов всех форм обучения. Так, если в 2010-11 учебном году было 5 849 000 студентов, из них 900 000 заочного обучения и 237 000 очно-заочного, то к 2014-2015 году общая численность студентов снизилась на 1 млн. до 4 406 000 человек, из них 649 000 студентов заочного и 130 000 очно-заочного обучения (таблица 1).

В то же время конкурс в высшие учебные заведения в период с 2000 по 2014 годы вырос в 2,5 раза, а в профессиональные образовательные учреждения практически не изменился, что отрицательно сказывается на подготовке различных кадров в стране.

В основе заочного образования лежит принцип совмещения обучения и работы, который:

- обеспечивает востребованность такой формы обучения в современных условиях

Таблица 1 - Динамика количества студентов в Российской Федерации

Показатели	Годы набора студентов				
	2010/11	2011/12	2012/13	2013/14	2014/15
Число государственных и муниципальных образовательных организаций	653	634	609	578	548
Численность студентов в государственных и муниципальных образовательных организациях, тыс. человек	5849	5454	5145	4762	4406
из них обучалось на отделениях:					
очных	4712	4444	4233	3895	3627
заочных	900	803	733	715	649
очно-заочных	237	207	179	152	130
Численность студентов государственных и муниципальных образовательных организаций на 10 000 человек населения	409	381	359	331	301

- дает студентам возможность соотносить теорию с практикой, дополняя одно другим
- позволяет студентам приобрести в период обучения профессиональный опыт, повышая свою конкурентоспособность на рынке труда
- в целом способствует успешной профессиональной интеграции обучающихся в производство и бизнес в кризисный период [3].

Специфика заочного обучения предопределяет и его особенности, которые заключаются в следующем:

1. Основной отличительной чертой заочного образования является более продолжительный срок обучения.

2. Получение образования без отрыва от производства.

3. Возможности очно-заочной формы обучения (один раз в неделю по выходным).

4. Возрастной состав студентов. Так, на очном обучении большую часть составляют студенты, которые начали свое обучение сразу после получения среднего образования. В то время как на факультете заочного обучения в большинстве обучаются студенты старше 25 лет, которые уже работают по своей специальности

В настоящий момент студентам заочного факультета Технологического университета предлагается обучение в течение одного учебного дня в выходной с проведением одной и той же дисциплины в первую и вторую половину дня. В то время как раннее

в выходной у групп были два занятия, одна дисциплина утром, вторая – после обеда. Считается, что при новом графике студенты будут сконцентрированы на определенном материале и быстрее подготовятся к зачету или экзамену. Однако существуют проблемы, которые постепенно проявляются в выступлениях студентов, которые считают, что времени на подготовку к экзамену, а тем более на написание курсовых не достаточно. Организация обучения и контроль знаний студентов заочной формы обучения представлена на рисунке 1 .

Заочное обучение имеет определенную специфику по сравнению с другими формами обучения, например периодичный характер. Учащийся готовится по переданным ему материалам сам, потом посещает курс лекций, которые читаются в течение одной-двух недель. Кульминацией занятий для студента-заочника является экзамен. Тогда как итоговая оценка в очном обучении может складываться как из суммы текущих отметок и экзаменационного балла, так и состоять только из оценки, полученной на экзамене. В случае с заочным обучением важнее всего то, как студент проявит себя на экзамене, ведь он готовился к нему в течение нескольких недель в основном самостоятельно, выполняя контрольные или курсовые работы и консультируясь с педагогами [4].

На качество заочного обучения влияют:

- уровень предыдущего образования студентов;
- заинтересованность студентов в получении знаний;
- индивидуальные особенности студентов;
- время, отводимое на подготовку к занятиям;
- оснащенность аудиторий;
- профессиональная подготовка преподавателя;
- материально-техническое обеспечение.

Следует отметить, что с переходом к Болонской системе, в заочном обучении Технологического университета произошли следующие изменения:

- изменились сроки освоения образовательной программы;
- прекращена подготовка специалистов многих направлений;
- прекращена подготовка специалистов и по сокращенной форме обучения, для студентов ранее закончивших колледж.
- основным направлением подготовки заочного обучения является бакалавриат.

Рисунок 1 - Организация обучения и контроль знаний студентов заочной формы обучения

В Технологическом Университете на факультете заочного обучения функционирует большое количество направлений подготовки. Количество групп полного обучения выросло с 49 до 56 за период 2011-2015 г.г, одновременно происходило значительное снижение сокращенного и второго высшего обучения (таблица 2).

Таблица 2 - Динамика численности студентов заочного отделения Технологического университета

Учебный период	Полная форма обучения	Количество студентов факультета ФЗО	
		абсолютное	%
2011-2012	49	1289	100
2012-2013	50	1041	80
2013-2014	49	933	72
2014-2015	52	851	66
2015-2016	56	863	67

Необходимо отметить ряд причин, по которым наблюдается данная тенденция:

1. В связи с прекращением обучения планомерно снижается количество групп сокращенного и второго высшего обучения.

2. Значительное увеличение количества групп полной формы обучения к 2015-2016 учебному году при одновременном снижении численности студентов до 67% по сравнению с 2011/12 годом.

Тенденция увеличения количества групп, вероятно, связана с открытием новых направлений подготовки на ФЗО:

-54.03.01 «Дизайн»

-24.05.01 «Проектирование, производство и эксплуатация ракет и ракетно-космических комплексов»

-38.05.02 «Таможенное дело»

На фоне увеличения количества групп полного обучения наблюдается снижение численности студентов ФЗО до 66-67% по отношению к 2011 учебному году. На этот процесс помимо отмены с 2014 года приема студентов на сокращенные формы обучения и второе высшее, переход обучения от специалитета к бакалавриату, влияет финансовый кризис и несовершенство организации и технологий обучения.

Численность студентов в различных группах при приеме и в конце обучения также изменяется. Для более детального изучения, была рассмотрены динамика численности ряда групп, которые поступили в 2011 году и в 2016 учебном году заканчивают обучение по разным направлениям подготовки бакалавров [5].

В таблице 3 показано, как количество студентов в различных группах 2011 года набора сокращалось на протяжении времени обучения. В ряде групп снижение достигло 56-63 %. В среднем снижение количество студентов достигает 46%, это значит, что университет заканчивает примерно половина поступивших на первый курс.

Таблица 3 - Динамика численности студентов в различных группах ФЗО

Группа	Годы обучения					% снижения
	2011	2012	2013	2014	2015	
УЗ-11	10	11	7	7	7	30
ЭБЗ-11	12	10	10	12	11	9
МЗ-11	16	15	11	7	7	56
ГЗ-11	19	17	12	9	7	63
ИБЗ-11	12	11	7	5	5	58

Технологический Университет осуществляет обучение не только граждан России, но и граждан других стран. По классической форме заочного обучения в университете обучаются 289 студентов из Туркменистана.

В настоящий момент численность студентов на факультете очно-заочного обучения составляет 863 человек, из них 41 студент имеют иностранное гражданство. На первом месте Узбекистан 12 человек, далее Украина 11 чел и Армения 6 чел. (таблица 4).

Таблица 4 - Контингент студентов заочной формы обучения

Страна	Количество студентов ФЗО 2015/16
Россия	832
Армения	6
Белоруссия	1
Грузия	2
Киргизия	1
Молдова	4
Таджикистан	4
Узбекистан	12
Украина	11
В том числе: студенты факультета по работе с иностранными студентами	
Туркменистан	289

Таким образом, в результате исследования выявлены основные противоречия системы заочного обучения в Технологическом университете:

- возрастающий спрос на заочное обучение в вузах и низкое количество выпускаемых студентов, свидетельствующее о необходимости совершенствования форм обучения;

- растущими потребностями современного регионального рынка труда и наличием безработных выпускников вузов;

- растущим объемом необходимого для изучения материала и инертностью в совершенствовании и создании пособий для самостоятельного обучения, их отсутствием по специализированным дисциплинам;

- потребностью во внедрении электронных УМК и недостаточным количеством педагогических кадров, обладающих ИКТ - компетентностью для его создания и внедрения в систему заочного обучения.

Литература

1. Асташева Н.П., Аверин В.С. Электронный учебно-методический комплекс дисциплины "Охрана труда" [Текст] / сборник трудов по материалам II Международной научно-практической Интернет-конференции 19 декабря 2014 г.: Королёв МО: Изд-во «Алькор Паблишерс», ФТА, 2015. - 456 с.

2. Вержбицкий В.В. Дистанционное обучение в странах СНГ: мониторинг образовательных потребностей и возможностей.

Аналитический обзор / В.В. Вержбицкий, Ю.Ю. Власова. М.: Институт ЮНЕСКО по информационным технологиям в образовании, 2003. - 74 с.
3. Донской А.Д., Сабо С.Е., Штрафина Е.Д. Дистанционные образовательные методики в дополнительном образовании с использованием современных электронных образовательных ресурсов. I Международная научно-практическая интернет-конференция «Современные образовательные технологии, используемые в очном, заочном и дополнительном образовании» 20.12.2013
4. Исаев В.Г. Нормативные документы контроля качества различных форм образовательной деятельности. «Каржы»-«Финансы» №2-3(2). Февраль-Март 2014г.
5. Строителев В.Н., Жидкова Е.А. Инновационные подходы в обучении студентов ВУЗОВ // Вопросы региональной экономики. - 2011.

ФИНАНСОВО-ЭКОНОМИЧЕСКИЙ ФАКУЛЬТЕТ

КАФЕДРА ФИНАНСОВ И БУХГАЛТЕРСКОГО УЧЕТА

ОСНОВЫ УПРАВЛЕНИЯ ОБЩЕСТВЕННЫМИ ФИНАНСАМИ

Акиндинова Наталья Вадимовна, студентка 3 курса кафедры Финансов и бухгалтерского учета
Научный руководитель: **Самошкина Марина Викторовна**, к.э.н., доцент кафедры Финансов и бухгалтерского учета

Статья посвящена эффективному и ответственному управлению государственными финансами, которое имеет фундаментальное значение для всех стран с точки зрения обеспечения устойчивости бюджетных систем, а также с точки зрения общей финансовой безопасности и устойчивого экономического роста. Целью данной статьи является исследование общих закономерностей и особенностей управления общественными финансами, а также выявление проблем и рассмотрение решений этих проблем.

Общественные финансы, государственный сектор, управление общественными финансами.

PUBLIC FINANCE MANAGEMENT BASICS

Akindinova Natalia, 3rd year student of the Department of finance and accounting
Scientific adviser: **Samoshkina Marina**, Candidate of Economic Sciences, Associate Professor of the Department of finance and accounting

Effective and accountable public financial management is of fundamental importance for all countries in terms of the sustainability of budget systems, as well as in terms of overall financial security and sustainable economic growth. The purpose of this article is the study of general regularities and features of public finance management, as well as identifying problems and considering solutions to these problems.

Public finance, public sector, public finance management.

Под общественным сектором экономики страны, как правило, понимают государственный сектор, представляющий и обслуживающий интересы всего населения.

Финансы общественного сектора экономики выступают как отношения, связанные с формированием и использованием фондов денежных средств государства, муниципальных образований и некоммерческих организаций [1].

Финансы общественного сектора экономики Российской Федерации включают в себя:

- государственные финансы, к которым, в свою очередь, относятся: федеральный бюджет; государственный кредит; государственные бюджетные и внебюджетные фонды; бюджеты республик, краев, областей, находящихся в составе Российской Федерации; региональные отделения государственных внебюджетных фондов, а также внебюджетные фонды, создаваемые региональными органами власти;
- муниципальные финансы, а именно: бюджеты городских округов, внутригородских муниципальных образований городов федерального значения, городских и сельских поселений; внебюджетные фонды, создаваемые муниципальными органами;
- финансы государственных и муниципальных унитарных предприятий, государственных корпораций и иных подконтрольных органам власти предприятий и организаций;
- финансы некоммерческих организаций [3].

Все указанные элементы объединяет задача обеспечения предоставления социальных благ.

Выбранная тема является актуальной, так как на сегодняшний день качественное управление общественных финансов, а также рациональное их использование и распределение бюджетных средств представляет собой огромный интерес в развитии страны.

Система управления финансами – это комплекс мер, инструментов, финансовых институтов, обеспечивающих стабильное и эффективное функционирование финансовой системы в целом и ее отдельных звеньев, способствующих развитию социально-экономических процессов в обществе.

Система управления финансами, являясь сложным образованием, состоит из таких относительно самостоятельных, но тесно взаимодействующих блоков, как финансовое планирование, прогнозирование, программирование, финансовое регулирование, финансовый контроль, комплекс правового обеспечения финансовой деятельности, система методов мобилизации финансовых ресурсов.

Конкретные цели – сбалансированность бюджета, оптимизация государственного долга, устойчивость национальной валюты, гармонизация экономических интересов государства и его граждан.

В управлении государственными финансами принимают участие высшие органы власти страны, и организовано оно следующим образом.

Президент РФ регламентирует деятельность финансовой системы, устанавливая основные параметры бюджета в ежегодном бюджетном послании, подписывает Федеральный закон о федеральном бюджете на предстоящий год и т.д.

Правительство РФ является единым центром управления финансами. Органом, на практике осуществляющим реализацию финансовой политики, является Минфин РФ. Министерство обеспечивает единство финансовой, денежно-кредитной и валютной политики, координирует финансовую деятельность федеральных органов исполнительной власти. Счетная палата РФ осуществляет парламентский контроль за федеральными денежными средствами. Она независима от Правительства РФ и подотчетна лишь Федеральному Собранию.

Федеральное Собрание вводит налоги, сборы, неналоговые платежи, утверждает федеральный бюджет, принимает законы, регламентирующие финансовую деятельность государства.

Федеральное агентство по управлению федеральным имуществом управляет государственным имуществом с целью получения доходов неналогового характера (арендная плата, доходы от продажи государственного имущества).

Федеральная служба по финансовым рынкам контролирует деятельность участников фондового рынка, способствуя тем самым увеличению поступлений в бюджетный фонд.

Федеральная налоговая служба и МВД осуществляют контроль за правильностью исчисления, полнотой и своевременностью внесения в бюджетные фонды налогов, сборов и других платежей.

Центральный банк РФ – важный орган реализации денежно-кредитной и финансовой политики. ЦБ РФ наряду с Федеральным казначейством осуществляет кассовое исполнение бюджета, контролирует деятельность кредитных организаций.

В субъектах РФ, их административно-территориальных и муниципальных образованиях финансовую политику проводят соответствующие финансовые учреждения.

Важным элементом бюджетного процесса является государственный и муниципальный финансовый контроль, который

обеспечивает эффективность функционирования государственной финансовой системы.

Основное назначение финансового контроля состоит в том, чтобы обеспечить эффективность процесса формирования и расходования денежных средств, находящихся в руках государства. Контроль является неотъемлемым элементом процесса государственного управления. Он способствует успешной реализации задач, стоящих перед бюджетной системой страны.

Объектом финансового контроля является бюджетная система и бюджетный процесс.

Большую роль в развитии экономики страны играет государственные и муниципальные кредиты. И к основным целям государственного и муниципального кредита относятся:

-решение проблем финансирования бюджетного дефицита;

-проведение региональной финансово-кредитной политики, направленной на выравнивание социально-экономических условий жизни населения и функционирование региональных экономик;

-поддержка муниципальных образований в решении неотложных социально-экономических задач;

-поддержка приоритетных для экономики секторов и видов деятельности.

Как известно, заимствование денег ведет к образованию внутренней и внешней задолженности.

В управление общественных финансов также входит управление государственным и муниципальным долгом.

Управление государственным долгом – это деятельность государства в качестве заемщика, кредитора и гаранта, включающая в себя централизованные действия по подготовке, выпуску и размещению долговых обязательств, регулированию рынка ценных бумаг, своевременному обслуживанию и погашению долга, предоставлению гарантий.

Управление долгом включает в себя три составляющие – мониторинг и прогнозирование долга, формирование благоприятного имиджа заемщика, операции по управлению долгом. Задача мониторинга возложена на Минфин РФ. Прогнозирование долга связано с оценкой вероятного размера обязательств и вероятного исполнения по ним. Формирование благоприятного имиджа включает в себя: сохранение хорошей кредитной истории, получение

кредитного рейтинга и обеспечение информационной прозрачности долговой и бюджетной политики [4].

Таблица 1 - Показатели задолженности России с 2010 по 2015 гг.

Показатель	Год					
	2010	2011	2012	2013	2014	2015
Государственный долг РФ, % ВВП	9,3	9,8	11,9	13,1	13,7	13,4
Доля государственного внутреннего долга в общем объеме госдолга РФ, %	70,7	78,4	75,1	75,5	74,9	74,6

Однако до сих пор ряд недостатков и нерешенных проблем сохраняется в сфере управления государственными финансами.

- законодательно не определен статус органов государственного финансового контроля Российской Федерации и ее регионов, место и роль каждого субъекта государственного финансового контроля в его целостной системе;
- органы контроля слабо взаимодействуют между собой, присутствует некоторая разобщенность в приоритетах деятельности контрольных органов;
- «отсутствие определения государственного финансового контроля в бюджетном законодательстве, национальных и федеральных стандартов контроля, не существует четкой и полной нормативно-правовой базы регулирования ГФК, и собственно, нет единого федерального закона о системе финансового контроля;
- организационная структура органов государственного финансового контроля недостаточно отражает специфику государственного устройства Российской Федерации;
- отсутствует единая информационная база, единый методологический подход к процессу осуществления контроля;
- отсутствует четкое разграничение сфер деятельности, что вызывает перекладывание ответственности. кроме того, действия органов финконтроля не скоординированы.
- отсутствуют общегосударственные принципы планирования контрольной работы, классификация финансовых нарушений [3].

Все вышеперечисленные проблемы, несомненно, влияют на качество управления государственными финансами.

В настоящее время работа органов государственного финансового контроля в России характеризуется несогласованностью

и разобщенностью, отсутствием четкого взаимодействия. И связано это, в первую очередь, с несформированностью целостной системы контроля за государственными финансами. Сейчас финансовый контроль - это, скорее, набор госорганов, ведомств и служб, выполняющих определенные контрольные функции. Более 260 законов, указов, постановлений регулируют их контрольную деятельность, что не только не облегчает взаимоотношения между ними, но зачастую вносит элементы хаоса и дезорганизации». Статус и полномочия контрольных органов определяются многочисленными правовыми актами, зачастую допускающими дублирование и параллелизм при выполнении некоторых функций.

Для того чтобы разрешить сложившиеся проблемы, необходимо систематизировать предложенные решения:

1. Так как существуют условия для увеличения бюджетных расходов, которые превышают доходы, то необходимо мотивировать органы государственной власти разных уровней в области повышения эффективности расходования средств и стимулировать к рациональному использованию федеральных бюджетных средств. Для получения более эффективного бюджета нужно, чтобы поставленные цели и задачи соответствовали средне- и долгосрочным целям социально-экономического развития, что позволит увеличить эффективность расходования средств.

2. Для борьбы с коррупцией, что представляется очень серьезным явлением в бюджетной сфере, необходимы крайне эффективные методы борьбы, такие как проведение расследований судебной системой и привлечению к ответственности с использованием необходимых санкций для нарушителя;

3. Построение эффективной системы ГФК проходит медленными темпами. В данной области существует ряд проблем, решение которых возможно только благодаря качественно разработанной и принятой концепции, в которой должны быть явно прописаны все цели и задачи ГФК, требования и стандарты ГФК, полномочия и функции контрольных органов и т.д.

4. В связи с множественностью различных контролирующих служб и органов, которые выполняют одинаковые работы, появляется дублирование и параллелизм их полномочий. Для того, чтобы органы в полной мере проявляли свои возможности, необходимо ограничения учреждений сузить до минимального уровня или разумно обосновывать уже поставленные определенные ограничения.

Цель управления финансами – это финансовая устойчивость, которая проявляется в макроэкономическом балансе, в балансе между профицитом и дефицитом бюджета, а также в снижении государственного долга с целью социально-экономического развития и исполнения всех функций государства в сочетании с интересами всех членов общества.

Построение системы управления государственными финансами невозможно без преодоления многочисленных препятствий, которые помогают эффективно развиваться финансовой системы России.

Литература

1. Государственные и муниципальные финансы: Учебник / И.Н. Мысляева. - 3-е изд., перераб. и доп. - М.: НИЦ ИНФРА-М, 2014. - 393 с.
2. Финансовый контроль в России / Васильева М. А., Корчагина А. С. / Статья публикуется в рамках Международной заочной научно-практической конференции студентов, аспирантов и молодых ученых «Молодые ученые о современном финансовом рынке РФ», 28 апреля, 2011 г., Пермь.
3. Финансы: Учебник. / Под ред. А.Г. Грязнова, Е.В. Маркина, М.Л. Седова. — М.: Финансы и статистика, 2012. — 496 с.
4. Финансы: Учебник. — 2 е изд. / Миляков Н.В. — М.: ИНФРА М, 2004. — 543 с. — (Высшее образование).
5. Экономика и финансы общественного сектора: Учебник. / Пономаренко Е.В. — М.: ИНФРА-М, 2013. — 377 с.
6. Экономика общественного сектора: Учебник. – 2-е изд., доп. и перераб. / Под ред. П.В. Савченко, И.А. Погосова, Е.Н. Жильцова. — М.: ИНФРА-М, 2015. — 556 с.

ФИНАНСОВЫЕ ПРАВОНАРУШЕНИЯ В БЮДЖЕТНОЙ СФЕРЕ: ОСОБЕННОСТИ, СПОСОБЫ РЕШЕНИЯ ПРОБЛЕМЫ

Воробин Алексей Валентинович, студент 3 курса кафедры Финансов и бухгалтерского учёта
Научный руководитель: **Салманова Ирина Павловна**, к.э.н., доцент кафедры Финансов и бухгалтерского учёта

Современное государство и его структурные единицы напрямую зависят от корректного и рационального распределения и перераспределения доходов на всех уровнях его бюджетной системы.

А сами доходы, полученные от бюджетов других уровней в виде финансовой помощи и бюджетных ссуд, являются для некоторых структурных единиц ключевыми. Как следствие, нарушения в процессе формирования бюджетов данных единиц, может повлечь за собой негативное влияния как для конкретно взятой области, так и для государства в целом. Так же немаловажным является факт воздействия на экономику России определённых санкционных запретов, а также положение дел на рынках экспортируемых Россией ресурсов, в первую очередь нефти и газа. Исходя из этого, рассмотрение вопросов укрепления финансовой дисциплины и правопорядка в финансово–бюджетной системе имеет исключительное значение.

Финансовые правонарушения, ужесточение системы наказания.

FINANCIAL OFFENSES IN THE PUBLIC SECTOR: CHARACTERISTICS, METHODS OF SOLVING PROBLEMS

Vorobin Alexei, 3rd year student of the Department of finance and accounting
Scientific adviser: **Salmanova Irina,** Candidate of Economic Sciences, Associate Professor of the Department of finance and accounting

Current countries and all of its structures are directly depending on a rational distribution of income at all levels of its budget system. All of income received from other budgets in a form of financial assistance or budgetary loans is a key factor for several structure units. As a result, disturbances in the formation of these unit's budgets can result in a negative impact for the individual state and country as a whole. Another important factor is a negative impact on Russia's economy created by sanctions, as well as the situation on the market of export, primarily it's oil and gas. Based on this, addressing issues of strengthening financial discipline and order in the fiscal system currently stands as priority.

Financial offenses, increase penalties system.

Ни для кого не будет секретом, что на данном этапе, благосостояние, как всего нашего государства, так и конкретно взятых его структурных единиц, напрямую зависят от корректного и рационального распределения, а также от перераспределения его доходов на всех уровнях бюджетной системы. Также не стоит

забывать, что для некоторых структурных единиц доходы, получаемые от бюджетов других уровней в виде финансовой помощи, по факту являются ключевыми. И как следствие, нарушения в процессе формирования, а ещё главнее в исполнении, данных бюджетов, может повлечь, и несомненно повлечёт в определённый момент времени, за собой негативное влияния как для конкретно взятой единицы, так и для государства в целом. Добавляя к вышесказанному воздействие на экономику России ряд определённых санкционных запретов, действующих на данный момент, а также не очень благоприятное положение дел на рынках традиционно экспортируемых Россией природных ресурсов. Можно сделать вывод об всё большей актуализации вопросов укрепления финансовой дисциплины и правопорядка в финансово–бюджетной системе.

Прежде чем перейти к рассмотрению уже вызванных данной проблемой негативных последствий, мне бы хотелось затронуть законодательную базу, действующую на данный момент непосредственно по отношению к финансово–бюджетной системе.

И как ни странно, на данный момент финансовое законодательство не содержит единого, комплексного понятия финансового правонарушения, но тем не менее закрепляет определения его разновидностей — налогового правонарушения и нарушения бюджетного законодательства.

Согласно ст. 106 НК РФ [1] налоговым правонарушением признается совершенное противоправное (в нарушение законодательства о налогах и сборах) деяние (действие или бездействие) налогоплательщика, налогового агента и их представителей, за которое НК РФ установлена ответственность.

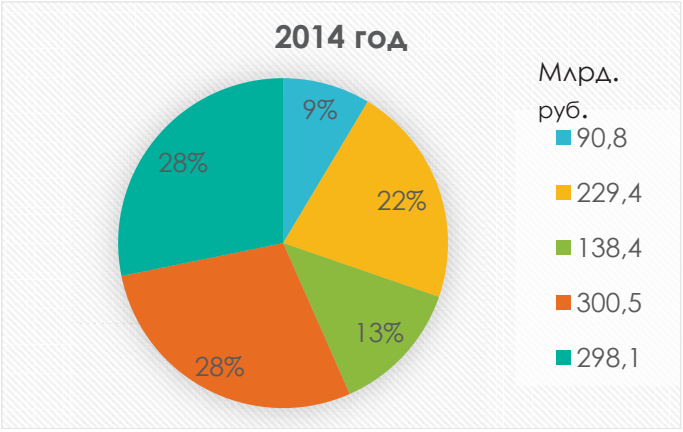
Статья 281 БК РФ [2] относит к нарушениям бюджетного законодательства неисполнение либо ненадлежащее исполнение установленного БК РФ порядка составления и рассмотрения проектов бюджетов, утверждения бюджетов, исполнения и контроля за исполнением бюджетов бюджетной системы Российской Федерации, которое влечет применение к нарушителю мер принуждения.

Исходя их этого, можно утверждать, что определение финансового правонарушения является обобщающей (собирательной) категорией, отражающей совокупность юридических признаков внутриотраслевых правонарушений. И как следствие, можно вывести определение «финансового правонарушения»:

Финансовое правонарушение — это совершенное противоправное (в нарушение финансового законодательства) деяние (действие или бездействие) субъекта финансового права, за которое финансовым законодательством установлена ответственность.

Говоря об ответственности, хочется упомянуть про меры принуждения, имеющие место быть против лица нарушившего бюджетное законодательство. А именно, к нарушителю бюджетного законодательства могут быть применены следующие меры:

1. Предупреждение о ненадлежащем исполнении бюджетного процесса;
2. Блокировка расходов;
3. Изъятие бюджетных средств;
4. Приостановление операций по счетам в кредитных организациях;
5. Наложение штрафа;
6. Начисление пени;
7. Иные меры, предусмотренные Кодексом и федеральными законами.



Неправомерное расходование бюджетных средств, в том числе нецелевое использование
Неэффективное использование бюджетных средств
Нарушения в сфере государственных закупок
Нарушения порядка ведения бухгалтерского (бюджетного) учета и отчетности
Другие нарушения, в том числе недопоступление платежей в бюджет, государственные внебюджетные фонды, расхождения фактического наличия бюджетных средств с данными бухгалтерского учета.

Рисунок 1 – Сравнительная диаграмма объёмов выявленных нарушений в 2014 году

Как видно, ключевой мерой принуждения, применяемой органами Федерального казначейства, является бесспорное списание бюджетных средств. За нарушения предусмотрено применение различных санкций: наложение штрафа; изъятие в бесспорном порядке бюджетных средств, используемых не по целевому назначению, а также при наличии состава преступления – уголовное наказание в соответствии с УК РФ.

Второй год подряд объем выявленных Федеральной службой финансово-бюджетного надзора нарушений превышает 1 трлн. рублей.

Как видно (рис.1), в 2014 году общий объем выявленных нарушений, составил 1 057,2 млрд. рублей нарушений [4].

Но несмотря на и без того крайне солидную сумму, объём выявленных правонарушений за 2015 год (рис.2), не только не уменьшился, но и наоборот подскочил до планки в 1542,7 млрд. рублей. Хочу отметить, что и доля наиболее серьёзных финансовых нарушений увеличилась почти в полтора раза [5].

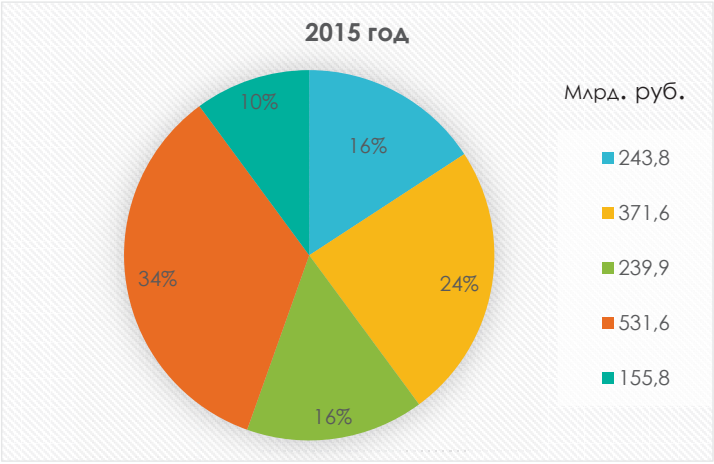


Рисунок 2 – Сравнительная диаграмма объёмов выявленных нарушений в 2015 году

Цифры вполне солидные и подобные недостачи, особенно в текущей геополитической ситуации, являются фактором, крайне пагубно влияющем на жизнь граждан в целом.

Возможными путями минимизации данных правонарушений могут стать:

- Комплексная доработка системы наказания, построенная на принципе неотвратимости ответственности за нарушения бюджетного законодательства.
- Развитие и корректировка аудита, для более открытой и «прозрачной» отчётности

Бесспорно, современные условия требуют усиления контроля за использованием средств бюджетов всех уровней, в связи с чем, все большее значение приобретает принцип неотвратимости ответственности за нарушения бюджетного законодательства.

На мой взгляд, система наказания за финансовые правонарушения всех видов (неправомерное расходование бюджетных средств; неэффективное использование бюджетных средств и т.д.) является крайне лояльной и малоэффективной. Приоритетной задачей при рассмотрении подобных правонарушений, является компенсация средств, виновным лицом. Для дальнейшего привлечения данного лица к ответственности, как правило, необходимо собрать внушительную базу, что, к сожалению, удается не слишком часто, особенно если речь идёт о высокопоставленных лицах. Также в результате этого, дело может «повиснуть» на долгое время. Тем самым постепенно откладываясь и снижая в приоритете новым, более актуальным проблемам.

Наряду с вышесказанным большой проблемой, с которой сталкиваются уже уполномоченные службы является фиктивные юридические лица или иначе – фирмы «однодневки». Т.е. организации с фиктивными признаками, как правило, отсутствуют по адресам гос. регистрации и задолго до применения к ним мер административного воздействия фактически прекращают свою деятельность. Соответственно, все мероприятия по взысканию штрафных санкций, как правило, заканчиваются ничем.

Ещё одним аспектом снижения подобных правонарушений может стать более открытая и «прозрачная» система отчётности, для чего необходимо совершенствовать аудиторскую деятельность. Например, закрепить право в ходе внешних проверок качества работы аудиторских организаций осуществлять встречные проверки,

направлять запросы аудируемым лицам относительно сведений и документов, относящихся к предмету проверки. А также установить административную ответственность за невыполнение требований о проведении обязательного аудита.

Литература

1. РФ ГД ФС Бюджетный кодекс российской федерации" от 31.07.1998 N 145-ФЗИ. - 31.07.1998 г.
2. РФ ГД ФС Налоговый кодекс российской федерации (часть первая)" от 31.07.1998 N 146-ФЗ. - 16.07.1998 г.
3. Соколова Е.Ю. Финансовое право [Текст] / Грачева Э.Д. // МОСКВА: Инфра-М, 2013. - стр. 352 стр.
4. Информационные материалы, характеризующие динамику работы службы по основным направлениям деятельности за период 2013-2015 ГОДОВ. Федеральная служба финансово-бюджетного надзора. Электронный ресурс. Режим доступа: http://www.rosfinnadzor.ru/documents/osnovnye-pokazateli-deyatelnosti/informatsionnye-materialy-kharakterizuyushchie-ym-napravleniyam-deya(дата обращения: 13.12.2015).
5. Доклад о результатах и основных направлениях деятельности службы в 2015 году. Федеральная служба финансово-бюджетного надзора. Электронный ресурс. Режим доступа: http://www.rosfinnadzor.ru/documents/osnovnye-pokazateli-deyatelnosti/doklad-ob-osnovnykh-napravleniyakh-deyatelnosti-sluzhby-v-2015-godu (дата обращения: 19.02.2016).

НОВАЦИИ И ПЕРСПЕКТИВЫ БЮДЖЕТНОГО ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ

Гаврилов Дмитрий Александрович, студент 4 курса кафедры Финансов и бухгалтерского учёта
Научный руководитель: **Таран Екатерина Михайловна,** к. пед.н., доцент кафедры Финансов и бухгалтерского учёта

Основной идеей предлагаемых новаций в области бюджетного законодательства является консолидация в единую систему принятых за последние годы федеральных законов, регулирующих бюджетные правоотношения, с целью принятия стабильного, системного и удобного для правоприменения кодифицированного акта. Параллельно возникает необходимость в своевременном приведении в соответствие с Бюджетным кодексом Российской

Федерации иных законов и нормативных правовых актов, регулирующих бюджетные правоотношения. Это позволит системно описать бюджетный процесс, реализовать комплексно отдельные новации, провести масштабную работу по юридико-техническому уточнению норм и обеспечить большую стабильность норм бюджетного законодательства.

Бюджетное законодательство, Бюджетный кодекс Российской Федерации, бюджетный процесс.

INNOVATIONS AND PERSPECTIVES OF THE RUSSIAN FEDERATION'S BUDGET LEGISLATION

Gavrilov Dmitry, 4th year student of the Department of finance and accounting
Scientific adviser: **Taran Ekaterina,** Candidate of Pedagogical Sciences, Associate Professor of the Department of finance and accounting

The main idea of the intended innovations in the field of budget legislation is to consolidate federal laws, which has been adopted within the last years and regulate budgetary legal relationships, into an unified system, in order to adopt a codified act which would be stable, systematic and convenient for law enforcement. At the same time, it is necessary to bring in time to conformity with the Budget Code of the Russian Federation and other laws and legislative instruments regulating budgetary legal relationships. This will make the systematic description of the budgeting process, integrated implementation of certain innovations, as well as tremendous work on more precise legal and technical definition of laws and regulations, and ensuring of big stability of statutory regulations to be possible.

Budget laws, Budget Code of the Russian Federation, budgeting process.

Среди множества новаций в сфере бюджетного законодательства основной следует считать разработку Министерством Финансов проекта новой редакции Бюджетного кодекса Российской Федерации. Работа над этим важнейшим документом продолжается, принимаются во внимание все замечания и предложения.

Работа по совершенствованию бюджетного законодательства проводится в соответствии с Программой повышения эффективности

управления общественными (государственными и муниципальными) финансами на период до 2018 года, утвержденной распоряжением Правительства Российской Федерации от 30 декабря 2013 года № 2593-р, и государственной программой Российской Федерации "Управление государственными финансами и регулирование финансовых рынков", утвержденной постановлением Правительства Российской Федерации от 15 апреля 2014 года № 320 (основное мероприятие 2.1 "Совершенствование бюджетного законодательства") [2].

С момента введения в действие Бюджетного кодекса Российской Федерации осуществлялось внесение многочисленных изменений в его положения (с 2000 года 109 федеральных законов, вносящих изменения или приостанавливающих действие отдельных положений, т.е. в среднем 8 законов в год), что не способствует его стабильности и системности применения.

Новая редакция Бюджетного кодекса Российской Федерации позволит:

1) системно описать бюджетный процесс и реализовать комплексно отдельные новации;

2) обеспечить большую стабильность норм бюджетного законодательства;

3) провести масштабную работу по юридико-техническому уточнению норм, в том числе в части исключения положений, утративших силу, пересчета структурных единиц, актуализации структуры Кодекса для приведения его в соответствие с современными требованиями, предъявляемыми к оформлению законодательных актов [2].

Изменения направлены на описание правовых основ бюджета и бюджетного процесса в такой форме, которая бы позволила достигать задачи государственной политики в области экономики и финансов с минимальными изменениями в Бюджетный кодекс Российской Федерации.

Следует отметить тот факт, что работа над новой редакцией Бюджетного кодекса шла в течение последних нескольких лет, и очень многие нововведения уже реализованы в поправках в БК РФ.

Предлагается изменить структуру Бюджетного кодекса, перегруппировать по-новому статьи, чтобы более чётко описать сущность бюджетного процесса, взаимодействие между бюджетами, бюджетное устройство и бюджетную систему. Кроме того,

появляется целый ряд новых глав, в том числе глава о регулировании эмиссии и обращения государственных (муниципальных) ценных бумаг, которая до сих пор регулировалась отдельным Федеральным законом. Таким образом, только сейчас кодекс становится по-настоящему кодифицированным законодательным актом, который охватывает всю сферу бюджетных правоотношений.

Предлагается уточнить ряд базовых терминов бюджетного законодательства.

Вместо термина «источник финансирования дефицита бюджета», вызывающего целый ряд вопросов, предлагается использовать более ясный и соответствующий международным стандартам термин «источник финансирования бюджета».

Термин «получатель бюджетных средств» предложено заменить тоже более понятным термином «администратор бюджетных расходов». А под получателем средств из бюджета следует понимать юридических лиц, которые получают субсидии из соответствующего бюджета, и, таким образом, тоже частично попадают под действие бюджетного законодательства.

Будет введён новый принцип бюджетной системы – принцип сбалансированности и устойчивости бюджетов. Предлагается законодательно закрепить целый ряд требований к бюджетной политике, чтобы бюджеты всех уровней были сбалансированы и устойчивы.

Продолжается дальнейшее развитие концепции расходных обязательств публично-правовых образований. Предлагается ввести новое понятие «Публичное обязательство». Вместе с тем сохраняется и понятие расходного обязательства, под которым понимается публичное обязательство, подлежащее отражению в расходах бюджета, поскольку имеются еще и публичные обязательства, связанные с исполнением долговых обязательств. Предлагается создать более стройную правовую основу для планирования расходов бюджета: сначала возникает публичное обязательство, потом расходное, затем оно трансформируется в бюджетное обязательство, денежное обязательство (рис. 1). Предлагаемая измененная концепция обязательств позволит закрепить основания для предоставления публично-правовыми образованиями средств из бюджета, а также классифицировать обязательства по основаниям их возникновения.

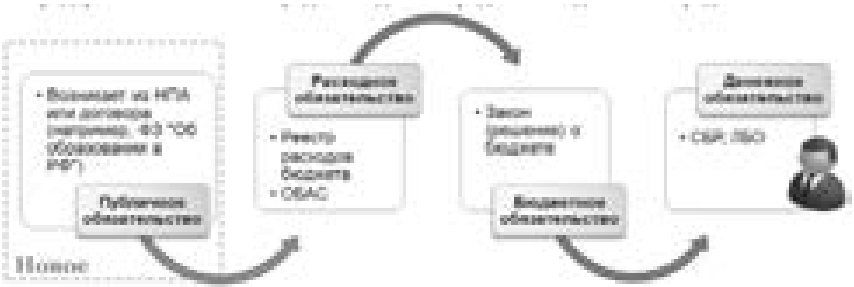


Рисунок 1 – Понятие «Публичное Обязательство»

Концепция расходных обязательств публично-правовых образований получит дальнейшее развитие. Предлагается закрепить, что обязательства публично-правового образования независимо от основания их возникновения являются публичными обязательствами, поскольку принимаются от имени соответственно Российской Федерации, субъекта Российской Федерации, муниципального образования.

При этом предусматривается разделение публичных обязательств на нормативно-правовые обязательства, возникающие в соответствии с законом, иным нормативным правовым актом и не требующие заключения договора (соглашения), и подтверждения в ежегодном бюджетном процессе, а также договорные обязательства, обусловленные договором (соглашением, контрактом), для которых, прежде чем их принять, нужно установить лимиты бюджетных обязательств.

Действующий механизм формирования расходов бюджетов сохраняется, согласно которому формирование расходов бюджетов осуществляется в соответствии с расходными обязательствами.

При этом согласно предлагаемым изменениям предусматривается возможность формирования расходов бюджета на основе проектного финансирования договорных обязательств. Данные изменения направлены на повышение эффективности расходов бюджета, а также привлечение внебюджетных инвестиций.

В рамках внедрения проектного финансирования договорных обязательств будет обеспечено:

1) проведение анализа и оценки вариантов реализации проекта;

2) выбор оптимального варианта финансового обеспечения проекта, наилучшего соотношения бюджетной поддержки и внебюджетного финансирования;

3) заключение договора (соглашения, контракта) о реализации

проекта, в том числе долгосрочного договора (соглашения, контракта) на срок, выходящий за пределы планового периода, но в пределах средств, предусмотренных государственными программами Российской Федерации.

При этом договор (соглашение, контракт) включает:

1) обязательства по достижению определенных целей, имеющих измеримые показатели финансово-экономической деятельности;

2) планы достижения установленных показателей (в том числе их промежуточных значений);

3) обязанность возврата средств в бюджет при недостижении указанных показателей.

Отмечается, что договор (соглашение, контракт) предполагает достижение конкретного результата за определенный срок, что определяет эффективность предоставления бюджетных средств.

Таким образом, отказ от использования принципов проектного финансирования требует дополнительного обоснования в порядке, установленном Правительством Российской Федерации.

Формирование расходов федерального бюджета на основе проектного финансирования позволит оценивать целесообразность бюджетной поддержки реализации проектов с точки зрения их влияния на экономический рост на этапе формирования федерального бюджета и более качественно управлять эффективностью такой поддержки.

В новой редакции Бюджетного кодекса не будет предлагаться существенных новаций в сфере межбюджетных отношений, поскольку эти вопросы уже были урегулированы в предыдущие годы. Тем не менее, вводится ряд точечных поправок, которые должны облегчить формирование и исполнение региональных и местных бюджетов. В частности, одна из существенных новаций – это требование к тому, чтобы распределение всех субсидий утверждалось законами (решениями) о бюджетах. Кроме того будет введена такая категория, как дотации на сбалансированность бюджетов.

В состав документов, которые будут представляться одновременно с проектами о бюджетах в законодательные представительные органы, будут включены основные направления долговой политики.

Одна из существенных новаций заключается в законодательном закреплении новой системы критериев долговой устойчивости субъектов Российской Федерации и муниципальных образований. К

уже известным двум параметрам добавляется третий. И их совокупность как раз и должна будет определять обоснованность долговой политики регионов и муниципалитетов (рис. 2).

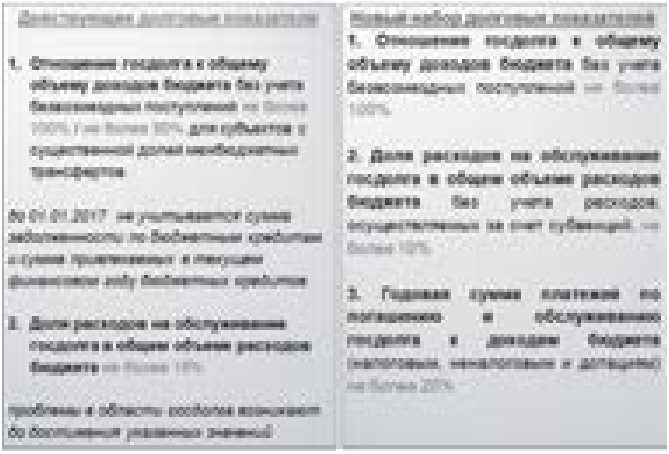


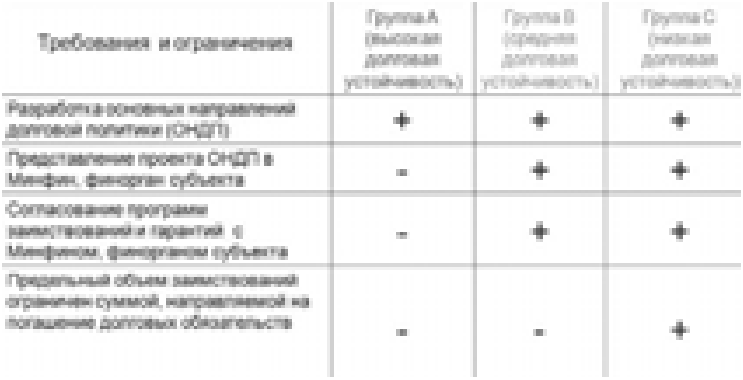
Рисунок 2 – Изменение состава долговых показателей субъектов Российской федерации и муниципальных образований

По значениям этих критериев субъекты Российской Федерации будут разделены на три группы (рис.3):

1) с высокой долговой устойчивостью;
2) со средней долговой устойчивостью;
3) с низкой долговой устойчивостью.

Рисунок 3 – Классификация заёмщиков по группам долговой устойчивости

И к регионам, которые попадут в так называемую «красную» группу, будут применяться особые дополнительные требования. Они будут состоять в том, что абсолютно все субъекты Российской Федерации должны будут формировать и представлять в Министерство Финансов основные направления долговой политики. Но только для регионов третьей группы будет введено требование согласования этого документа с Министерством Финансов с ограничением уровня заимствований (рис. 4). Кроме того, будет введено требование об утверждении и выполнении плана восстановления платёжеспособности субъектов Российской Федерации с низкой долговой устойчивостью.



Требования и ограничения	Группа А (высокая долговая устойчивость)	Группа В (средняя долговая устойчивость)	Группа С (низкая долговая устойчивость)
Разработка основных направлений долговой политики (ОНДП)	+	+	+
Представление проекта ОНДП в Минфин, финорган субъекта	-	+	+
Согласование программ заимствований и гарантий с Минфином, финорганом субъекта	-	+	+
Предельный объем заимствований ограничен суммой, направляемой на погашение долговых обязательств	-	-	+

Рисунок 4 - Требования к заемщикам в зависимости от группы долговой устойчивости

Предусматривается реформирование системы бюджетных платежей, поскольку учреждениями Банка России и территориальными органами Федерального казначейства осуществляются дублирующие однородные операции при осуществлении расчетов между бюджетами.

В рамках управления единым казначейским счетом осуществляется многочисленный перевод средств между этими счетами, при этом срок осуществления платежей составляет до 3 рабочих дней, имеется значительный объем операций с наличными денежными средствами.

В этой связи в рамках приказа Министерства финансов Российской Федерации от 29 августа 2013 года № 227 "Об утверждении Концепции реформирования системы бюджетных платежей на период до 2017 года" с учетом положений Федерального закона о национальной платежной системе разработана новая глава

"Бюджетные платежи и система бюджетных платежей" (рис. 5) [5].

Рисунок 5 – Соотношение системы бюджетных платежей и национальной платежной системы

Основная ее цель – на законодательном уровне закрепить необходимость проведения всех государственных платежных операций через единый казначейский счет Федерального казначейства в Банке России, переведя многочисленные банковские счета бюджетов бюджетной системы в учётную систему Федерального казначейства.

Положения указанной главы позволят решить следующие задачи:

1) обеспечить безопасность прохождения бюджетных средств;

2) создать условия для повышения эффективности управления бюджетными средствами;

3) сократить сроки прохождения денежных средств в бюджеты и из бюджетов;

4) минимизировать объем наличных денежных средств в секторе государственного управления.

Также введение главы о системе бюджетных платежей позволит снизить транзакционные издержки при осуществлении операций со средствами бюджетов, расширит платежные сервисы, повысит доступность и комфортность оплаты государственных и муниципальных услуг для граждан и организаций. В этой связи закрепляются положения, регламентирующие виды бюджетных платежей и принципы функционирования их системы

(непрерывность, безотзывность), определяются участники системы бюджетных платежей и их полномочия, устанавливаются общие требования к формам расчетов.

Бюджетный кодекс Российской Федерации предлагается дополнить новой версией принципа подотчетности и прозрачности (открытости), который означает обязанность государственных (муниципальных) органов предоставить отчетность о результатах использования бюджетных средств, а также их ответственность за исполнение своих полномочий и принятых расходных обязательств. Указанным принципом предполагается распространить нормы Бюджетного кодекса на неучастников бюджетного процесса, в том числе в части предоставления отчетности о результатах использования бюджетных средств, в связи с чем проводится работа по уточнению полномочий по государственному (муниципальному) финансовому контролю (рис. 6).

Рисунок 6 – Уточнение полномочий по государственному (муниципальному) финансовому контролю

Ещё одна новация – введение понятия «Налоговые и неналоговые расходы бюджетов». Эти параметры должны будут представляться вместе с проектом бюджета в законодательные представительные органы. И только он позволит оценить полный объём ресурсов, которые используются на достижение тех или иных целей государственных и муниципальных программ. К сожалению, в

настоящее время мы не знаем ни полного объёма введённых налоговых льгот и преференций, ни самое главное того, на какие цели они направлены, как используются для достижения целей государственных и муниципальных программ. Введение этого понятия позволит решить все эти задачи [8].

Порядок введения в действие новой редакции Бюджетного кодекса будет определён в отдельном проекте федерального закона «О введении в действие Бюджетного кодекса Российской Федерации».

В целях создания надлежащих условий для применения новой редакции Кодекса предлагается:

Во-первых, в этом году планируется ввести положения, которые позволят подготовить проекты бюджетов бюджетной системы Российской Федерации на 2017 год в соответствии с требованиями новой редакции Кодекса;

Во-вторых, с 1 января 2017 года планируется осуществлять исполнение бюджетов с учётом требований новой редакции Кодекса;

В-третьих, с 2019 года планируется ввести систему показателей оценки долговой устойчивости субъектов Российской Федерации [2].

Устаревшая структура Бюджетного кодекса Российской Федерации затрудняет его использование как гражданами и организациями, так и государственными (муниципальными) органами. В связи с этим, законопроект предусматривает новую его структуру, исключая утратившие силу нормы. Указанные изменения будут способствовать удобству применения Бюджетного кодекса Российской Федерации, а также иных законов и нормативных правовых актов, регулирующих бюджетные правоотношения.

Таким образом, вводимые новации направлены на совершенствование бюджетных правоотношений, на развитие открытости бюджетного процесса и информированности граждан о бюджете и бюджетном процессе. Также в Кодексе существенно расширены нормы о безусловном исполнении публично-правовым образованием действующих расходных обязательств (особенно публичных нормативных обязательств, связанных с выплатами бюджетных средств физическим лицам). Предлагаемые нормы по реформированию системы бюджетных платежей направлены на более комфортное осуществление оплаты государственных (муниципальных) услуг гражданами и организациями.

Литература
1. "Бюджетный кодекс Российской Федерации" от 31.07.1998 N 145-ФЗ (ред. от 15.02.2016);
2. Пояснительная записка к проекту федерального закона "Бюджетный кодекс Российской Федерации";
3. Программа повышения эффективности управления общественными (государственными и муниципальными) финансами на период до 2018 года (Утверждена распоряжением Правительства Российской Федерации от 30 декабря 2013 г. N 2593-р);
4. Государственная программа Российской Федерации "Управление государственными финансами и регулирование финансовых рынков" (Утверждена постановлением Правительства Российской Федерации от 15 апреля 2014 г. N 320);
5. Приказ Министерства финансов Российской Федерации от 29.08.2013 N 227 "Об утверждении Концепции реформирования системы бюджетных платежей на период до 2017 года";
6. Бюджетное послание Президента РФ Федеральному собранию от 13.06.2013 "О бюджетной политике в 2014 - 2016 годах";
7. Официальный сайт компании "КонсультантПлюс" (http://www.consultant.ru/).
8. Развитие налоговой политики стран Таможенного союза Таран Е.М., Таран М.А. // Перспективы, организационные формы и эффективность развития сотрудничества ВУЗов стран Таможенного союза и СНГ сборник научных трудов Международной научно-практической конференции. 2013. С. 461-471.

КРЕДИТНЫЕ ПОЛИТИКИ РЕГИОНАЛЬНЫХ КОММЕРЧЕСКИХ БАНКОВ

Гридин Евгений Игоревич, студент 3 курса кафедры Финансов и бухгалтерского учета
Научный руководитель: **Салманов Олег Николаевич**, д.э.н., профессор кафедры Финансов и бухгалтерского учета

Основная доля рынка финансовых услуг (примерно 75-80%) принадлежит пятидесяти крупнейшим банкам, но в России на 1 января 2015 года насчитывается около восемьсот пятидесяти банков. В статье анализируется проблема выживаемости небольших региональных коммерческих банков, их кредитной

политике, направленной на конкурирование с крупными банками, хотя бы в своем регионе.

В статье раскрывается несколько особенностей используемых региональными коммерческими банками в своей кредитной политике, для снижения рисков и получения финансовой устойчивости.

Кредитная политика, региональные банки, особенности кредитной политики.

CREDIT POLICIES OF REGIONAL COMMERCIAL BANKS

Gridin Evgeny, 3rd year student of the Department of finance and accounting
Scientific adviser: **Salmanov Oleg**, Doctor of Economic Sciences, Professor of the Department of finance and accounting

The major share of the financial services market (about 75-80%) belongs to the fifty largest banks, but in Russia on January 1, 2015, there are about eight hundred and fifty banks. The article analyzes the problem of the survival of small regional commercial banks, their credit policies to competition with large banks, at least in its region.

The article reveals several features used by regional commercial banks in their lending policies to reduce risks and gain financial stability.

Credit policy, regional banks, especially credit policies.

Кредитная политика - это главное направление развития коммерческого банка в области кредитования (предоставления ссуд) физическим и юридическим лицам

В кредитной политике прописываются задачи и приоритеты кредитной деятельности банка, средства и методы их достижения, а также как будет организован кредитный процесс.

Главная цель кредитной политики – достижение максимальной прибыли при минимальных рисках.

Разрабатывая кредитную политику, руководство банка основывается на ряде факторов: субъект кредитования, или кому будет предоставлена ссуда, характер займа – зачем или на какие цели субъект кредитования берет заем, сроки кредитования и какие отраслевые направления будет кредитовать банк. В сумме все выше перечисленные факторы образуют кредитный портфель банка,

который ляжет в основу кредитной политики банка и как раз поможет решить главную задачу банка – максимизация прибыли при минимизации рисков.

Но кредитная политика это не такой документ, который написал и забыл. Вся сложность начинается как раз после её составления. Рынок нестабилен, все быстро меняется, поэтому банк должен всегда держать руку на пульсе, моментально реагировать на изменения и перестраивать свою политику кредитования [3].

Вот, например:

Как только в январе 2015 года задолженность по кредитам, предоставленным физическим лицам выросла почти на 5 триллионов рублей, банки незамедлительно пересмотрели свою кредитную политику и в первом квартале 2015 года уменьшили объем выдачи кредитов физическим лицам практически вдвое (см. рис. 1 и рис. 2) [1].

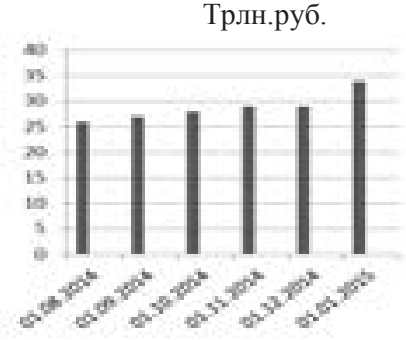


Рисунок 1 - Динамика задолженности по кредитам конец 2014, начало 2015

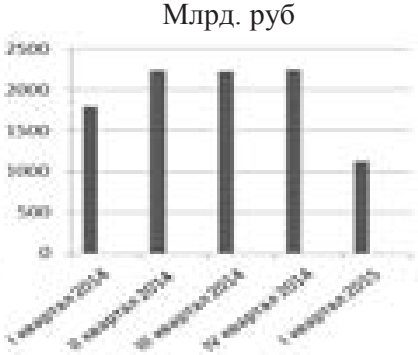


Рисунок 2 - Динамика выдачи кредитов конец 2014, начало 2015

Эти методы минимизации рисков достаточно очевидны, их используют все банки без исключений. Но в чем же особенности кредитной политики региональных коммерческих банков? Чем же все-таки они привлекают клиентов? Ответы на эти вопросы будут даны в этой статье.

Кредитная карта России.

В первую очередь, перед составлением кредитной политики, региональный банк оценивает общую кредитную атмосферу в своем регионе. Для этого можно обратиться к так называемой «кредитной карте России».

На ней можно оценить общую загруженность региона кредитами (рис. 3). В пятерку наиболее кредитно-активных регионов входят Москва (5,9% доля в общем количестве выданных кредитов), Московская область (4,05%),Свердловская область (3,59%), Краснодарский край (3,99%), Башкортостан (3,27%).

Наименьшая кредитная активность в Чукотском и Ненецком автономных округах, Ингушетии, Еврейской и Магаданской областях.

Рисунок 3 - Кредитная активность регионов

В регионах-лидерах активно развивается ипотечное и авто кредитование, люди привыкли к кредитам, у многих заемщиков есть по несколько кредитов. Банки в свою кредитную политику активно включают услугу перекредитования. В то время как в регионах, где берут мало кредитов, заемщики только начинают пробовать кредитные продукты. Естественно и конкуренция среди банков в регионах-лидерах выше [5].

Таблица 2 - Показатель PTI по регионам

Вообще нормальным показателем кредитной нагрузки считается 30-35%. В целом по стране у нас сейчас примерно 41%. Лишь в семи

регионах показатель PTI не превышает норму. Основная часть регионов находится в диапазоне 40-60%.

Высокий показатель уровня кредитной нагрузки, влечет за собой риски по ухудшению платежной способности заемщика в этих регионах.

Следующее что оценивает региональный коммерческий банк, это доля просроченной задолженности в регионе.

Самую высокую долю просроченной задолженности имеют Ингушетия (41,19%), Карачаево-Черкесии (30,29%).Самая низкая доля просроченной задолженности в Чукотском автономном округе (9,01%),Ненецком автономном округе (10,31%) [5].

Но нельзя так просто брать и откидывать регионы с большой задолженностью в них тоже можно успешно работать. В первую очередь задолженность нужно проанализировать по каждому кредитному продуктам, потому что по каждому продукту, в зависимости от региона, может быть свой процент задолженности.

Например:

Кредитам наличными – это самый высоко рисковый кредитный продукт. Доля просроченных кредитов в нем составляет 20,7%.

Хуже всего с возвращение кредитов наличными дело обстоит в Кабардино-Балкарии (50,39% кредитов наличными просрочено) и Ингушетии (29,73%). Самая низкая доля просрочки по кредитам наличными в Чукотском и Ненецком округе 8,76% и 10,15% соответственно.

Доля просроченной задолженности в авто кредитовании ниже она составляет 11,2%. Хуже всего по авто кредитам платит Бурятия (28,18% авто кредитов просрочено) и Приморский край (24,59%).Но а, например в Амурской области доля просроченных авто кредитов всего 5,56%.

Доля просроченной задолженности по ипотечному кредитованию составляет всего 3,58% от общего количества активных кредитов. Самая высокая доля задолженности по ипотечному кредитованию в Северной Осетии (11,79%), Кабардино-Балкарию (11,08%) и Дагестан (8,42%).А в Костромской области и на камчатке доля просроченных ипотечных кредитов составляет всего 0,47% и 0,80% соответственно.

Делая такую глубокую оценку своего региона, коммерческий банк, наполняет свой кредитный портфель качественными кредитами

и решает главную цель кредитной политики минимизация рисков и максимизация прибыли [1].

Так же коммерческий банк оценивает потребности региона исходя из его географического расположения.

Так, например:

1.Недавнее исследование национального агентства финансовых исследований (НАФИ) показало, что вклады делают в основном жители Москвы и Санкт-Петербурга, а берут клиенты в регионах. 65 % всех вкладов россиян приходится на Москву и Санкт-Петербург. А берут кредиты чаще в регионах, на них приходится примерно 60 % выданных кредитов.

Из этого можно сделать вывод, что в своей кредитной политике делать упор на привлечение вкладов региональным банкам вряд ли стоит.

2.Но различия есть не только между центральными городами и регионами, но и каждый регион по-своему уникален.

Например, в Южных регионах гораздо реже берут ипотеку на квартиры, чем на частные дома. Объясняется это «казацким» укладом жизни. Люди в этих регионах просто не привыкли жить в квартирах. Так же в южных регионах востребованы авто кредиты из-за того, что там принято иметь несколько машин на семью.

Так же так как Юг традиционно является местом отдыха людей, большим спросом там пользуются кредиты на земельные участки со стороны частных предпринимателей. Землю местные берут в основном для организации торговли или общественного питания.

3.В Сибири региональные банки делают упор на оперативность расчетно-кассового обслуживания (РКО), потому что крупные банки часто не могут оперативно решить задачи без согласования со своим центральным офисом.

4.В регионах находящихся восточнее уральских гор, люди обычно берут кредиты на покупку поддержанных авто, связано это с территориальной близостью региона к Японии.

Из этого всего можно сделать вывод, что региональные коммерческие банки очень детально исследуют потребности своего региона, они прекрасно представляют себе образ своего клиента. И на основе этого выстраивают свою кредитную политику и формируют уникальное предложение. Региональные банки знают, что нужно предложить своим клиентам здесь и сейчас.

Так же одним из ключевых столпов устойчивости коммерческого банка является диверсифицированная база клиентов.

Диверсифицированная база клиентов означает, что у банка нет клиента, от которого бы он серьезно зависел. Нет компании или человека, которые давали бы более 5% от совокупного дохода, или держали бы более 10% общей суммы остатков на счетах. Диверсификация базы клиентов очень актуальна в кризис. У банка с диверсифицированной базой клиента не будет такого, что одному клиенту стало плохо, или он решил перевести обслуживание бизнеса в другой банк – и все, банк потерял основную часть своего дохода [6].

Основные требования Центрального банка к коммерческим банкам

Ну и естественно для того, что бы спокойно и долго работать банк должен соблюдать действующее законодательство и нормативные акты банка России. А в соответствии с новыми требованиями, вступившими в силу в 2015 году по документу Базель III, соблюдать все нормы для небольших региональных коммерческих банков стало очень непросто. Но не соблюдать их нельзя.

Основные требования ЦБ (или за что банки лишают лицензии):

1.Достаточность банковского капитала первого уровня должна быть не менее 6%. (не менее 300 млн. руб.)

Это новое требование, вступившее в силу в соответствии с документов Базель III. В начале 2015 года застало врасплох 171 банк, и в основном это были как раз региональные коммерческие банки. Этим банкам пришлось увеличить объем собственных средств, примерно на четверть, для того что бы, не лишиться лицензии.

2.Банк должен отвечать по своим кредитным обязательствам в течении 14 дней со дня возникновения финансовых требований.

3.В процессе своей деятельности банк не должен допускать снижение размера капитала, ниже установленного минимума.

Так же есть требования, по которым ЦБ может лишить банк лицензии, но не сразу:

1.Банк предоставил недостоверные отчетные данные.

2.Банк задержал ежемесячную отчетность более чем на 14 дней.

3.Банк больше года не осуществляет банковские операции, предусмотренные лицензией, или наоборот осуществляет операции, не имея на них лицензии.

4.Выявлено несоблюдение законов РФ и нормативных актов [1].

Выводы:

Кредитная политика – это главное направление кредитной деятельности банка. Кредитная политика – это документ, который требует постоянных доработок. Для того что бы достичь цели кредитной политики – максимальная прибыль при минимальных рисках, банк должен не на минуту, не выпускать из виду рынок, и незамедлительно менять свою политику кредитования в соответствии с произошедшими на рынке изменениями.

Региональные коммерческие банки, при составлении кредитной политики должны максимально глубоко погружаться в потребности своего региона. Оценивать его потребности исходя из идеологического состояния региона, географического расположения. Должны оценивать кредитную активность в регионе, показатель PTI, или другими словами показатель кредитной нагрузки в регионе, ну и конечно оценить уровень задолженности по кредитам в регионе. Банк должен плотно проанализировать задолженность, отсортировать те кредитные продукты, по которым в регионе высокая задолженность и сделать упор в своей кредитной политике на отрасли кредитования, по которым задолженность приемлемая.

Так же для своей устойчивости и долголетия финансовой деятельности баку нужно стараться разделять или диверсифицировать свою базу клиентов, для того что бы максимально снизить свои риски, в случае если одному из клиентов станет плохо.

И обязательно, банк должен плотно и правильно контактировать с регулятором, хоть в последнее время это становится все сложнее и сложнее, но, тем не менее, добросовестно исполняя все требования можно оставить о своем банке хорошую репутацию, что непременно приведет к поднятию престижа и рейтинга банка.

Литература

1. Отчет ЦБ РФ. Экспресс выпуск: “Обзор банковского сектора российской федерации” №155 2015 год. Режим доступа: http://www.cbr.ru/analytics/bank_system/obs_ex.pdf (дата обращения 10.12.2015)

2. Бизнес-планирование в коммерческом банке: Учебное пособие / Н.Н. Куницына, А.В. Малеева, Л.И. Ушвицкий. - М.: Магистр: НИЦ ИНФРА-М, 2014. - 384 с.: 60х90 1/16. (переплет) ISBN 978-5-9776-0096-5, 300 экз.

3. Банковское дело: Учебник / Е.Б. Стародубцева. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 464 с.: 60х90 1/16. - (Высшее образование). (переплет) ISBN 978-5-8199-0575-3, 500 экз.
4. Информационный портал – BANKI.RU, Статья ОТ 23.09.2013 - «БАЗЕЛЬ-3» КАК «Санитар леса». Электронный ресурс. Режим доступа: http://www.banki.ru/news/bankpress/?id=5441600 (Дата обращения: 20.12.2015).
5. Информационный Портал – BANKI.RU, Статья от 25.05.2015 «Мы такие разные: как берут и отдают кредиты в российских регионах». электронный ресурс. режим доступа: http://www.banki.ru/news/daytheme/?id=8013281 (Дата обращения 20.12.2015).
6. Журнал: Экономические науки, издательство: ООО "Экономические науки" (Москва), ISSN: 2072-0858, «Особенности кредитной политики региональных коммерческих банков». Электронный ресурс. Режим доступа: http://elibrary.ru/item.asp?id=10025865&SesCookieID=386722031&UserID=171594151 (дата обращения 25.12.2015)

АНАЛИЗ ФИНАНСОВОЙ УСТОЙЧИВОСТИ РЕГИОНАЛЬНЫХ БАНКОВ

Иванова Екатерина Валерьевна, студентка 3 курса кафедры Финансов и бухгалтерского учета
Научный руководитель: **Салманов Олег Николаевич,** д.э.н., профессор кафедры Финансов и бухгалтерского учета

Современная экономическая ситуация в стране создает сложные условия для существования и развития банковской сферы. Особенно это касается таких мелких игроков, как региональные банки. Финансовая устойчивость местных банков, является основной характеристикой качества банка, которое формируется совокупностью целевых установок различных сторон заинтересованных в результатах его деятельности. Целью авторского исследования является изучение устойчивости региональных банков Республики Татарстан, Ростовской и Самарской областей при использовании методики рейтингового агентства «Эксперт».

Региональные банки, банковская сфера, финансовая устойчивость.

BANK QUESTION: WHETHER REGIONAL BANKS WILL SURVIVE

Ivanova Ekaterina, 3rd year student of the Department of finance and accounting
Scientific adviser: **Salmanov Oleg,** Doctor of Economic Sciences, Professor of the Department of finance and accounting

The current economic situation in the country creates a challenging environment for the existence and development of the banking sector. This is especially true of small players such as regional banks. Financial stability of the local banks, is the main characteristic of the quality of the bank, which is formed by a set of targets of the various parties interested in the results of its operations. The aim of the author's research is to study the stability of the regional banks in the Republic of Tatarstan, Rostov and Samara regions using the methodology of the rating agency "Expert".

Regional Bank and the banking sector, financial stability.

Термин «региональный банк» представляется в виде множества разрозненных трактовок отечественных и зарубежных исследователей, именно поэтому достаточно сложно оперировать одним конкретным определением. Однако, универсальным являются следующие характеристики присущие исключительно местным банкам:

- Региональный банк – имеет главный офис в одном из регионов;
- Региональный банк функционирует в одном конкретном регионе, с присущими ему спецификами [1].

Региональные банки являются важным элементом всей банковской системы. Их роль как регуляторов финансового оборота, центров аккумуляции, накопления и перераспределения денежных ресурсов возлагает на них весомую ответственность перед обществом и требует постоянной нацеленности на повышение своей надежности и финансовой устойчивости [7].Пожалуй, основным положительным фактором для региональных банков является близость к местной экономике. Они лучше осведомлены о деловой репутации и реальном положении дел хозяйствующих субъектов, имеют наработанные связи с властными структурами, обладают мобильными схемами

работы с клиентами, обслуживают различные категории граждан, учитывая их возможности и специфические проблемы.

Региональные банки являются движущей силой в кредитовании малого и среднего бизнеса. Обусловлено это тем, что кредитным организациям в целях минимизации рисков по невозврату кредитов следует оценивать не только заемщиков, но и его поставщиков, подрядчиков, покупателей. Безусловно, в данном случае преимущество у региональных банков. Поскольку у местных банков имеется больше возможностей для сбора информации о потенциальных заемщиках в отличие от федеральных банков.

Важно учесть и слабые стороны местных банков. К ним относится: ограниченность капитала, дорогое фондирование, высокие риски потери деловой репутации, меньшая линейка продуктов и услуг [3].

Возрастание банковских рисков, усиление межбанковской конкуренции, ужесточение требований которые предъявляют надзорные органы к кредитным организациям, актуализируют задачи управления финансовой устойчивостью кредитных организаций, от эффективности решения которых в полной мере зависит благополучие самих банков, формирование резервов и фондов функционально ориентированное на содействие их развитию.

Финансовая устойчивость коммерческого банка – это характеристика его деятельности, базирующаяся на способности эффективно формировать и эффективно использовать финансовые потоки для обеспечения четкого выполнения необходимых, общественно значимых функций, создания достаточных резервов в целях предотвращения неблагоприятных ситуаций, а так же дальнейшего расширения деятельности на основе качественного менеджмента [4].

В настоящее время существует большое многообразие методик оценки финансовой устойчивости коммерческих банков, которые подразделяются на две больших категории, а именно зарубежные и российские. К российским методикам относятся:

- Методики Банка России (методики в соответствии Указанием Банка России от 30 апреля 2008 г. № 2005-У и Указанием Банка России от 16 января 2004 г. № 1379-У)
- Методики рейтинговых и информационных агентств, авторские методики (методики «Коммерсант», В. Кромонова, Аналитического центра финансовой информации, рейтингового

агентства «Эксперт», «Оргбанка», информационного центра «Рейтинг») [5].

Следует сказать, что проблемам функционирования местных банков, как одному из звеньев всей банковской системы, их устойчивости и роли в развитии экономики уделяется минимальное внимание.

В связи с этим на трех регионах России (Республика Татарстан, Ростовская и Самарская области) была апробирована методика агентства «Эксперт» для анализа и оценки финансовой устойчивости банков данных регионов.

Данные регионы были выбраны, поскольку они являются наиболее развитыми в России, уступая лишь Москве и Санкт-Петербургу. Так в республике Татарстан сложилась хорошая система мелких (55%), средних (36%) и крупных банков (9%). Причем преобладают местные самостоятельные банки: их насчитывается 22, что составляет около 60% всех коммерческих банков, работающих в регионе. Характерной особенностью банковского сектора республики является тесное сотрудничество с местными властными структурами в поддержке регионального бизнеса. Исторически сложилось так, что еще в девяностых годах руководство республики уделяло значительное внимание развитию местного банкинга. В результате сейчас республиканская банковская система стала одной из мощнейших в стране.

Именно эффективное взаимодействие двух институтов— власти и бизнеса — помогло банкам республики выйти в лидеры рынка и сохранить свои лучшие качества даже в условиях острой конкуренции между собой и с филиалами крупнейших банков страны. Следующими по развитости банковского сектора являются Ростовская и Самарская области. Ростовская область является лидером на Юге России по активности кредитных организаций и их филиалов. В значительной мере это объясняется производственно-экономическим и торговым потенциалом региона. В регионе расположено наибольшее в ЮФО число кредитных организаций. Все они относятся к категории «финансово-стабильные». На данный момент в Ростовской области действует 14 региональных банка, что составляет 41% всех коммерческих банков региона. В качественном отношении банковский сектор Ростовской области представлен в основном малыми (73%) и средними банками (27%). Наиболее

крупными региональными кредитными организациями являются ОАО КБ Банк «Центр Инвест», ООО КБ «Донинвест» [2].

В Самарской области, как и в Ростовской количество региональных банков равно 14, однако самостоятельные банки занимают меньше 1/3 банковского сектора области, приблизительно 30% [8]. Можно утверждать, что основная часть рынка банковских услуг региона приходится на банки федерального уровня, среди которых доминируют государственные банки. В их группу целесообразно включить Сбербанк России, ВТБ с дочерними банками и Россельхозбанк.

Для исследования и анализа финансовой устойчивости данных регионов была использована методика рейтингового агентства «Эксперт». Выбор был обусловлен тем, что проанализировать банковскую структуру регионов можно было полагаясь на общедоступные данные на сайте Центрального Банка России. Сама методика представляет собой попытку построения комплексного сравнительного рейтинга и подразделяется на две главные части. Первая часть носит название статистической и предполагает сравнение банков в координатном пространстве «прибыльность-надежность». Расчет показателя прибыльности есть отношение балансовой прибыли к нетто-активам. Показатель надежности, в свою очередь, это соотношение собственного капитала банка и привлеченных средств.

Результаты анализа текущего состояния местных банков данных регионов наносятся на плоскость с осью абсцисс, соответствующей показателю надежности, и с осью ординат, соответствующей показателю прибыльности, в итоге координатное пространство распадается на четыре основных сегмента. Первый сегмент, так называемых «звездных» банков, характеризуется наиболее удовлетворительной надежностью и доходностью, их значения находятся выше средних. Второй – «прибыльнооориентированнный» характеризуется весьма рентабельным использованием относительно объемов привлеченных средств-ресурсов. «Капитализированным» банкам (третий сегмент) свойственен высокий объем капитала, при имеющейся невысокой доходности использования ресурсов. «Депрессивные» банки – это последний и самый неблагоприятный сегмент, характеризующийся как невысокой прибыльностью, так и минимальной надежностью. Координатная система «прибыльность-надежность» представлена на рис. 1.

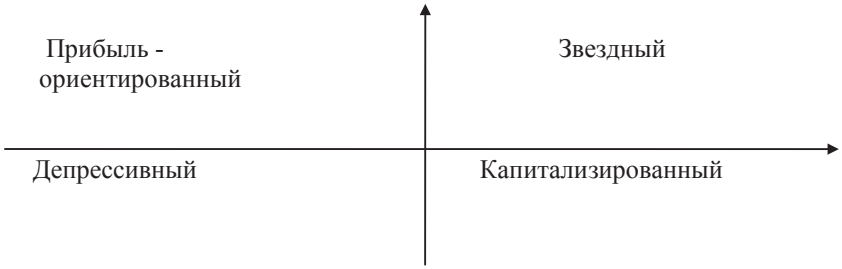


Рисунок 1 - Координатная система «прибыльность-надежность»

Вторая часть заключается в анализе имеющихся параметров прибыльности и надежности [6]. Согласно методике рейтингового агентства «Эксперт» была проанализирована финансовая устойчивость региональных банков представленных областей по состоянию на 1 ноября 2015 г. Результаты двухкритериального анализа текущего состояния по методике рейтингового агентства «Эксперт» были следующими. Результаты анализа Республики Татарстан представлены на рисунке 2. Названия банков были заменены на условные. Исходя из получившегося графика ясно, что 50% всех банков относятся к категории «депрессивные», 29% являются прибыль - ориентированными, 17% - звездные, 4% - капитализированные.

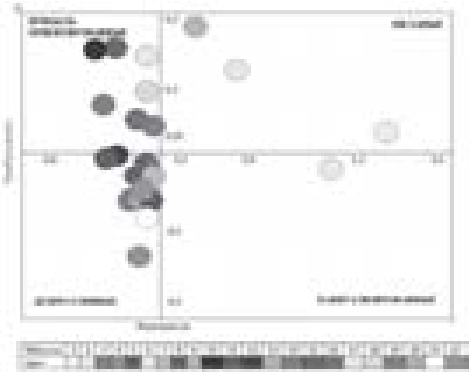


Рисунок 2 - Результаты анализа Республики Татарстан по методике рейтингового агентства «Эксперт»

На рисунке 2 представлены результаты двухкритериального анализа текущего состояния банков Ростовской области. По которым понятно, что большую часть всех местных банков, как и в Республике Татарстан занимают депрессивные банки – также 50%, прибыль – ориентированные банки – 21,5%, звездные – 21,5%,

капитализированные – 7%.Следует сказать, что к числу позитивных перспектив для данного региона можно отнести вероятный переход прибыльно ориентированных банков в категорию звездных, при условии повышения их капитализации, что объясняется близостью прибыльно ориентированных банков к границе категорий.

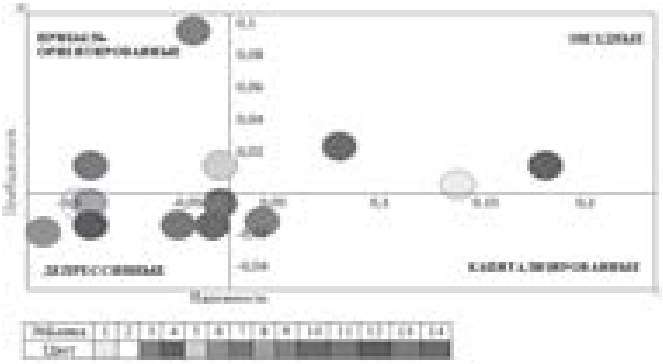


Рисунок 3 - Результаты анализа Ростовской области по методике рейтингового агентства «Эксперт»

Региональные банки Самарской области представлены на рисунке 3. Депрессивные банки данного региона занимают больше половины всех региональных банков – целых 64%, прибыль – ориентированные банки – 21%, звездные – 7,5%, капитализированные – 7,5%.

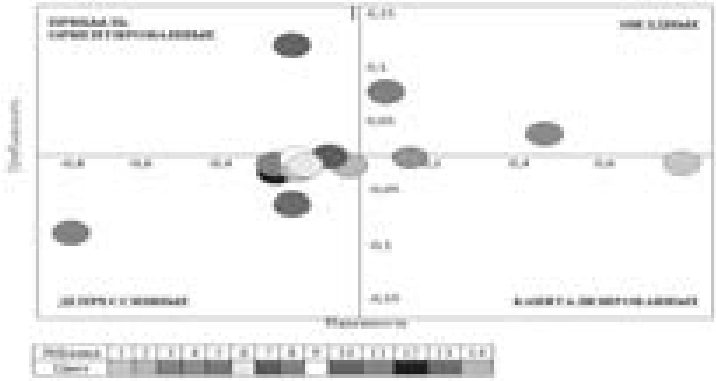


Рисунок 4 - Результаты анализа Самарской области по методике рейтингового агентства «Эксперт»

Важно отметить, что количество банков во втором и третьем сегменте оказалось одинаковым, а именно в сегменте

капитализированных банков, характеризующихся высокой достаточностью капитала при невысокой доходности использования ресурсов и в сегменте звездных банков, доходность и надежность которых выше средних.

Как видно из получившихся диаграмм большинство региональных банков рассмотренных регионов относится к категории депрессивных банков, надежность которых является неудовлетворительной, и при этом наблюдается невысокая прибыльность использования значительных объемов привлеченных средств и категории прибыльно ориентированных банков, обладающих высокорентабельным использованием относительно больших объемов привлеченных средств.

Не менее важное значение имеет показатель надежности банка, определяющий степень покрытия привлеченных средств собственным капиталом. Значение данного показателя находится в диапазоне от 12 до 24% для депрессивных банков, что обусловлено их малой капитализацией; учитывая тот факт, что прибыль является одним из самых надежных источников наращивания капитала, а депрессивные банки характеризуются низкой прибыльностью, нынешнее положение данных банков может в среднесрочной перспективе усугубиться.

Как уже было сказано, позитивная перспектива это вероятный переход прибыльно ориентированных банков в категорию звездных, при условии повышения их капитализации. Капитализированные же банки, напротив, стремятся к группе депрессивных, в связи с этим важно приложить максимум усилий для предотвращения данного перехода, а звездным банкам использовать все возможности для сохранения своих позиций.

Таким образом, сложившаяся ситуация сигнализирует о необходимости разработки стабилизирующих мер, способствующих повышению устойчивости функционирования коммерческих банков и в конечном итоге формированию устойчивой региональной банковской системы в данных областях и республике состоящей из звездных и прибыльно ориентированных банков, на которые на данный момент приходится только 46% анализируемых региональных банков.

Литература
1. Аванесян Г. электрон. версия, 2011. Нужны ли региональные банки экономике современной России. Электронный ресурс. Режим доступа: http://www.funansust.ru (дата обращения 11.10.15-5.11.15)
2. Банки.ру электрон. версия. Электронный ресурс. Режим доступа: http://www.banki.ru/banks/bank/centr-invest/ (дата обращения: 29.10.2015- 15.11.2015)
3. Войлуков А.А. Перспективы развития региональных кредитных организаций [Текст] /А.А. Войлуков// Деньги и кредит - 2012. - №11-93с.
4. Глотова А.С. Финансовая устойчивость региональных коммерческих банков [Текст] /А.С. Глотова // НИУ «БелГУ» - 2014. – 1с.
5. Клаас Я.А. Определение финансовой устойчивости региональных банков посредством действующих методик [Текст] /Я. А. Клаас// - 2014.- 50с.
6. Клаас Я.А. Определение финансовой устойчивости региональных банков посредством действующих методик [Текст] /Я. А. Клаас// - 2014.- 52с.
7. Уварова Л.Ф. Оценка финансовой устойчивости региональных коммерческих банков, их оздоровление и укрепление [Текст] /Л.Ф. Уварова // Журнал правовых и экономических исследований - 2013. – 147с.
8. Центральный банк Российской Федерации. Электронный ресурс. Режим доступа: http://www.cbr.ru/credit/f123.asp?when=20151101&regn=3461 (дата обращения: 13.10.2015-02.12.2015)

ПАТРИОТИЗМ, КАК НРАВСТВЕННЫЙ РЕСУРС МОСКОВСКОЙ ОБЛАСТИ

Кузнецова Екатерина Павловна, Митина Елизавета Александровна, студентки 2 курса кафедры Финансов и бухгалтерского учета
Научный руководитель: **Викулина Евгения Викторовна,** к.э.н., доцент кафедры Финансов и бухгалтерского учета

Уважение к своему государству, к его истории, желание и стремление изменить свою страну к лучшему, сделать ее прекраснее, беречь и ценить родину – чаще всего в этом проявляется

патриотизм каждого человека. Но интересно было бы узнать каков патриотизм в наше время, готово ли современное молодое поколение в случае необходимости поступить, как их деды и прадеды, которые, будучи обычными подростками, рвались на фронт, чтоб защитить свое отечество.

Патриотизм, молодежь, родина.

PATRIOTISM AS A MORAL RESOURCE OF THE MOSCOW REGION

Kuznetsova Ekaterina, Mitina Elizaveta, 2nd year students of the Department of finance and accounting
Scientific adviser: **Vikulina Evgeniya**, Candidate of Economic Sciences, Associate Professor of the Department of finance and accounting

Respect to their state and to desire and desire to change their country for the better, to make it more beautiful, to be cherished and treasured homeland – most often this is the manifestation of patriotism of each person. But it would be interesting to know what patriotism is in our time is whether the current young generation if necessary to do what their grandfathers and great-grandfathers, who, being normal teenagers, rushed to the front to defend the country.

Patriotism, youth, homeland.

Тема патриотизма сегодня, как и в любые другие времена, очень актуальна. Это тема была выбрана не случайно. В наше время, когда существует проблема отсутствия национальной идеи, необходимо уделять большое внимание гражданско-патриотическому воспитанию. В данной статье мы рассмотрим патриотизм, как нравственный ресурс Московской Области.

С этой целью было проведено статистическое исследование среди молодого населения Московской области и на основе анализа полученных результатов сделаны выводы о значении патриотизма для современного общества и даны рекомендации по дальнейшему его развитию среди молодого поколения. Количество респондентов, принявших участие в опросе, составило 164 человека, большая часть из которых находится в возрастной категории от 19 до 25 лет.

В ходе проведения статистического исследования были решены следующие задачи:

➢ проведен опрос среди молодого поколения Московской Области согласно разработанной анкете;

➢ обработаны полученные данные, результаты представлены в виде соответствующих графиков и диаграмм;

➢ сделаны выводы об основных аспектах патриотического воспитания среди молодёжи и рассмотрены дальнейшие пути развития патриотического воспитания [1].

На сегодняшний день очень сложно давать четкое определение патриотизму. Патриотизм - личное дело каждого человека, и каждый его понимает по-своему – через свое воспитание, через профессию, свою семью и так далее. Это чувство, которое делает народ и каждого человека ответственным за жизнь страны.

Но все же общество смогло дать обобщенное определение патриотизму. Патриотизм — нравственный и политический принцип, социальное чувство, содержанием которого является любовь к родине и готовность пожертвовать своими частными интересами во благо интересов отечества.

При проведении исследования респондентам были заданы вопросы, касающиеся их оценки патриотического воспитания молодежи.

При ответе на первый вопрос они дали своё определению патриотизму (рис. 1). 70% респондентов считают, что патриотизм – это любовь к Родине. 15,5% - активная позиция по отношению к Родине. А вот 7,8% опрошенных указало, что это готовность к самопожертвованию. Незначительная доля считает, что патриотизм – любовь к месту рождения и лишь 1,5% сказало, что это любовь к семье. Как видно, большинство людей понимает патриотизм именно как любовь к Родине, нежели любовь к семье [1].

Рисунок 1 - Как вы понимаете слово «патриотизм»? Что оно обозначает?

Далее был задан следующий вопрос: «Считаете ли Вы себя патриотом России?». Большинство молодого поколения считают себя

патриотами (рис. 2). Они ответили «скорее да» и «да» (47% и 30% соответственно). А вот остальная молодежь в равном количестве ответили иначе: скорее нет, нет и затруднились ответить. Таким образом, молодежь Московской Области считает себя патриотами своей страны [2].

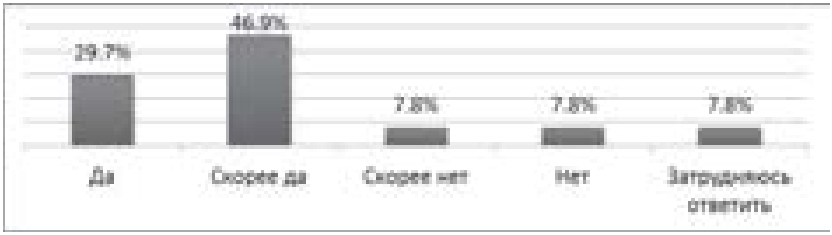


Рисунок 2 – Считаете ли вы себя патриотом России?

Доказательство этому выводу можно найти в ответах на такой вопрос: «Что для Вас 9 мая?» (рис. 3). Абсолютное большинство считают, что это исторический праздник, день памяти воинам-освободителям, хождение на торжественное возложение венков, военный парад на Красной площади, праздничный салют. Но есть и такие, кто ответил, что это выходной и обычный, ничем не примечательный день [3].

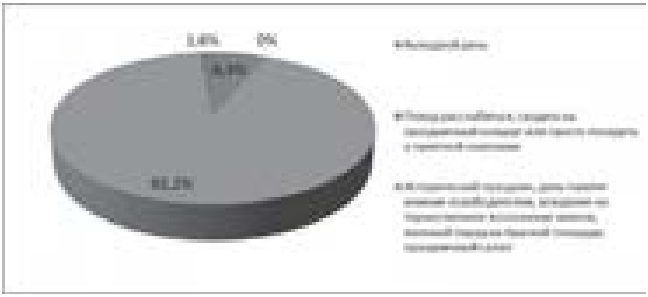


Рисунок 3 - Что для Вас 9 мая?

Следующий вопрос звучал так: «Что, прежде всего, внушает Вам чувство гордости за Россию?». Патриотизм зачастую понимается как проявление чувства гордости за свою страну (рис. 4). Как показал опрос, молодёжь большей частью гордится Российской историей, природными богатствами, Российской культурой, вооруженными силами, размерами страны, спортивными достижениями. Довольно небольшое число респондентов испытывает чувство гордости за положение России на международной арене, современные

достижения Российской науки. Еще один тревожный показатель – только 9,5% россиян гордятся своими согражданами. И всего лишь 6,3% городятся системой Российского образования [4].

Рисунок 4 - Что, прежде всего, внушает Вам чувство гордости за Россию?

Люди выражают свой патриотизм, участвуя и в политических мероприятиях (рис. 5).

Рисунок 5 - В каких политических мероприятиях вы принимали участие?

Так половина опрошенных не остаются равнодушными к выборам. Некоторые участвовали в сборе подписей, петиций. Часть принимала участие в митингах, пикетах и забастовках. Небольшое количество даже работала в политических партиях. Но, к сожалению, есть и та часть молодёжи, которая не участвовала в политических мероприятиях. Эта группа опрашиваемых составила 37%. Бездействие можно было бы обосновать их возрастом, но основная

часть респондентов в данном опросе составляет возрастную категорию от 19 до 25 лет. Возможно, это связано с тем, что молодёжь не считает политические мероприятия патриотичными и важными в их жизни, что является негативным фактом [5].

В ответе на следующий вопрос: «Чего, по Вашему мнению, не хватает для поддержания патриотизма в нашей стране?» (рис. 6) подавляющие большинство опрошенных считает, что для поднятия патриотизма не хватает его зарождения от семьи. Также многие считают, что нужно сделать большой уклон в сторону знаний русского языка, истории России и русской отечественной литературы и повысить степень доверия населения у правительства. Чуть меньше опрошенных считает необходимым поднимать патриотизм посредством СМИ, вводить больше уроков по поддержанию патриотизма в учебных учреждениях, организовывать военные игры для подрастающего поколения, создать особую национальную идею. Оставшаяся часть молодёжи думает, что надо поднять православную религию для поддержания патриотизма. А некоторые из них разделились на две группы: одни считают, что в нашей стране с патриотизмом все хорошо, а другие утверждают, что не хватает ровным счетом ничего для поддержания патриотизма [6].

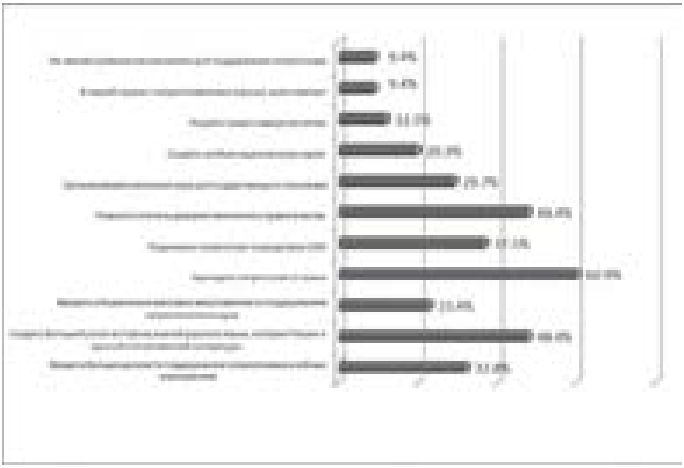


Рисунок 6 - Чего, по Вашему мнению, не хватает для поддержания патриотизма в нашей стране?

Также, несмотря на достаточно распространенный миф о том, что те, кто критикует действующий режим, не являются настоящими

патриотами, около 82% россиян придерживаются крайне противоположной точки зрения (рис. 7).

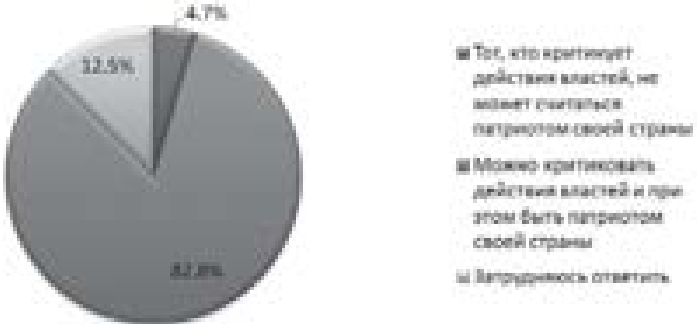


Рисунок 7 – Какая из следующих точек зрения Вам ближе?

Проведенный опрос также показывает обострение нетерпимости к «чужакам» (рис. 8). На вопрос о том, должно ли правительство ограничить приток приезжих в Россию, 62,3% россиян ответили утвердительно. Но почти 30% молодёжи считает, что не стоит ставить на пути притока приезжих административных барьеров. А вот 10% затруднились ответить на этот вопрос [8].

Рисунок 8 - Как Вы думаете, какой политики должно придерживаться правительство России?

И наконец, мы подошли к самому важному вопросу, который был сформулирован так: «Что такое, по вашему мнению, истинный патриотизм?» (рис. 9). Тут мнение респондентов разделилось в основном на 2 группы: одни считают, что это защита Отечества, служба в армии (48,8%), а 43,5% считают, что это уважений традиций. Также небольшая часть молодёжи ответила, что истинным патриотизмом является укрепление семейных ценностей и празднование исторических событий [9].

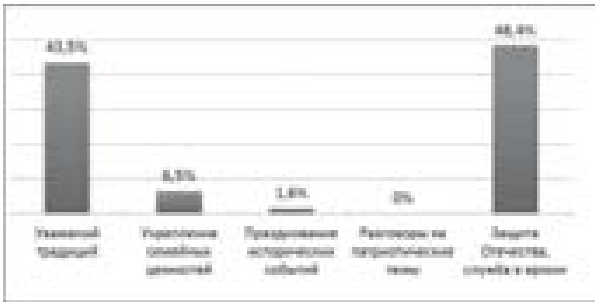


Рисунок 9 - Что такое, по вашему мнению, истинный патриотизм?

Анализируя все ответы на поставленные вопросы в целостности, можно сделать вывод о том, что большинство опрошенных связывает понятие патриотизма с любовью к своей стране. Как показало проведенное исследование, патриотизм в России принимает различные формы. Согласно существующим подходам к определению смысла патриотизма и его направленности, патриотизм признается как приоритетом для национальной идеологии, так и основой для естественного, личного чувства. Важным моментом является то, что российские власти и граждане уделяют огромное внимание патриотическому воспитанию молодого поколения, что является одной из приоритетных задач государства. В связи с этим можно выделить следующие первоочередные мероприятия, которые помогут поднять уровень патриотизма молодежи России на еще более высокий уровень. К ним можно отнести:

1.В школах и других учебных учреждениях нужно возрождать военно-спортивные и другие мероприятия патриотической направленности. То же касается и различных конкурсов об историческом развитии России. Например, литературные – на лучшее сочинение об отечественной войне, художественные – на лучший детский рисунок о величии Родины.

2.Дополнить перечень музеев, которые составляют национальное достояние Родины.

3.Необходимо активно использовать самые современные технологии, чтобы привлекать внимание молодежи. Речь идет о создании сайтов патриотической направленности в сети интернет и другие мероприятия патриотической направленности.

Проведенное исследование показало, что в настоящее время патриотизм стал актуальной темой среди молодёжи и это поколение

неравнодушно относится к данной проблеме. Это чувство, которое делает народ и каждого человека ответственным за жизнь страны и дальнейшее её развитие. Патриотизм должен быть в сердце каждого человека, так как это позволяет ставить перед собой высокие цели и достигать максимального результата, а также способствовать её процветанию.

Литература

1. Общая теория статистики: Учебное пособие / С.Н. Лысенко, И.А. Дмитриева. - Изд., испр. и доп. - М.: Вузовский учебник: НИЦ ИНФРА-М, 2014
2. Официальный сайт Федеральной службы государственной статистики Российской Федерации - http://www.gks.ru
3. Официальный сайт правительства Московской Области - http://mosreg.ru

ОСОБЕННОСТИ ФОРМИРОВАНИЯ УЧЕТНОЙ ПОЛИТИКИ НА ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЯХ

Малинова Мария Павловна, студентка 3 курса кафедры Финансов и бухгалтерского учета
Научный руководитель: **Банк Ольга Анатольевна**, к.э.н., доцент кафедры Финансов и бухгалтерского учета

Умело составленная учетная политика является одним из важнейших инструментов управления деятельностью фирмы и достижения поставленных целей менеджмента. Выбор учетной политики должен быть обоснованным, с тем, чтобы в конкретных условиях деятельности организации она наилучшим образом обеспечивала реализацию поставленной задачи.

Учетная политика, промышленное предприятие, бухгалтерская отчетность, ответственность, внесение изменений.

FEATURES OF FORMATION OF AN ACCOUNTING POLICY ON INDUSTRIAL ENTERPRISES

Malinova Maria, 3rd year student the Department of finance and accounting
Scientific advisor: **Bank Olga,** Candidate of Economic Sciences, Associate Professor of the Department of finance and accounting

Skillfully composed an accounting policy is one of the most important management instruments of a company and achieve its objectives of management. The choice of an accounting policy should be reasonable, so that in the specific context of a organization it is best to provide the implementation of the task.

Accounting policy, industrial enterprise, the financial statements, the responsibility, changes.

В настоящее время роль учетной политики огромна, поскольку она является частью системы регулирования бухгалтерского учета, инструментом управления финансовыми результатами и оптимизации налогообложения, средством поддержания порядка в бухгалтерском учете организации, весомым доказательством в судебных разбирательствах. Состоящая из взаимодействующих между собой элементов и представляющая многокомпонентную систему, грамотно подготовленная учетная политика позволяет обеспечить необходимой информацией всех заинтересованных пользователей и эффективность деятельности организации [3].

Экономический смысл учетной политики организации сводится к обеспечению формирования и отражения в учете оптимальных финансовых результатов ее деятельности. С разделением налогового, финансового и управленческого учета именно эти возможности учетной политики выходят на первый план.

В современных условиях в зависимости от целей, поставленных менеджерами фирмы, величина формируемого финансового результата может варьироваться в сторону, как увеличения, так и уменьшения. Сроки включения затрат в себестоимость, подходы к определению величины отдельных статей затрат, формирование фондов и резервов за счет источников, включаемых в себестоимость, могут существенно занизить потенциальный финансовый результат, подлежащий распределению между собственниками. Это может послужить целям пополнения средств на развитие предприятия.

В то же время, действуя в аналогичной ситуации, но выбрав иной вариант учетной политики, можно добиться обратного эффекта, если, например, приоритетным в данном периоде является привлечение инвесторов, получение кредитов и т.п.

Таким образом, умело составленная учетная политика является одним из важнейших инструментов управления деятельностью фирмы и достижения поставленных целей менеджмента. Кроме того,

грамотно составленная учетная политика должна помочь бухгалтерам, экономистам, аналитикам фирмы, которые не могут по каким-либо причинам оперативно связаться напрямую со своими руководителями (например, работают в отдаленных филиалах), уяснить общую стратегию организации и ведения налогового и бухгалтерского учета в компании в целом и на их участках работы в частности. Положения учетной политики должны помочь им избежать ошибок и противоречий в отражении учетных и отчетных данных, охватывать все уровни управления организацией [3].

В настоящее время можно констатировать существование трех основных видов учета: бухгалтерский, налоговый и управленческий, важнейшим инструментом формирования которых, соответственно, являются: учетная политика для целей бухгалтерского учета, учетная политика для целей налогового учета, учетная политика для целей управленческого учета.

Организации осуществляют различные виды деятельности, в том числе и в географических регионах с различными возможностями роста, имеют разные источники получения дохода и т.д. Все эти различия влияют на состав элементов, формирующих учетную политику. На основании этого можно говорить о существовании учетных политик для предприятий промышленной деятельности, торговой деятельности, предприятий оказания услуг и т.д. [3].

В зависимости от вида деятельности хозяйствующего субъекта учетную политику можно классифицировать на применяемую коммерческими организациями и применяемую некоммерческими организациями. Необходимость формирования учетной политики предусмотрена ст. 6 Федерального закона «О бухгалтерском учете». ПБУ 1/2008 «Учетная политика организации» устанавливает правила формирования учетной политики для всех юридических лиц, являющихся таковыми по законодательству РФ, за исключением кредитных организаций и государственных учреждений. Что касается учетной политики промышленного предприятия, она может включать следующие элементы:

1. рабочий план счетов;
2. формы первичной документации, которая необходима для оформления операций хоз. деятельности;
3. формы внутренних отчетов;
4. порядок, согласно которому будет осуществляться инвентаризация;

5. способы оценки обязательств и активов;

6. правила осуществления документооборота и методы обработки информации, полученной в результате учетной деятельности;

7. другие решения, необходимые для грамотного ведения бухгалтерского учета;

8. решения о принятии той или иной налоговой политики.

Таким образом, учетной политикой организации регламентируют осуществление бухгалтерского и налогового учета с учетом действующего законодательства. В последствии контролирующие органы будут проверять соответствие ведения учетной деятельности данному документу.

Что понимается под способами бухгалтерского учета? Это методы группировки и оценки фактов хозяйственной деятельности, организация документооборота, инвентаризации, погашения стоимости активов, способы примененияисчетов бухгалтерского учета, системы учетных регистров и т.д. [2].

Принятые способы бухгалтерского учета применяются всеми структурными подразделениями предприятия независимо от их месторасположения, в том числе и выделенными на отдельный баланс. Установленные способы ведения бухгалтерского учета применяются с 1 января года, следующего за годом издания соответствующего приказа, т. е. приказ об учетной политике предприятия вступает в силу с 1 января независимо от даты его утверждения. Исключением являются вновь создаваемые организации, для которых приказ об учетной политике считается вступившим в действие с момента приобретения ими прав юридического лица. Эти организации должны оформить избранную учетную политику до первой публикации бухгалтерской отчетности, но не позднее 90 дней со дня государственной регистрации.

При формировании учетной политики промышленное предприятие имеет право самостоятельно:

1. устанавливать порядок начисления износа по основным средствам и нематериальным активам;

2. определять порядок списания затрат по ремонту основных средств на себестоимость продукции;

3. выбирать способ группировки и списания затрат на производство;

4. выбирать вариант синтетического учета производственных запасов;

5. выбирать способ учета выпуска продукции (работ, услуг);

6. выбирать метод оценки производственных запасов, готовой продукции, товаров отгруженных, незавершенного производства;

7. выбирать способ учета затрат на производство;

8. определять сроки погашения расходов будущих периодов;

9. выбирать метод определения выручки от реализации;

10. выбирать момент реализации по работам долгосрочного характера;

11. создавать резерв сомнительных долгов;

12. выбирать способы распределения косвенных расходов между отдельными объектами учета и калькулирования;

13. выбирать метод учета затрат на производство и калькулирования себестоимости продукции;

14. создавать резервы и фонды специального назначения;

15. выбирать способ оценки задолженности по кредитам и займам;

16. выбирать способ учета курсовых разниц.

Учетная политика производственного предприятия предусматривает также самостоятельный выбор формы бухгалтерского учета. Это способы и последовательность учетной регистрации, взаимосвязь и строение учетных регистров. Перечень применяемых учетных регистров тоже выбирается организацией самостоятельно. Учетные регистры представляют собой специальные формы, предназначенные для учетных записей. Различают регистры аналитического и синтетического учета в зависимости от объема их содержания. Регистры также бывают хронологическими и систематическимив зависимости от видов учетных записей. Сейчас в бухгалтерии используются журнально-ордерная, мемориально-ордерная и автоматизированная формы учета [4].

Помимо этого, необходимо оценить величину предстоящих бухгалтерских работ. Разумеется, техническое обеспечение необходимо довести до уровня программного. Но в этом случае (если автоматизация учета проводится с нуля) лучше доводить характеристики компьютера до требований программы, а не наоборот. Не лишним также будет учесть и возможность обслуживания программы, так как большинство типовых программ неизменно требует «подгонки» под деятельность данного

конкретного предприятия. Существует также и еще один фактор, зачастую упускаемый из виду руководством предприятия - это самое обыкновенное удобство. В подобных условиях хозяйственной деятельности двум разным бухгалтерам могут показаться более приемлемыми разные программы. Один просто не в состоянии нормально работать, не имея возможности ввести без программного специалиста необходимые субсчета, а для второго главное – разнообразие справочных отчетов. Если есть возможность, лучше все-таки учесть и индивидуальные особенности будущего пользователя.

Обязательному раскрытию в бухгалтерской отчетности подлежат способы погашения стоимости основных средств и нематериальных активов, оценки товаров, признания прибыли от реализации товаров и т. д.

Статья 6 Федерального закона «О бухгалтерском учете» регламентирует основные требования, предъявляемые к приказу об учетной политике промышленного предприятия, т. е. минимальный объем данных, который должен быть внем отражен. В приказе об учетной политике отражаются следующие моменты бухгалтерского учета:

1) «…рабочий план счетов бухгалтерского учета, содержащий синтетические и аналитические счета, необходимые для ведения бухгалтерского учета всоответствии с требованиями своевременности и полноты учета и отчетности;

2) формы первичных учетных документов, применяемых для оформления хозяйственных операций, по которым не предусмотрены типовые формы первичных учетных документов, а также формы документов для внутренней бухгалтерской отчетности;

3) порядок проведения инвентаризации и методы оценки видов имущества и обязательств;

4) правила документооборота и технология обработки учетной информации;

5) порядок контроля за хозяйственными операциями, а также другие решения, необходимые для организации бухгалтерского учета» [5].

Учетная политика промышленного предприятия утверждается приказом лица, ответственного за организацию и ведение бухгалтерского учета. Подобная формулировка может на первый взгляд указывать и на главного бухгалтера промышленного

предприятия. Но в п. 1 ст. 6 Федерального закона «О бухгалтерском учете» указывается, что «…ответственность за организацию бухгалтерского учета на промышленном предприятии, соблюдение законодательства при выполнении хозяйственных операций несут руководители предприятия».

Таким образом, конечная ответственность за все последствия, вытекающие из хозяйственной деятельности промышленного предприятия, лежит на руководителе предприятия. Создавая новое предприятие, руководитель должен оценить объем предстоящих учетных работ и в зависимости от этого решить, кто будет проводить эти работы, т. е. он может:

1. учредить бухгалтерскую службу как структурное подразделение, возглавляемое главным бухгалтером;
2. ввести в штат должность бухгалтера;
3. передать на договорных началах ведение бухгалтерского учета централизованной бухгалтерии, специализированной организации или бухгалтеру-специалисту;
4. вести бухгалтерский учет лично [6].

От правильного принятия этого решения во многом будет зависеть вся дальнейшая деятельность промышленного предприятия. Неоправданно расширять бухгалтерский штат, разумеется, невыгодно. Но экономия, при которойна сотрудника буквально наваливается объем работ, с которым он просто физически не в состоянии справиться, обязательно приведет к срыву нормального ведения учета и сдачи отчетности. Поэтому правильно оценить объем предстоящих работ по ведению бухгалтерского учета очень важно в самом начале.

Итак, приказ об учетной политике подписан. Но в ходе деятельности промышленного предприятия выясняется, что он требует изменений или дополнений. Тому может быть много причин, это совершенно нормально. Согласно п. 4 ст. 6 Федерального закона «О бухгалтерском учете» причинами изменения учетной политики на промышленном предприятия могут послужить изменения в законодательстве РФ, а также в нормативных актах органов, регулирующих бухгалтерский учет. Это могут быть также и внутренние причины (например, разработка новых способов ведения бухгалтерского учета или значительные изменения в условиях ее деятельности). Соответственно, вносить изменения в утвержденную учетную политику промышленного предприятие можно, но

вышеуказанный Закон ставит одно условие: любые изменения учетной политики должны вводиться с начала финансового года. Кроме того, если изменения в учетной политике не связаны с изменением законодательных актов, они должны быть оценены промышленным предприятием в стоимостном выражении. Эта оценка изменений в учетной политике должна быть произведена на основании выверенных организацией данных на первое число месяца, с которого будут применяться измененные способы ведения бухгалтерского учета. Практически это 1 января года, следующего за годом утверждения нового приказа.

В годовой бухгалтерской отчетности отражаются данные о применении избранной предприятием учетной политики. Они раскрываются в пояснительной записке, являющейся частью бухгалтерской отчетности организациизa отчетный год. Однако, если с момента сдачи последней отчетности, в которой эта информация была отражена, изменений в учетной политике не произошло, бухгалтерская отчетность может не содержать информацию об учетной политике промышленного предприятия [2].

Изменения в учетной политике промышленного предприятия и причины этих изменений, а также оценка последствий этих изменений в стоимостном выражении раскрываются в бухгалтерской документации обособленно.

Универсального решения для всех (или хотя бы большинства) организаций вобласти формирования и раскрытия эффективной учетной политики не существует. Ежегодно, как уже отмечалось выше, требуется производить всесторонний анализ действующих положений учетной политики. Однако нормативное регулирование этих вопросов остается единым для всех организаций, являющихся юридическими лицами по законодательству Российской Федерации (кроме кредитных организаций и бюджетных учреждений) [7].

В условиях нестабильности и противоречивости законодательства крайне сложно создавать достоверную бухгалтерскую отчетность при условии минимизации налоговых рисков. Особенно важным является разработка способов ведения бухгалтерского и налогового учета в нестандартных экономических и правовых ситуациях. Совокупность способов ведения бухгалтерского и налогового учета находит отражение в системе внутренних стандартов. При этом базовым стандартом является учетная политика организации.

Необходимость формирования учетной политики у организации возникает, когда законодательными актами предусмотрено несколько вариантов способов бухгалтерского учета, и организация выбирает один из них: когда законодательство не содержит регламентаций отражения в бухгалтерском учете тех или иных операций и действий, и организация разрабатывает их самостоятельно; когда организация утверждает особенности применения принципов, определенных вышестоящими нормативными документами, исходя из специфик и условий хозяйствования: отраслевой принадлежности, структуры, размеров и т.п.

Учетная политика организации позволяет реализовать организации определенные финансовые задачи, поставленные перед ее администрацией собственниками: минимизация уплачиваемых налогов; привлечение средств инвесторов; другие цели.

Выбор учетной политики должен быть обоснованным, с тем, чтобы в конкретных условиях деятельности организации она наилучшим образом обеспечивала реализацию поставленной задачи и предоставление информации о финансовом положении и результатах деятельности организации.

Изменения в учетной политике возможны, если они целесообразны с точки зрения реальности отражения хозяйственных процессов и финансовых результатов.

Литература

1. 25 Положений по бухгалтерскому учету. – Москва : Проспект, 2016. – 208 с.
2. Банк, С. В. Особенности учетно-аналитического обеспечения финансовой отчетности машиностроительных корпораций / Банк С. В., Банк О. А. // РИСК: Ресурсы, информация, снабжение, конкуренция. - 2013. - № 3. - С. 353-359.
3. Банк, С. В. Формирование учетной политики по учету основных средств / Банк С. В. // Все для бухгалтера. - 2005. - № 7. - С. 17-21.
4. Кузнецова, В. А. Учетная политика / В.А. Кузнецова. - М.: Дело и сервис, 2015. - 144 с.
5. Кондратов, В. Учетная политика 2015. Бухгалтерская и налоговая / В. Кондратов. - М.: АйСи Групп, 2015. - 152 с.
6. Рассказова-Николаева, С. А. Учетная политика 2015 / С.А. Рассказова-Николаева, Е.М. Калинина, О.А. Самойлюк. - М.: Питер, 2016. - 272 с.

7. Учетная политика в 2016 г [Электронный ресурс]. – Режим доступа: http://pravovest-audit.ru – Учетная политика в 2016 г.
8. Содержание учетной политики [Электронный ресурс]. – Режим доступа: http:/www.klerk.ru - Содержание учетной политики.

МАЛЫЙ БИЗНЕС – КАК ФАКТОР РАЗВИТИЯ ЭКОНОМИКИ ЯРОСЛАВСКОГО РЕГИОНА

Слободянюк Евгения Ильинична, студентка 3 курса кафедры Финансов и бухгалтерского учета
Научный руководитель: **Коба Екатерина Евстафьевна**, д.э.н., доцент, заведующий кафедрой Финансов и бухгалтерского учета

В статье рассматриваются критерии отнесения к малому бизнесу, приведено сравнение количества предприятий малого бизнеса в Ярославской области, России и за рубежом. Конкретно речь идет об экономики Ярославского региона, а именно дается анализ направлений деятельности предприятий малого бизнеса, рассматривается объем валовой продукции, недостатки в работе малого бизнеса. Предпринимается попытка найти наиболее успешное направление развития предприятий малого бизнеса в данном регионе и предлагается бухгалтерский аутсорсинг.

Малый бизнес, бухгалтерский аутсорсинг, развитие предприятий малого бизнеса, экономика Ярославского региона.

SMALL BUSINESS AS A FACTOR OF ECONOMIC DEVELOPMENT OF YAROSLAVL REGION

Slobodyanyuk Eugene, 3rd year student of the Department of finance and accounting
Scientific adviser: **Koba Ekaterina**, Doctor of Economic Sciences, Associate Professor, Head of the Department of finance and accounting

The article discusses the criteria for small businesses, the comparison of the number of small businesses in the Yaroslavl region, Russia and abroad. Specifically, we are talking about the economy of the Yaroslavl region, namely the analysis of the activities of small businesses, discusses the gross domestic product, the deficiencies in the operation of small businesses. Attempt to find the most successful direction of development of small businesses in the region and offers accounting outsourcing.

Small business accounting outsourcing, the development of small businesses, the economy of the Yaroslavl region.

«Россия и мир: взгляд в будущее». Под таким названием прошла с 13 по 15 января 2016 г. ежегодная международная научно-практическая конференция «Гайдаровский форум». Форум проводится с 2010 года в память о Егоре Гайдаре, выдающемся ученом-экономисте, идеологе российских реформ начала 1990-х годов. Форум объединяет ведущих мировых ученых и политиков, теоретиков и практиков, представителей финансовых кругов и бизнес-элиты.

В дискуссии Гайдаровского форума - 2016 принимали участие: Дмитрий Медведев, председатель Правительства Российской Федерации; Игорь Шувалов, первый заместитель председателя Правительства Российской Федерации и другие влиятельные эксперты со всего мира.

Дискуссии форума посвящены острейшим проблемам современности. Особое внимание уделяется темам, связанным со стратегической ролью России в мире и осмыслением ее положения. Не малое значение придается также проблемам малого бизнеса.

Актуальность работы заключается в том, что значение малого предпринимательства в рыночной экономике очень велико. Без малого предпринимательства экономика не может ни развиваться, ни функционировать. Трудно представить эффективно развивающийся регион без широкой сети мелких, гибких экономических образований. Так что же такое малый бизнес, и какие предприятия в него входят?

В России деятельность субъектов малого предпринимательства регулируется Федеральным законом 209-ФЗ «О развитии малого и среднего предпринимательства в Российской Федерации» (с последними изменениями от 29.12.2015 №408-ФЗ) принятым 24 июля 2007 года, в котором указаны критерии отнесения предприятия к малому предпринимательству. К малому бизнесу принято относить предприятия с численностью работающих до 100 человек. К категории малого бизнеса относят также микропредприятия (численность работников до 15 человек) и индивидуальных предпринимателей [4].

Следующий важный критерий – это балансовая стоимость активов или выручка от реализации товаров (работ, услуг) без учета

налога на добавленную стоимость (остаточная стоимость основных средств и нематериальных активов) за предшествующий календарный год не должна превышать предельные значения, которые составляют для микропредприятий 60 млн. рублей, для малых предприятий - 400 млн. рублей.

В России доля ВВП, приносимая малым бизнесом, составляет 26,3% от всего ВВП страны, в то время как за рубежом эта цифра достигает 50%. В развитых странах поддержка некрупных предприятий считается стратегически важной задачей для развития экономики. В Ярославской области доля ВВП, приносимая малым бизнесом, составляет всего 0,7% от всего ВВП страны [2].

Как отметил губернатор Сергей Ястребов, малый бизнес дает четверть валового регионального продукта Ярославской области и оказывает серьезное влияние на экономическую ситуацию в регионе, а также на обеспечение стабильности на рынке труда.

Рассмотрим и сравним количество малых предприятий в России и других развитых странах, на примере Германии и США (Рисунок 1). В России насчитывается 2,1 млн. малых предприятий, это около 25% от всех предприятий страны. В Германии 3,5 миллиона малых предприятий, и это составляет почти 80% всех предприятий страны. В США насчитывается около 10 млн. предприятий малого бизнеса. Американская статистика показывает, что сейчас в США 99% от всех предприятий - это компании малого бизнеса, но эти данные не могут сравниваться с Россией и Европой, так как показатели разделения предприятий сильно отличаются. Европейцу сложно понять, как казино, которое приносит выручку не менее 32,5 млн долларов США в год, рассматривается как малый бизнес.

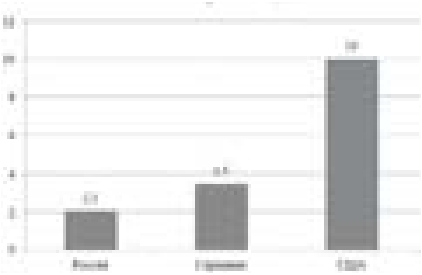


Рисунок 1 – Количество предприятий малого бизнеса, млн. единиц

В Ярославской области по состоянию на 1 июля 2015 года, как видно на рисунке 2, осуществляли хозяйственную деятельность 52026

субъектов малого предпринимательства (это 94,5% от всех субъектов предпринимательства в Ярославской области), в том числе:

•19509 микропредприятий (38%);

•2351 малое предприятие (4%);

•30116 индивидуальных предпринимателей (58%).

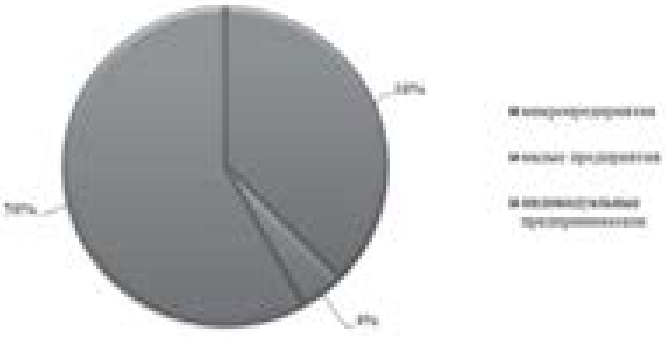


Рисунок 2 – Субъекты малого предпринимательства в Ярославской области

Количество субъектов малого предпринимательства, по сравнению с 2013 годом, в целом снизилось на 14,6%, количество индивидуальных предпринимателей выросло на 3,4% (Всего в 2013 году насчитывалось 54800 субъектов малого предпринимательства, из них: 23088 микропредприятий; 2547 малых; 29165 индивидуальных предприятий).

Малый предприниматель вправе заниматься весьма широким спектром видов деятельности, который охватывает многие отраслевые экономические сегменты. В Ярославской области структурное распределение малого бизнеса по видам экономической деятельности, в основном, соответствует общероссийской ситуации (Рисунок 3). Часть экономики региона, в которой традиционно доминируют малые предприятия – это сфера торговли и услуг.

Около 29% малых предприятий занимаются оптовой и розничной торговлей, порядка 19% действуют в сфере услуг (здравоохранение, социальные услуги, операции с недвижимым имуществом, наука, информационные технологии и др.). В промышленности занимается 19% предприятий (добывающие и обрабатывающие производства, производство и распределение электроэнергии, газа и воды). В строительстве сосредоточено 13,5%,

сельским и лесным хозяйством занимается 7,5%, 4,4% – гостиничным бизнесом, около 4% – транспортом и связью, 3,6% - прочие виды деятельности [3].

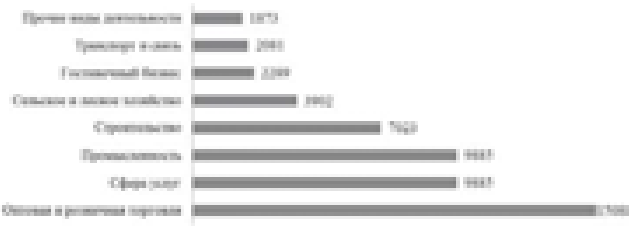


Рисунок 3 – Структурное распределение малого бизнеса по видам экономической деятельности в Ярославской области

Исходя из приведенных данных, приходится констатировать тот факт, что непроизводственная сфера по-прежнему более привлекательна, чем реальный сектор экономики. В малом предпринимательстве преобладают фирмы ориентированные на узкий рынок и сферу с быстрой оборачиваемостью капитала, а так же фирмы с невысокими инвестиционными возможностями [5].

На данное структурное распределение малого бизнеса в Ярославской области наибольшее влияние оказывают такие факторы, как:

•недостаток собственных финансовых ресурсов для развития бизнеса;

•сложность получения банковских кредитов;

•неразвитость инфраструктуры для поддержки малого предпринимательства;

•недостаток квалифицированных кадров, знаний и информации для ведения предпринимательской деятельности;

•сложные стартовые условия для начала бизнеса;

•низкая производственная активность малого бизнеса.

С целью снижения влияния вышеуказанных негативных факторов на предпринимательское сообщество, департаментом инвестиционной политики Ярославской области реализуется подпрограмма государственной программы «Экономическое развитие и инновационная экономика в Ярославской области» на 2014 – 2020 годы «Областная целевая программа развития субъектов малого и среднего предпринимательства Ярославской области на 2013 – 2015 годы».

Проведя анализ вышеперечисленных факторов, и, учитывая

направление моей подготовки «Экономика: бухгалтерский учет», считаю, что одним из секторов малого бизнеса является бухгалтерский аутсорсинг. Сама я родом из Ярославской области, поэтому считаю, что данное направление малого бизнеса в этом регионе будет успешно развиваться.

В российском законодательстве понятие аутсорсинга отсутствует. Термин «аутсорсинг» заимствован из английского языка (от английского «outsourcing») и дословно переводится как использование чужих ресурсов. Бухгалтерский аутсорсинг подразумевает передачу функций по составлению отчетности аутсорсеру, а также по организации и ведению бухгалтерского учета. То есть аутсорсинг бухгалтерии - это возможность перепоручить учет всех финансовых вопросов сторонней организации [1, С. 168].

Стоит отметить, что данный вид услуг – это совсем не новое направление в бизнесе. В Европейских странах рынок бухгалтерского аутсорсинга достиг степени своего развития, которая позволила 86% предприятий отказаться от услуг штатного бухгалтера. В США данный показатель составляет 92%, в Израиле – 96%. Рынок аутсорсинга в России все еще находится на стадии формирования. По оценкам маркетологов, на данный момент объем рынка бухгалтерского аутсорсинга составил 40%. Такой показатель наглядно демонстрирует перспективность данного направления. Как показывает статистика, на сегодняшний день бухгалтерский аутсорсинг наибольшей популярностью пользуется среди предприятий оптовой и розничной торговли. На их долю, от общего объема рынка аутсорсинга, приходится 80%.

Сравнение международной и отечественной практик по передаче ведения бухгалтерского учета на аутсорсинг позволило установить отставание масштабов и качества таких услуг в России. Причинами такого отставания могут быть:

- отсутствие научно обоснованных методик организации бухгалтерских аутсорсинговых услуг;
- высокий риск потери конфиденциальной информации;
- отсутствие опыта работы с аутсорсерами и недостаточный уровень качества продвижения аутсорсинговых услуг.

На рисунке 4 приведена схема аутсорсинг-проекта по организации бухгалтерского учета на условиях дистанционного обслуживания.

На первом этапе осуществляется предварительное ознакомление с потребностями клиента в бухгалтерском аутсорсинге, особенностями его бизнеса (специализация, масштаб бизнеса, численность персонала, объем документооборота, наличие структурных и обособленных подразделений), заключается договор на оказание услуг по ведению бухгалтерского учета на условиях дистанционного обслуживания.

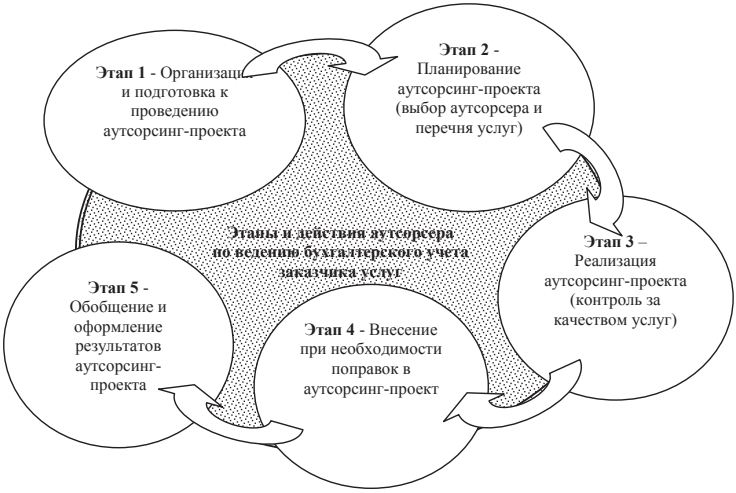


Рисунок 4 – Внутрифирменный регламент аутсорсинг-проекта бухгалтерского учета на условиях дистанционного обслуживания

На втором этапе определяются комплекты рабочих документов аутсорсера для аккумулирования информации о фактах хозяйственной жизни заказчика услуг и дистанционного ведения бухгалтерского учета и осуществления контроля за формированием отчетности.

На третьем этапе формируются рабочий План счетов, учетные регистры, разрабатывается учетная политика для финансовых и налоговых целей, совершаются учетные действия, формируется финансовая и налоговая отчетность.

На четвёртом этапе готовится письменная информация для руководства заказчика бухгалтерских аутсорсинговых услуг в форме сводного отчета по аутсорсинг-проекту бухгалтерского учета на условиях дистанционного обслуживания, оцениваются результаты работы аутсорсера.

На пятом этапе обобщаются результаты выполнения аутсорсинг-проекта, принимаются управленческие решения о продлении или прекращении договора на оказание услуг бухгалтерского аутсорсинга.

Несмотря на то, что бухгалтерские аутсорсинговые услуги нематериальны, в целях улучшения качества услуг, предоставляемых коммерческим организациям аутсорсинговая компания должна выработать четкую стратегию.

Таким образом, в современный период развитие малого предпринимательства имеет особое значение для Ярославской области и для России в целом. Именно малые предприятия, не требующие крупных стартовых инвестиций и гарантирующие высокие обороты ресурсов, способны наиболее быстро и экономно решать проблемы реструктуризации экономики, формирования и насыщения рынка потребительских товаров в условиях дестабилизации российской экономики и ограниченности финансовых ресурсов.

Литература

1. Аникин, Б. Аутсорсинг и аутстаффинг: высокие технологии менеджмента. учебное пособие. второе издание, переработанное и дополненное [ТЕКСТ] / Б. Аникин, И. Рудая // ИНФРА-М. – 2014. – 320 С.
2. Информация о состоянии малого и среднего предпринимательства Ярославской области. Портал органов государственной власти. Электронный ресурс. Режим доступа: http://www.yarregion.ru/depts/der/pages (дата обращения: 03.02.2016)
3. Территориальный орган Федеральной службы государственной статистики по Ярославской области. Малое и среднее предпринимательство. Электронный ресурс. Режим доступа: http://yar.gks.ru/wps/wcm/connect/rosstat_ts/yar/ru/statistics/enterprises/ (дата обращения: 15.12.2015)
4. Федеральный закон от 24.07.2007 N 209-ФЗ (ред. от 29.12.2015) «О развитии малого и среднего предпринимательства в российской федерации». электронный ресурс. режим доступа: http://www.consultant.ru/document/ cons_doc_law_52144/ (дата обращения: 26.01.2016)

5. Коба Е.ЕВГ. Организация и ведение бухгалтерского и налогового учета в сфере оказания услуг по ремонту и техническому обслуживанию автотранспортных средств [текст] / Коба Е.ЕВГ.// Научно-практический и теоретический журнал «Все для бухгалтера». – 2008. - №5 (221) - С.24-35.

АНАЛИЗ РЫНКА ТРУДА РФ В УСЛОВИЯХ НЕСТАБИЛЬНОЙ ЭКОНОМИКИ И ПУТИ СОВЕРШЕНСТВОВАНИЯ

Уварова Оксана Валериевна, студентка 3 курса кафедры Финансов и бухгалтерского учета
Научный руководитель: **Овсийчук Вадим Ярославович**, д.э.н., профессор кафедры Финансов и бухгалтерского учета

Благополучное экономическое развитие страны, а также улучшение уровня жизни населения Российской Федерации напрямую связано с эффективным функционированием рынка труда. Нестабильная экономика России оказывает на него непосредственное влияние, следовательно, данный рынок нуждается в стабилизации и оптимизации. В данной статье приведен анализ таких показателей, как численность уровня населения, динамика безработицы, заработной платы, реальных доходов населения и прожиточного минимума. А также представлены возможные варианты совершенствования рынка труда.

Рынок труда, занятость населения, уровень жизни, доходы.

THE ANALYSIS OF LABOR MARKET OF THE RUSSIAN FEDERATION IN THE CONDITIONS OF UNSTABLE ECONOMY AND WAYS OF IMPROVING

Uvarova Oksana, 3rd year student of the Department of finance and accounting
Scientific adviser: **Ovsiichuk Vadim,** Doctor of Economic Sciences, Professor of the Department of finance and accounting

Successful economic development of the Russian Federation and improving the living of the Russian population is directly connected with effective functioning of the labor market. The unstable economy exerts direct impact on it, therefore, this market needs to stabilize and optimize. The analysis of such indicators as number of the population, dynamics of unemployment, salary, real income of the population and living standard

is provided in this article. Moreover, possible options for improving the labor market are presented.

Labor market, employment of the population, standard of living, income.

В настоящее время состояние современного рынка труда Российской Федерации крайне подвержено влиянию как экономических, так и политических событий. Сюда относятся и присоединение Крыма, и санкции Запада, и рост цен, и остающийся высоким уровень безработицы, и события в Украине, и многое другое. В данных условиях нестабильной экономики возрастает необходимость анализа и прогнозирования динамики изменения рынка труда. Так как рынок труда России – важнейшее составляющее рыночной экономики. Его можно назвать индикатором благополучия отдельного гражданина и страны в целом. Это связано в первую очередь с возможностью выделить наиболее развитые отрасли страны и наиболее уязвимые. В совокупности немаловажную роль играет анализ показателей, таких как среднемесячная заработная плата, МРОТ и прожиточный минимум, именно они характеризуют социальное и финансовое положение страны. В связи с этим нами был проведен анализ РФ с разбивкой по субъектам и секторам экономической деятельности, а также анализ динамики среднемесячной номинальной заработной платы и реальных доходов населения за промежуток времени с 2011 по 2015 год.

Целью данной работы является решение следующих задач:

1. Выявление проблем рынка труда.
2. Разработка путей совершенствования рынка труда.

В связи с информацией Росстата ниже представлены данные (рис.1), которые характеризуют численность занятого постоянного населения России в период 2014-2015 гг.

Рисунок 1 - Динамика численности экономически активного населения РФ 2014-2015 (млн. чел.)

Относительно занятого населения, численность рабочих росла до августа 2015 года включительно (73,3 млн. человек), превысив отметку прошлого года на 1,3%, и далее опять начала снижаться. Таким образом, к концу 2015 года численность экономически активного населения России составила 76,7 миллиона человек, в том числе занятого - 72,3 млн. и безработных – 4,4 млн. человек [5].

Рассмотрим более подробно данные по безработице. В течение последних лет безработица в Российской Федерации имеет тенденцию к снижению. По данным Федеральной службы государственной статистики России, в начале 2011 года безработица была на уровне 7,8%, на конец 2015 года она составила 5,8% (рис.2). В период с начала осени 2014 года и до конца 2015 года произошел рост безработицы, в основном это связано с многочисленным сокращением персонала на предприятиях. Средний уровень безработицы по итогам 2015 года составил 5,6%.

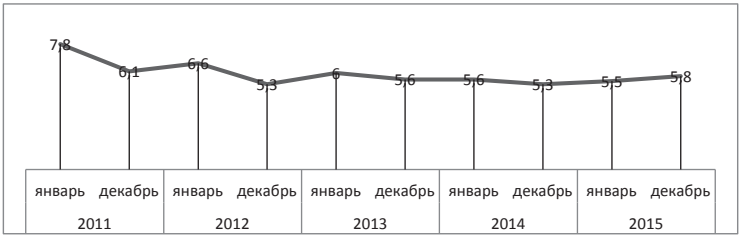


Рисунок 2 - Динамика уровня безработицы 2011-2015 (в %)

Вопреки тенденции к снижению, вопрос, связанный с безработицей не стал легче. Появился огромный дефицит в квалифицированных рабочих, особенно на промышленных производствах, в сферах жилищно-коммунального хозяйства и на предприятиях строительной отрасли. Главной причиной данного дефицита стало более доступное высшее образование. Возросло количество высших заведений, в частности негосударственных, которые готовы предоставить выпускникам диплом о высшем образовании. Молодым специалистам не хватает практики, так как работодатели в основном заинтересованы в более опытных кандидатах. По мнению Кадровых агентств России ещё одна немаловажная причина заключается в «неадекватной миграционной политике государства». Её основная мысль выражается в том, что работодатели предпочитают не высококвалифицированных работников, а дешевую рабочую силу. В связи с действующей

системой законов, намного выгоднее стало нанимать мигрантов нежели коренного жителя с нужными навыками и квалификацией [2].

Люди начинают задумываться о смене работы или кардинально профессии. Какие же профессии будут востребованы на рынке труда в 2016 году? По мнению руководителя службы исследований портала HeadHunter Марии Игнатовой, список профессий останется неизменным по сравнению с 2015 годом [1]. К ним относятся бухгалтера, менеджеры по работе с персоналом и по продажам, торговые представители, мерчендайзеры, юристы, секретари, офис-менеджеры, операторы колл-центров и кладовщики. Эксперты считают, что работодатели в новом году будут более тщательно подходить к выбору кандидатов. Для устройства на работу придется пройти не одно собеседование. Не секрет, что соискатели работы, которые готовы поменять свое место жительства, в первую очередь обращают внимание на среднюю заработную плату в различных городах и регионах, чтобы подобрать наиболее прибыльное место работы, а также приблизительно рассчитать ожидаемые выплаты. Так как именно средняя заработная плата является главным показателем уровня достатка населения (рис.3).

Рисунок 3 - Среднемесячная номинальная заработная плата по субъектам РФ в 2015 году (в руб.)

Исходя из данных Федеральной службы государственной статистики за последние 5 лет среднемесячные заработные платы ежегодно увеличиваются. В начале 2011 года средняя зарплата составляла 32809 рублей, к концу 2015 года её значение достигло рекордной отметки на сегодняшний день 42684 рубля (рис. 4). По сравнению с 2014 годом произошел рост на 3,8% [3].

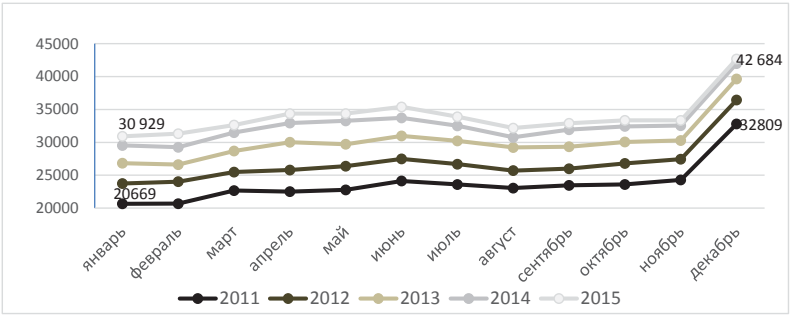


Рисунок 4 - Динамика среднемесячной номинальной заработной платы 2011-2015 (в руб.)

Что касается реальных располагаемых денежных доходов населения, в конце 2014 года наблюдалось снижение на 7,3% по сравнению с соответствующим периодом 2013 года. В среднем за 2015 год – денежные поступления населения уменьшились на 9% (рис. 5). В течение всего года изменение доходов по сравнению с предыдущим периодом было нестабильно, однако в декабре 2015 года произошел значительный рост на 27% по сравнению с предыдущем месяцем.

Рисунок 5 - Динамика среднемесячной реальной заработной платы в 2015 году (в %)

Среднемесячная номинальная заработная плата является основным фактором дифференциации населения по доходам. По данным 2015 года самый низкий уровень наблюдается в сельском хозяйстве и в гостиничном и ресторанном бизнесе, хотя в этих отраслях преобладают одни из самых тяжелых условий для работы (рис. 6). Более прибыльными отраслями в данном году стали

финансовая деятельность, добыча полезных ископаемых, а также сфера рыболовства.

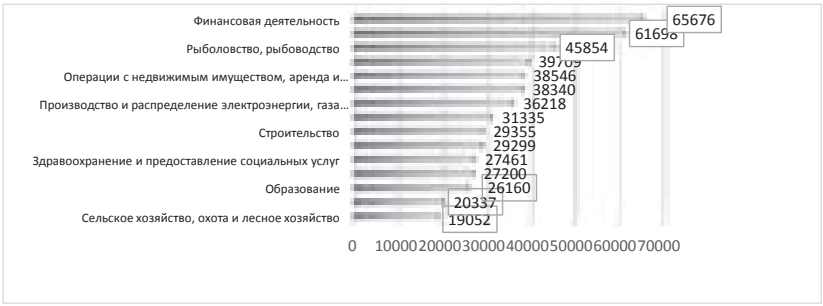


Рисунок 6 - Среднемесячная номинальная заработная плата по видам деятельности РФ в 2015 году (в руб.)

Стремительное возрастание цен служит первостепенной причиной для увеличения прожиточного минимума. Ибо именно он служит гарантией поддержки государством каждого гражданина Российской Федерации. Естественно в различных регионах уровень прожиточного минимума очень сильно колеблется. Однако рассмотрим среднюю тенденцию по России (рис. 7). Оба показателя за данный период несомненно возросли. К концу 2015 года ставка МРОТ равняется 5965 рублей. Что касается прожиточного минимума, с 2011 года заметно увеличение, свое высшее значение (10017 рублей) он достиг во 2 квартале 2015 года.

Рисунок 7 - Соотношение прожиточного минимума и МРОТ в РФ (в руб.)

На современном рынке труда прожиточный минимум обычно должен служить базой для определения минимальной ставки заработной платы. Однако Россия пока ещё не достигла равномерного соотношения между этими показателями, хотя постепенно стремится к этому. На данном графике показано, что

уровень минимального размера оплаты труда находится выше прожиточного минимума, особенно во 2 квартале 2015 года, где данное превышение достигает почти 50%. По обещаниям Министерства труда и социальной защиты Российской Федерации с 1 октября 2015 года МРОТ должен был составить 89% от стоимости прожиточного минимума, с 1 октября 2016 – 94% и дойти до 100% в 2017 году [4]. Однако в последующем периоде стало ясно, что достичь поставленных целей не удастся. Тогда чиновники предложили другой план, поставив новый рубеж – 65% в 2017 году. Выход на обещанные 100% теперь следует ожидать к 2020 году.

Важный и, безусловно, незаменимый орган по вопросам регулирования рынка труда и защите интересов рабочей силы – Международная организация труда. В её обязанности входит разработка международных трудовых норм в виде рекомендаций и конвенций, установление минимальных стандартов в области основных трудовых прав, анализ проблем современного общества и многое другое. Данная организация призывает государство к сосредоточению своих усилий на мерах, которые будут поддерживать уровень занятости населения, обеспечивать доступ рынка труда и облегчать процесс смены работы. Для данных целей необходимо сформировать новые и укрепить уже существующие государственные службы занятости и другие институты рынка труда, увеличить объем инвестиционных ресурсов для повышения уровня квалификации работников, повысить качество жизни благодаря стабилизации уровня реальных доходов, реформировать систему оплаты труда для заинтересованности работников в ожидаемом результате и обеспечить доступ к качественному образованию и обучению для подготовки более опытных и квалифицированных специалистов с помощью различных тренингов, волонтерства и бесплатных стажировок. Таким образом, данные меры помогут обеспечить совершенствование современного рынка труда. Ибо только эффективное действие рынка труда является оптимальным вариантом увеличения занятости населения и благополучного экономического развития страны.

Литература

1. HeadHunter - Электронный ресурс. Режим доступа: http://hh.ru/ (дата обращения: 26.02.2016)
2. Кадровые агентства России - Электронный ресурс. Режим доступа: https://person-agency.ru/ (дата обращения: 24.02.2016)

3. РБК-Quote - Электронный ресурс. Режим доступа: http://quote.rbc.ru/macro/ (дата обращения: 24.02.2016)
4. КонсультантПлюс - Электронный ресурс. Режим доступа: http://www.consultant.ru/ (дата обращения: 25.02.2016)
5. Федеральная служба государственной статистики - Электронный ресурс. Режим доступа: http://www.gks.ru/ (дата обращения: 24.02.2016)

КАФЕДРА ЭКОНОМИКИ

ИННОВАЦИОННОЕ ОБРАЗОВАНИЕ В ВЫСШЕЙ ШКОЛЕ

Бордачева Марина Николаевна, студентка 2 курса кафедры Экономики
Научный руководитель: **Рыжкова Татьяна Васильевна,** к.э.н., доцент кафедры Экономики

В статье исследуются технологии и методы подготовки специалистов для инновационной экономики, качество и уровень образования в высшей школе, степень его инновационности.

Инновационное образование, компетенции, инновационные методы обучения, образовательные технологии.

INNOVATIVE EDUCATION AT HIGHER SCHOOL

Bordacheva Marina, 2nd year student of the Department of economics
Scientific adviser: **Ryzhkova Tatyana,** Candidate of Economic Sciences, Associate professor of the Department of economics

The article examines the technologies and methods of training specialists for innovation economy, the quality and level of education in the graduate school, the degree of innovativeness.

Innovative education, competence, innovative teaching methods, educational technologies.

Высшее образование - это - то основание, на котором формируются национальные кадры и потенциал развития страны. От того, насколько эффективно работает эта система, зависит, насколько успешно будет развиваться любая национальная экономика.

Образование является приоритетным направлением и основным индикатором развития во всех цивилизованных странах мира. В национальной инновационной системе одно из центральных мест принадлежит образованию, которое обеспечивает ее кадрами, необходимой квалификации и компетентности (рисунок 1).

Определения инновационного образования характеризуются многообразием и отличаются по содержанию. Инновационное образование определено нами как образование, не столько ориентирующееся на передачу знаний, сколько позволяющее овладеть базовыми компетенциями для самостоятельного получения знаний.

Рисунок 1 - Национальная инновационная система

Приоритетной задачей высшего образования должно стать приведение содержания и структуры профессиональной подготовки кадров в соответствие с современными потребностями личности, общества и рынка труда, повышение доступности качественных образовательных услуг, создание независимой оценки контроля качества образования [5].

Для более полного изучения понятия инновационного образования в вузе необходимо уточнить его понятийный аппарат, который характеризует следующие терминологические понятия: инновационное обучение, инновационные методы, формы и технологии обучения, инновационная образовательная среда и главный компонент инновационного образования - компетентностный подход (рисунок 2).

В условиях перехода на образовательный стандарт ФГОС 3+ и 3++ компетентностно-ориентированная модель подготовки конкурентоспособного специалиста в вузе должна опираться на триединство взаимосвязанных составляющих – образование, науку и производство (рисунок 3). В этой модели образованию отводится роль активного звена. На основе расширения горизонтов и перспектив в создании и применении инновационных технологий использование такой модели позволит выйти на новый уровень разработки образовательных программ, повысить эффективность образовательной деятельности во всех направлениях - разработки

учебных программ и планов, обучения, проектной работы, НИР, обеспечить выпускнику конкурентные преимущества в условиях реализации инновационной стратегии развития [3].

Компонент	Сущность

Рисунок 2 - Компоненты инновационного образования

Рисунок 3 - Модель подготовки специалиста для инновационной экономики

Особое значение в формировании профессиональных качеств современного специалиста имеет внедрение в учебный процесс инновационных технологий обучения. Их следует рассматривать как инструмент, с помощью которого новая образовательная парадигма может быть претворена в жизнь.

Под инновационными педагогическими технологиями понимаются такие, реализация которых приводит к повышению эффективности процесса обучения. В настоящее время наибольший интерес представляют развивающее и активное обучение, обучение развитию критического мышления, обучение в сотрудничестве и проблемное обучение.

Многие технологии обучения продолжают оставаться слабо проработанными и не до конца освоенными. Нужно отслеживать, где они дают сбои, где неэффективны и даже мешают достижению промежуточных и конечных целей образовательного процесса, чтобы своевременно корректировать их.

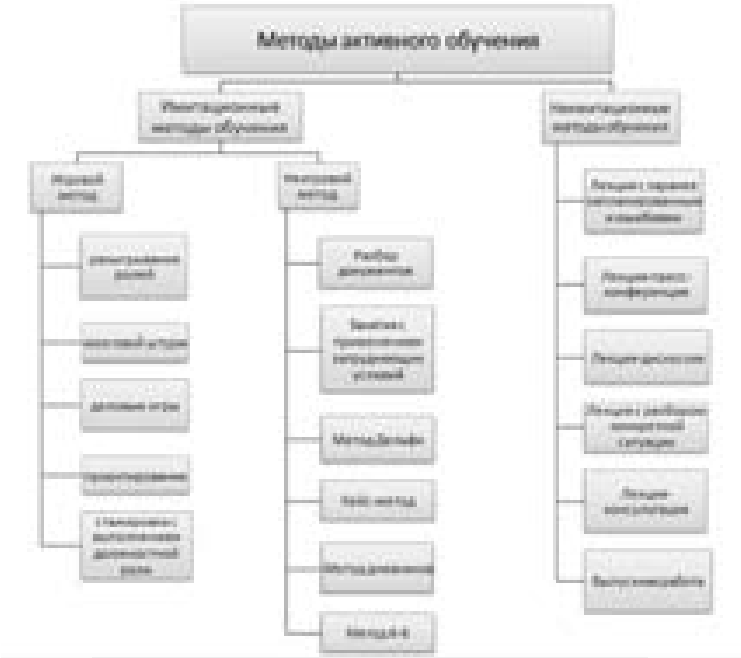


Рисунок 4 - Методы активного обучения

В настоящее время используется большое количество инновационных методов обучения и существует множество их классификаций. Одна из них - по источнику получения знаний, в основу которой положено существование трех источников знаний: слово, наглядность, практика. Соответственно выделяют словесные методы - источником знания является устное или печатное слово; наглядные методы - источниками знания являются наблюдаемые

предметы, явления, наглядные пособия; практические методы - знания и умения формируются в процессе выполнения практических действий.

В процессе обучения используются, как традиционные, так и инновационные методы обучения. Развивая инновационные методы обучения, целесообразно сочетать их с традиционными, которые не менее действенны.

Экономическое образование - образование особое. Кроме определенного запаса знаний и умений студент должен приобрести в учебном заведении элементарные навыки принятия научно обоснованных решений в разных, нередко экстремальных, ситуациях. Этого не обеспечивают пассивные методы обучения, предлагая студентам делать доклады и рефераты. Необходимо активное обучение, основанное на постановке жизненно-важных задач, требующие одновременно применения теоретических знаний и быстрого выполнения практических действий (рисунок 4). Это - деловая игра, кейс-метод, занятия с применением затрудняющих условий, метод 6-6, метод дневников [9].

Изменение социальной, экономической и политической ситуации в стране привело к модернизации российской системы образования, к актуализации компетентностного подхода в обучении. Квалификация выпускника определяется не уровнем знаний и умений в предметной области знаний, а сформированностью базовых компетенций.

Несмотря на разнообразие точек зрения, большинство ученых понимают компетенцию как способность и готовность индивида на основе приобретенных знаний и умений справляться с различными профессиональными задачами.

Анализ литературы показывает, что в настоящее время нет однозначной типологии компетенций, которые нужно формировать у обучающихся [9]. По мнению А. В. Хуторского, к ним в первую очередь следует относить ценностно – смысловую компетенцию, которая рассматривается, как способность ставить личные цели, понимать и осознавать смысл своей деятельности; общекультурную – способность ориентироваться в культурном пространстве; учебно – познавательную – способности, которые человек развил в себе благодаря познавательности; информационную – способность самостоятельного поиска, анализа, отбора и передачи необходимой информации; социально – трудовую – способность осуществлять

взаимодействие с социальными институтами, выполнять социальные роли; коммуникативную компетенцию, как способность взаимодействовать с окружающими людьми и работать в команде.

Компетенции экономиста должны быть основаны на фундаментальной экономической подготовке, которая является необходимой профессиональной базой. Но профессионал в области экономики должен не просто знать теоретические основы, а свободно ориентироваться в них, применять теорию на практике. Это значит, что он должен быть весьма компетентен в вопросах экономической теории [6, 7].

Развитие рыночных отношений и их динамизм повышает требования к уровню подготовки специалистов экономического профиля и обуславливает необходимость расширения их знаний и умений. Наряду с узкопрофессиональными умениями они должны владеть методологией планирования, учета и анализа деятельности предприятия, знать планово-учетную документацию, методы экономического анализа и моделирования экономических процессов и явлений [3, 4].

В условиях рынка специалисты-практики экономического профиля должны быть способны на основе комплексной и достоверной информации определить альтернативные варианты действий и экономически обосновать их целесообразность, планировать деятельность предприятия во времени и пространстве, определять фактическую себестоимость продукции, работ, услуг и прогнозировать динамику изменения ее уровня в перспективе.

Роль знаний в современной экономике, достаточно наглядно продемонстрировали исследования, проведенные в странах ЕС, которые показали, что предприятия, которые интеллектуальный капитал считают базой стратегического развития, получают в среднем не менее 61% прибыли от основной деятельности. Знания и информация выступают неисчерпаемыми ресурсами, активно формирующими ВВП любой страны. Важным условием доступа к этому ресурсу являются способности отдельного человека к познавательной деятельности, приобретаемые путем качественного образования [1].

Внедрение компетентностного подхода в систему высшего профессионального образования направлено на улучшение взаимодействия с рынком труда, повышение конкурентоспособности

специалистов, обновление содержания, методологии и соответствующей среды обучения [2].

Для оценки удовлетворенности образовательным процессом, его содержанием и качеством было проведено обследование студентов «МГОТУ» методом анкетирования. В опросе приняли участие 90 студентов, 69% из них - девушки.

Организацию учебного процесса в вузе студенты оценили достаточно высоко – на 4 балла по 5-балльной шкале. Содержанием образовательной программы и методами обучения удовлетворены 75% опрошенных студентов. На вопрос о соотношении между собой программы курсов и учебного графика 78% студентов выбрали ответ «да». Наличием современных информационных технологий, используемых в учебном процессе, и их доступностью в университете удовлетворены 84% студентов.

Использование преподавателями инновационных технологий на занятиях положительно оценили 71% студентов. На получение профессиональных знаний и умений специалиста в большой степени влияет усвоение учебного материала. 62% респондентов не всегда понимают учебный материал.

Одним из основных аспектов профессионального становления специалиста является педагогическая практика. 59% студентов испытывают недостаток практических знаний и умений для эффективной деятельности в будущем.

Инновационное образование направлено на развитие у студентов желания учиться на протяжении всей жизни. Для этого нужны соответствующие условия в университете. 97 % респондентов удовлетворены образовательной средой.

Целью высшего образования является подготовка студентов для профессиональной деятельности. 37% опрошенных студентов «МГОТУ» считают выпускников ВУЗа не подготовленными к труду в современных условиях.

Особого внимания заслуживают предложения студентов, касающиеся укрепления учебной дисциплины в части посещаемости занятий. Высокая доля участников опроса высказалась за перекличку на лекциях и семинарах, отработку пропущенных занятий (теоретических и практических), ограничение допустимого числа пропусков без уважительной причины. За увеличение контроля посещаемости занятий со стороны деканата высказались 27%, 13% -

за увеличение количества тем для самостоятельного изучения и 14% учащихся - за ужесточение требований промежуточной аттестации.

Наиболее существенными недостатками, по мнению студентов, в деятельности вуза являются: недостаточное количество выделяемых часов для наиболее значимых предметов; качество преподавания; несоответствие изучаемых дисциплин получаемой специальности.

Применение инноваций в вузе способствует повышению качества образования - с этим утверждением согласны 86% студентов.

Проведенное исследование показало, что одним из факторов, сдерживающих развитие инновационного образования в ВУЗе, является сопротивление обучающего персонала инновациям.

В соответствии с «Положением о нормах времени для планирования всех видов нагрузки ППС «МГОТУ» преподаватель в должности доцента работает на 1,5 ставки по 9 ч ежедневно. Несмотря на то, что норма рабочего времени, установленная федеральным законом, составляет только 36 часов в неделю. Однако фактическое значение продолжительности рабочей недели преподавателя соответствует 46 часам, что на 28% превышает норму и является недопустимым. На самом же деле многие педагоги работают значительно больше.

На подготовку к занятию преподавателю выделяется от 12 до 36 минут, а на написание учебного пособия 12 минут на 1 страницу. Имея такую перегрузку, преподаватель не может быть полноценным участником процесса инновационного образования, у него совершенно не остается времени ни на научную деятельность, ни на свое развитие. Он стал «рабочим у станка образования».

Для повышения качества высшего образования и приведение в соответствие его статуса инновационности, нами выдвинуты предложения:

- создания многоуровневого и многоступенчатого образования;
- урегулирования отношений системы образования и промышленной сферы экономики;
- изменения организации труда преподавателей и снижение их нагрузки;
- обучения ППС на курсах повышения квалификации на тему инновационного образования в ВУЗе;
- совершенствования ФГОС 3+;
- использования технологии практико - ориентированного

обучения;

- формирования инновационной образовательной среды ВУЗа;
- развития интеграционных процессов и междисциплинарных связей.

Систематическая работа по совершенствованию учебного процесса позволит достичь позитивного результата – высокое качество конечного продукта – экономистов – профессионалов, соответствующих требованиям времени. Современное предприятие испытывает потребность в работниках, способных брать на себя ответственность за результаты профессиональной деятельности, требуется новое качество профессионалов – компетентность как определенный уровень квалификации – умение принимать решения, исполнять и отвечать за них.

Литература

1. Лучицкая, Л.Б., Збышко, Б.Г. Социальная ответственность как фактор гармонизации регионального рынка труда и профессионального образования [Текст] / Л.Б. Лучицкая, Б.Г. Збышко // «Труд и социальные отношения» Наука Практика Образование. – 2012. – №5 (95). – С.45-54.
2. Проблемы реализации компетентностного подхода в высшей школе. Электронный ресурс. Режим доступа: http://www.tsutmb.ru/problemyi-realizaczii-kompetentnostnogo-podxoda-v-vyisshej-shkole?template=9 (дата обращения: 23.01.2016).
3. Рыжкова, Т.В., Колесниченко, К.В. Венчурное предпринимательство в системе инновационного развития экономики [Текст] / Т.В. Рыжкова, К.В. Колесниченко // Вестник Московского государственного университета леса - Лесной вестник. – 2010. – № 2(71). – С.164-169.
4. Рыжкова, Т.В., Колесниченко, К.В. Методы оценки венчурных предприятий [Текст] / Т.В. Рыжкова, К.В. Колесниченко // Вестник Московского государственного университета леса - Лесной вестник. – 2011. – №6(82). – С. 161-164.
5. Рыжкова, Т.В. Подготовка бакалавров для инновационной экономики [Текст] / Т.В. Рыжкова // Сборник трудов по материалам Международной научно-практической Интернет-конференции: Современные образовательные технологии, используемые в очном, заочном и дополнительном образовании. – 2013. – С. 320-334.
6. Рыжкова, Т.В. Теоретические аспекты экономической оценки эффективности деятельности предприятия [Текст] / Т.В. Рыжкова //

Вестник Московского государственного университета леса - Лесной вестник. – 2013. – № 4 (96). – С. 201-205.
7. Рыжкова, Т.В., Лаптев, Г.А. Экономическая эффективность труда: теоретические и методологические аспекты определения и оценки [Текст] / Т.В. Рыжкова, Г.А. Лаптев // Сборник статей открытой научно-практической конференции преподавателей кафедры экономики: Современная экономика: проблемы, пути решения – М.: ООО «Научный консультант». – 2015. – 204 с. – С 35-50
8. Современная образовательная среда проектной деятельности студентов. Электронный ресурс. Режим доступа: http://www.intuit.ru/studies/courses/14627/1291/lecture/25035 (дата обращения: 15.01.2016).
9. Хуторской, А.В. Определение общепредметного содержания и ключевых компетенций как характеристика нового подхода к конструированию образовательных стандартов [Текст] /А.В. Хуторской Компетенции в образовании: опыт проектирования: сб. науч. тр. // М.: Научно – внедренческое предприятие «ИНЭК». – 2007. – С.12-20.

ОБЗОР СОСТОЯНИЯ ПРОИЗВОДСТВА ИМПОРТОЗАМЕЩЕНИЯ ПРОДУКЦИИ НА ОТЕЧЕСТВЕННЫХ ПРЕДПРИЯТИЯХ

Буркина Анастасия Андреевна, студентка 4 курса кафедры Экономики
Научный руководитель: **Бронникова Тамара Семеновна**, к.э.н., доцент кафедры Экономики

В статье предлагается рассмотреть актуальную на сегодняшний день проблему импортозамещения. Данная стратегия направлена на рост конкурентоспособности отечественной продукции путем замещения импортных товаров отечественной продукцией. Такая политика даст возможность уменьшить зависимость экономики страны от импорта.

Импортозамещение, экспорт, импорт, различные сферы экономики, отечественные производители.

AN OVERVIEW OF THE STATUS OF PRODUCTION OF IMPORT SUBSTITUTION PRODUCTS FOR DOMESTIC ENTERPRISES

Burkina Anastasia, 4th year student of the Department of economics
Scientific adviser: **Bronnikova Tamara,** Candidate of Economic Sciences, Associate Professor of the Department of economics

The article proposes to consider the actual for today the problem of import substitution. The strategy is aimed at growth of competitiveness of domestic products by substituting imported goods with domestic products. This policy will give the opportunity to reduce the economy's dependence on imports.

Import substitution, export, import, various sectors of the economy, domestic producers.

В связи с событиями на Украине и присоединением Крыма к России странами ЕС были введены санкции, к которым присоединились Королёвство Норвегия, США, Канада, Австралия, Новая Зеландия и Япония. Санкционный список неоднократно расширялся и продлевался, последнее решение о продлении было принято 22 июня 2015 года [4].

Россия была исключена из состава Большой восьмерки и Парламентской Ассамблеи Совета Европы, было прекращено сотрудничество с Организацией Экономического Сотрудничества и Развития, причем ряду европейских компаний было рекомендовано прекратить финансирование инвестиционных проектов на территории России. В частности, 18 мая 2014 года Европейский Инвестиционный банк по прямой рекомендации Европейского совета, прекратил финансирование новых проектов в России. 30 июля 2014 года был установлен запрет на инвестиции в инфраструктурные, транспортные, телекоммуникационные и энергетические секторы, а также добычу нефти, газа и минералов. Была запрещена поставка оборудования для этих секторов, а также оказание им финансовых и страховых услуг, установлен запрет на покупку более 250 наименований российских товаров, в том числе полезных ископаемых, минералов и углеводороды. Европейским финансовым структурам было запрещено выдавать кредиты или приобретать доли в проектах, которые затронуты секторальными санкциями. Одновременно был введен запрет на экспорт в Россию определенных видов энергетического оборудования и технологий, в

том числе высокотехнологичного оборудования для добычи сланцевой нефти, нефти в Арктике и на глубоководном шельфе. Было ограничено долговое финансирование «Роснефть», «Транснефть» и «Газпромнефть», запрещена торговля облигациями этих компаний со сроком обращения свыше 30 дней и участие в эмиссии ценных бумаг; оказывалось давление на российский банковский сектор («Сбербанк России», «Банк ВТБ», «Газпромбанк», «Внешэкономбанк» и «Россельхозбанк») в форме ограничений на предоставление займов и инвестиционных услуг.

Москва отреагировала Указом Президента №560 «О применении отдельных специальных экономических мер в целях обеспечения безопасности Российской Федерации» от 6 августа 2014г. Во исполнение названного указа Правительство РФ ввело запрет на ввоз сельскохозяйственной продукции, сырья и продовольствия, страной происхождения которых являются США, страны ЕС, Королёвство Норвегия, Канада и Австралия по перечню согласно приложению сроком на 1 год. Санкции распространялись на свежее, охлажденное и замороженное мясо крупного рогатого скота, и свинину; свежее, охлажденное и замороженное мясо, и пищевые субпродукты домашней птицы; соленое, в рассоле, сушеное или копченое мясо; колбасы и аналогичные продукты из мяса, мясных субпродуктов или крови, а так же изготовленные на их основе готовые пищевые продукты; молоко и молочную продукцию; молокосодержащие продукты, на основе растительных жиров; готовые продукты, включая сыры и творог на основе растительных жиров; рыбу, ракообразных, моллюсков и прочие водные беспозвоночных; овощи, съедобные корнеплоды и клубнеплоды (картофель, томаты, капуста, лук); фрукты и орехи [13].

Под ограничение не попали некоторые виды готовой продукции из мяса и рыбы. 20 августа правительство РФ исключило из списка продуктов, на которые распространяются ответные продовольственные санкции России, концентраты растительных и животных белков, спортивное питание, безлактозное молоко, БАДы и витаминно-минеральные комплексы. Также был снят запрет на поставки семенного картофеля, лука-севка, сахарной гибридной кукурузы и гороха для посева, а так же мальков лосося и форели для функционирования отечественной аквакультуры. Украинским авиакомпаниям были запрещены транзитные рейсы через Россию [4].

Контрсанкции России простимулировали начатую с 1998 года программу импортозамещения. 27.01.2015 был утвержден нацелен-

ный на выявление приоритетных отраслей и замещение отдельных видов импортируемых товаров на товары, произведенные на внутреннем рынке «План первоочередных мероприятий по обеспечению устойчивого развития экономики и социальной стабильности в 2015 году». В соответствие с ними 31 марта Министерством торговли и промышленности были утверждены 19 так называемых «дорожных карт», или отраслевых планов, направленных на импортозамещение. К приоритетным отраслям были отнесены металлургия, машиностроение, химическая, фармацевтическая, медицинская и легкая промышленность наряду с сельскохозяйственной отраслью. Немаловажную роль сыграла значительность доли импорта в перечисленных сферах.

Реакция российских производителей была неоднозначной. Предприятия – производители сельскохозяйственных товаров восприняли санкционный пакет России достаточно оптимистично, поскольку вступление РФ в ВТО 22 августа 2012 вкупе с неразработанностью мер защиты национальных производителей оказало в целом негативное влияние. Основной удар принял на себя средний бизнес, причем 34% предприятий отметили значительное ухудшение ситуации, в то время как выгоды коснулись лишь 12,5%. Под значительным давлением оказались российские производители молока, молочных продуктов и свинины. В подобном ограждении рынка России от международной конкуренции производители увидели, прежде всего, шанс на укрепление собственных позиций.

Таблица 1 – Индекс роста цен на отдельные группы продовольственных товаров (ноябрь – декабрь 2015г. к январю - ноябрю 2014г., (%) [12]

№	Вид продукции	Индекс цен, %
1	Продовольственные товары без алкогольной продукции	120,8
2	Хлеб и хлебобулочные изделия	114,3
3	Крупа и бобовые	144,9
4	Макаронные изделия	122,7
5	Мясо, включая мясо птицы	115,4
6	Рыба и морепродукты	129,5
7	Молоко и молочная продукция	113,9
8	Сливочное масло	114,1
9	Подсолнечное масло	130,4
10	Яйца	118,2
11	Сахар – песок	142,7
12	Плодоовощная продукция	130,7
13	Алкогольные напитки	112,0

Вместе с тем под предлогом инфляции, подорожания ГСМ, удобрений и проч. были заметно подняты отпускные цены на сельскохозяйственную продукцию.

По официальным данным, при сокращении реальной заработной платы на 9,2% к январю – ноябрю 2014г. рост цен к январю – ноябрю 2014г. составил 15,8%, в том числе на продовольственные товары – 9,6%, на продовольственные товары без плодоовощной продукции – на 9,9%. Индекс цен на продовольственные товары без алкогольной продукции в январе – ноябре 2015 к январю – ноябрю 2014г. составил 120,8%; на хлеб и хлебобулочные изделия – 114,3%; крупу и бобовые – 144,9; макаронные изделия – 122,7%; мясо и птицу – 115,4%; рыбу и морепродукты – 129,5%; молоко и молочные продукцию – 113,9%; сливочное масло - 114,1%; подсолнечное масло – 130,4%,; яйца – 118,2%; сахар – песок – 142,7%; плодоовощную продукцию – 130,7% и алкогольные напитки – 112% [10].

Падение спроса на продовольственные товары наряду с непродовольственными ряд исследователей объясняют как реакцией потребителей на рост цен и девальвацию рубля, так и контрсанкциями [9]. Международная аудиторско-консалтинговая компания КПМГ провела в 1 полугодии 2015г. исследование перспектив импортозамещения через локализацию в России, опросив представителей государственных органов, ответственных за реализацию политики импортозамещения в стране, и иностранных инвесторов. В результате было выявлено, прежде всего, расхождение точек зрения власти и бизнеса в данном вопросе. Большинство респондентов – чиновников отметили, что подобная политика импортозамещения носит вынужденный и запоздалый характер, причем 21% респондентов не были уверены в целесообразности проведения подобной программы. «В импортозамещении в первую очередь заинтересовано правительство, так как получает возможность улучшить торговый баланс и усилить позиции страны с геополитической точки зрения. Бизнес же интересуется скорее показателями объема рынка и рентабельности», — отметил финансовый аналитик ИХ «ФИНАМ» Тимур Нигматуллин [7].

20 октября 2015 года по инициативе Торгово – Промышленной Палаты РФ прошел «круглый стол», посвященный продовольственной безопасности страны в условиях импортозамещения. В его ходе была констатирована успешность усилий в области импортозамещения. Согласно данным Росстат, в

2014 году объем сельскохозяйственного производства вырос на 3,7%, превысив 4 трлн. рублей. За восемь месяцев 2015 года он вырос еще на 1,8%, достигнув 4,252 трлн. рублей. При этом с августа 2014 года в натуральном выражении возрос объем производства мяса, мясной продукции, молока и сыров. Россия полностью обеспечила собственные потребности в мясе птицы и начала экспортировать этот вид продукции. В 2014 году был собран рекордный урожай зерновых в объеме более 105 млн. тонн. Урожай 2015 года составил порядка 103 млн. тонн. По сообщению Министерства сельского хозяйства, продовольственная безопасность по зерну в 2015 году была обеспечена на 142%, по растительному маслу – на 146%, картофелю – на 99%, сахару – на 95%, овощам открытого типа – 88% [12].

Слабым местом остается молочная отрасль, мясное животноводство, производство овощей и фруктов. Характерно, что в течение последних десяти лет не отмечалось существенного прироста в молочном животноводстве [12]. В условиях физического сокращения поголовья молочного скота удои поддерживались за счет увеличения доли высокоудойных пород в общем поголовье. Самообеспеченность по тепличным овощам России составляет 34%, по фруктам – 37%, что обуславливает необходимость ежегодного импортирования овощей, составляет в объеме почти 1,5 млн. тонн при общей сумме закупок почти в $1 млрд. и ввоз почти 3 млн. тонн фруктов. Для замещения данного вида импортной продукции необходимо ежегодно вводить около 300га новых теплиц. Для этого перекрытия ниши до 2020 года нужно заложить около 65 тысяч садов [12].

По данным министерства сельского хозяйства, в результате ответных российских санкций на рынок не поступило 848 тыс. тонн импортного мяса. Одновременно дополнительный прирост в сельском хозяйстве России составил более 350 тыс. тонн мяса, причем прирост производства свинины составил более 6 %, мяса птицы - около 6 %. В результате импортозамещение на 60 – 70% было обеспечено за счёт прироста отечественного производства, а не за счёт альтернативных поставщиков. При этом один открывшийся в 2015 году Брянской области комплекс замещает по оценкам около 7% импортного мяса. Импортозамещение коснулось и деликатесов. В Свердловской области успешно развивается производство такого деликатеса, как хамон; в республике Татарстан и Вологодской области производят сыр сорта «пармезан», на Алтае – «камамбер» и

«маскарпоне» на Алтае. В Новороссийске по состоянию на весну 2015 года шло строительство предназначенного для разведения в промышленных масштабах трюфелей агрокомплекса «Трюфельная Долина». В отдельных тепличных хозяйствах России выращиваются тропические фрукты, примером может служить выращивание бананов в Брянской области. Были адаптировны к местным условиям сорта хлопка в Астраханской и Волгоградской областях, а так же на Ставрополье.

В машиностроение импортозамещение составило порядка 33%, в отдельных областях – например, средтвах общественного транспорта – достигая показателя в 88%. Характерен пример предприятий по добыче углеводородов: лишившись доступа к передовым технологиям добычи, помимо введения в свой капитал сервисных компаний с высокотехнологичным оборудованием и опытом работы с месторождениями в сложных климатических условиях они развивали собственные НИОКР. «НоваТЭК» использует собственные методы газодобычи во льдах, бурения горизонтальных скважин, создания насыпных островов. Как результат, на Юрхаровском месторождении под дном Тазовской губы добывается 30 млн. т газа в год. Между тем соседняя Норвегии не применяют технологии добычи сырья во льдах.

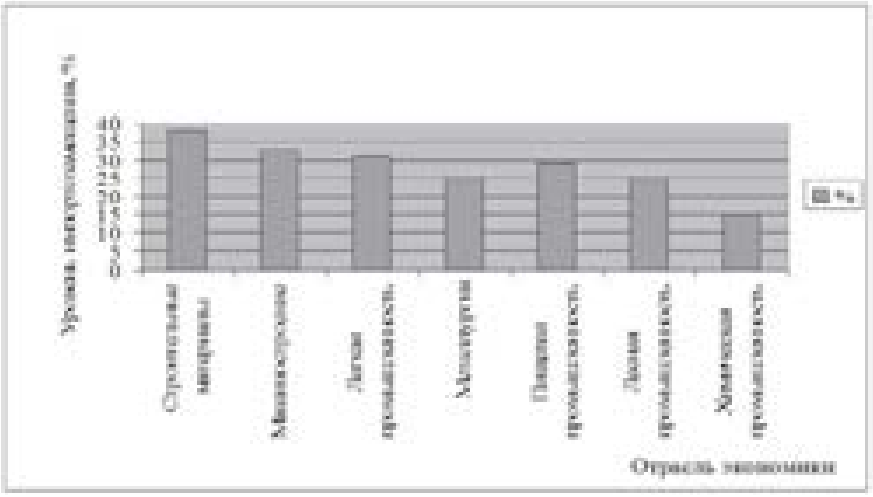


Рисунок 1 – Уровень достигнутого импортозамещения на III квартал 2015г. (%) [10]

«Сургутнефтегаз» в 2013г. так же самостоятельно добыл в сложных условиях баженовской свиты первый миллион тонн трудноизвлекаемой нефти, используя собственные наработки и оборудование. Опытные испытания российской технологии, альтернативной гидроразрыву пласта, для извлечения нефти из глубоких горизонтов проводила в 2014 - 2015гг. компания РИТЭК (входит в ЛУКойл). Речь идет о термогазовом воздействии на пласт: принцип был разработан еще в СССР, но применяться начал только пять лет назад [9].

В сфере производства строительных материалов импортозамещение на III квартал 2015 года составило 38%, в легкой промышленности – 31%, металлургии – 25%, пищевой промышленности – 29%, лесной – 25%, химической – 15%. При этом в числе сдерживающих факторов производители отмечали низкое качество сырья либо отсутствие отечественных аналогов наряду с низким уровнем доверия потребителей к продукции отечественного производства [8].

В то же время импортозамещение стало одним из основных драйверов роста российского ИТ - рынка и рынка информационной безопасности. Расстановка сил на данном рынке изначально складывалась так, что российские разработчики занимали сильные позиции в сегменте обеспечения безопасности компьютеров и серверов, сталкиваясь со значительной конкуренцией в области средств защиты сетей. Критериями выбора в данной сфере для потребителей являются конкурентоспособная цена, лицензированность продукции и соответствие требованиям регуляторов [7].

Для оптимизации импортозамещения в России целесообразно применять:

-кластерный подход, прежде всего в области высоких технологий;

-целевое инвестирование проектов; работу на перспективу, т.е. создание новых видов продукции для потенциальных клиентов. Данный момент обусловлен как высокими темпами развития технологий, так и тем, что в настоящий момент уже прояснились контуры нового постиндустриального мира [5];

-повышение уровня квалификаии как специалистов, так и рабочей силы.

Практика показывает эффективность кластеров в российских условиях, в том числе посредством формирования вокруг них специфичной инфраструктуры и возникновения особой атмосферы, порождающей чувство причастности к чему – то прогрессивному и значимому и мотивирующей сотрудников. Целевое финансирование снижает риск расхищения средств и построения различных мошеннических схем. Вместе с тем скорость устаревания навыков и умений в современном мире все возрастает, что ставит вопрос, как о высокой планке отбора персонала, так и систематического повышения уровня его знаний и умений, в том числе в форме переаттестации.

Литература

1. Бронникова Т.С. Разработка бизнес-плана проекта: учебное пособие / Т.С. Бронникова,− М.: АльфаМ; ИНФРА-М, 2014. − 224 с.− (Технологический сервис). http://znanium.com/bookread2.php?book
2. Старцева Т.Е., Бронникова Т.С. Экономика и управление инновационным развитием предприятия: методологический инструментарий: монография/ Т.Е. Старцева, Т.С. Бронникова.− М.: РУСАЙНС, 2016. – 202 с.
3. Трофимов Г. Механизмы импортозамещения на уровне отраслей / Институт финансовых исследований. М.: 2015 – 154 с.
4. URL: http://www.aif.ru/money/economy/trend_1552 (дата обращения - 16.02.2016)
5. URL: http://biznesklubonline.com/stati/568-sanktsii-rossii-v-otnoshenii-evropy/ (дата обращения - 16.02.2016)
6. URL:http://expert.ru/ural/2014/44/tehnologicheskaya-bezopasnost-v-opasnosti/(Дата обращения – 16.02.2016)
7. URL: http://expert.ru/siberia/2015/46/udivitelnoe-importozamesch (Дата обращения – 16.02.2016)
6. URL: http://expert.ru/northwest/2015/35/tonkie-rostki (Дата обращения – 16.02.2016)
7. URL: http://expert.ru/ural/2014/4 (Дата обращения - 16.02.2016)
8. URL: http://www.itsec.ru/articles2/itogi/importozameschenie
9. http://www.rbc.ru/opinions/economic (дата обращения - 16.02.2016)
10. http://www.rea.ru/ru/org/managements/Situa-centr/
11. URL: http://www.rg.ru/2014/08/07/pravitelstvo-site (дата обращения - 16.02.2016)
12. URL: http://ruxpert.ru/ Сельское хозяйство России (дата обращения 04.02.2016)

13. URL: http://www.tpp-inform.ru/analytic_journal/6259.html (дата обращения 04.02.2016)

ИМПОРТОЗАМЕЩЕНИЕ ТЕХНИКИ И ТЕХНОЛОГИЙ В МОСКВЕ И МОСКОВСКОЙ ОБЛАСТИ

Вершинин Александр Алексеевич, студент 3 курса кафедры Экономики
Научный руководитель: **Котрин Вадим Владимирович,** советник при ректорате, к.э.н., доцент кафедры Экономики

С 2014 года в России активно действует политика импортозамещения продукции. Данная политика направлена на замещение импорта для более независимого функционирования экономики. Но для того, чтобы производить отечественную продукцию, необходимы мощности. Поэтому прежде чем производить продукцию, нам необходимо произвести новые станки, оборудование, обучить персонал.

Импортозамещение, техника и технологии, импорт, экспорт.

THE SUBSTITUTION OF ENGINEERING AND TECHNOLOGY IN MOSCOW AND THE MOSCOW REGION

Vershinin Alexander, 3rd year student of the Department of economics
Scientific adviser: **Kotrin Vadim**, Adviser of the University administration, Candidate of Economic Sciences, Assistant Professor of the Department of economics

Russia has been active policy of import substitution products since 2014 year. This policy is aimed at import substitution to a more independent functioning of the economy. But in order to produce domestic products, the power is required. So before, to increase the production of products we need to produce new machines, equipment and staff training.

Import substitution, technology, import, export.

Проблема, связанная с импортозамещением, т.е. замены импортного товара на российском рынке отечественным, не нова и периодически поднимается, в том числе и руководством страны. Именно импортозамещение связывают с решением одной из главных задач экономики Российской Федерации – ее диверсификацией. К

сожалению, разработать целостную политику власти решили только после введения санкций против России. О необходимости преодоления критической зависимости от зарубежной техники и технологий, а также промышленной продукции говорил в послании Президент РФ Федеральному Собранию в конце 2014 года. Он посоветовал использовать возможность, складывающуюся в связи с санкциями для выхода на новые рынки и рубежи, а также призвал к этому в ходе "прямой линии" в апреле прошлого года.

В 2013 году по данным Федеральной службы статистики доля импорта в объеме внутреннего рынка России по некоторым обрабатывающим видам деятельности составила: производство тканей, одежды и обуви – 70%; производство машин и оборудования – 62%; производство электро- и оптического оборудования – 53%; и т.д. [2, С.81].

На данный момент, по оценкам Правительства, доля импорта в различных отраслях экономики страны очень высока. Для примера, РФ импортирует в гражданском самолетостроении более 80% комплектующих, в тяжелом машиностроении – порядка 70%, в нефтегазовом оборудовании – 60%, в энергетическом оборудовании – около 50%, в сельхозмашиностроении в зависимости от категории продукции – от 50% до 90% деталей и т. п.

Многие говорят, что тяжелые для экономики страны моменты, связанные со снижением иностранного спроса на поставляемое Россией сырье и материалы, и закономерное удешевление рубля, являются своеобразным окном возможностей для масштабного углубления импортозамещения.

В 2015 году по сравнению с 2014 годом произошло уменьшение экспорта с 345,84 млрд. долларов США до 263,4 млрд. долларов США, Данные изменения произошли в результате падения цен на нефть до уровня 40$, т.к. экономика России является сырьевой и 65% доходов идет с продажи нефти. Импорта уменьшился с 188,22 млрд. долларов США до 135,8 млрд. долларов США, в связи с введение эмбарго на ряд иностранных товаров, но при этом чистый экспорт остался положительным, хоть и тоже уменьшился с 155,62 млрд. долларов США до 127,6 млрд. долларов США. Данные изменения побуждают производить нам самим, в связи с сокращением источников для внутреннего рынка. В итоге задача России заключается в том, чтобы рос экспорт и падал импорт, а также

необходимо изменить структуру экспорта, чтобы вместо сырья продавать готовую продукцию.

В результате проведения политики импортозамещения могут быть достигнуты следующие результаты: рост занятости населения, рост образовательного и научно-технического уровня, повышение конкурентоспособности отечественных товаров, упрочнение экономической и продовольственной безопасности страны, сохранение валютной выручки страны.

Однако не стоит забывать и о рисках, связанных с импортозамещением. Среди них можно выделить следующие:

- Снижение конкурентоспособности, вызванное устранением конкуренции с ведущими зарубежными поставщиками;
- Снижение эффективности экономики страны в целом, если продукция национальных производителей будет по качеству уступать своим зарубежным аналогам;
- Может произойти увеличение нагрузки на бюджет страны [1, С.57].

В данном случае, проблемы, возникающие в сфере импортозамещения можно структурировать на проблемы спроса и проблемы предложения. К проблемам спроса можно отнести:

- Проблемы финансирования подготовки производства и обеспечения предприятий-производителей Москвы и МО оборотным капиталом;
- Дискриминация со стороны крупных и международных ритейлеров;
- Коррупционные схемы проведения тендеров, государственных закупок и государственных заказов.

Для удовлетворения спроса на импортозамещение возможный производитель должен иметь информацию об объемах спроса, качестве и предполагаемой цене товара. Для развертывания производства по импортозамещению необходимо финансовые источники для создания производственных площадок и их обеспечению высокотехнологичным оборудование и качественным сырьем.

К проблемам предложения можно отнести:

- Отсутствие сведений о технологических и производственных возможностях поставщиков Москвы и МО.
- Проблемы финансирования подготовки производства и обеспечения предприятий-производителей Москвы и МО оборотным

капиталом.

- Низкое качество подготовки технико-экономического обоснования, бизнес-планов и финансовых моделей инициаторами импортозамещающих проектов.
- Дефицит подготовленных промышленных площадок, оснащённых необходимой инфраструктурой.
- Существенное ослабление роли и профессиональных возможностей головных научно-технических институтов Москвы и Московской области.
- Дороговизна сырья, применяемого в производстве импортозамещающей продукции.
- Отсутствие возможностей для производства сопутствующих товаров, выпуски которых снижает общую себестоимость импортозамещающей продукции.

Одним из примеров проблемы спроса является закупка Правительством г. Москвы трамваем в Польше и Франции. В то же самое время в г. Твери вагоностроительный завод готов поставить г. Москве современные, экономичные, удобные, низкопольные трамваи, что, несомненно, позволит Москве сэкономить валюту, а заводу в Твери, получив заказ, выжить в трудных условиях и не увольнять по сокращению сотрудников завода из-за отсутствия спроса на продукцию. Необходимо уточнить, что на осуществление плана импортозамещения в сельском хозяйстве на 2014-2015 года были выделены денежные средства в размере 1 триллиона 818,2 миллиардов рублей.

При обсуждении вопросов импортозамещения на столичном рынке было отмечено, что с момента введения продовольственного эмбарго цены на социально значимые продукты остаются стабильными.

В 2014 году Министерство промышленности и торговли провели анализ импортозамещения промышленности в итоге, получилось, что наиболее перспективными оказались:

1. станкостроение (для импорта в потреблении по разным оценкам) – 90%;
2. тяжёлое машиностроение – 60-80%;
3. лёгкая промышленность – 70-90;
4. электронная промышленность – 80-90%;
5. фармацевтическая, медицинская промышленность – 70-80%;

6. машиностроение пищевой промышленности – 60-80%.

Для решения проблем, связанных со спросом и предложением, организовываются тематические выставки, центры импортозамещения. В 2015 году прошло несколько выставок в Москве и Московской области.

Тематическая выставка в Центре импортозамещения и локализации Московского района. В октябре 2015 года участвовали более 30 предприятий в тематической выставке. Московский район стал первым из 18 районов. Выставка способствовала его высокой результативности, следовательно, другим районам будет к чему стремиться.

На представленной выставке были продемонстрированы реальные промышленные модели отечественной продукции наших предприятий. Выставка создана для того, чтобы производители и потребители находили друг друга. Например, подведомственные предприятия могут быть не в курсе, что петербургскими компаниями выпускается достаточно большой перечень продукции, которая могла бы заменить импорт. В Центре часто проводятся совещания, на которых подробно анализируют проделанную работу, оценивают результаты и недостатки, планируют перспективы.

Результаты Московского района на площадке Центра импортозамещения и локализации, конечно же, есть. Руководители и представители после активных переговоров подписали несколько соглашений. В последующем Московский район планирует участвовать в сфере здравоохранения и показать свои достижения.

Выделена задача по наведению мостов - между прошлой экономической мощью района и будущей высокотехнологичной, конкурентоспособной отечественной индустрией, которая частично выполнена.

Проблема зависимости от импорта остро стоит в области транспортной инфраструктуры, для которой по целой линии продукции отсутствует изготовление аналогов.

Комитет проводит мероприятия, направленные на стимуляцию совершенствования российских подрядных организаций, а также разных компаний по вопросам производства конкурентоспособных товаров и услуг. Комитет значится основным распределителем бюджетных средств, инвестиционным заказчиком, а реализация проектов Комитета совершается через подведомственные организации, которые являются техническими заказчиками. По всем

направлениям деятельности Комитета и в рамках действующих контрактов проводится работа только с отечественными подрядчиками. Для формирования необходимости Комитета в отечественной продукции и определения вероятности ухода от импорта, образованы специальные рабочие объединения.

Подведомственными подразделениями запущен электронный мониторинг, где любой отечественный изготовитель может принять участие, подав должную заявку. Учитывая требования технических заданий к продукции, изготовитель заполняет единую форму и отдаёт её на рассмотрение.

Планируется комплексная поддержка городского бизнеса в 2016 году. В сфере поддержки предприятий реального сектора и импортозамещения в план вошла поддержка следующих отраслей производства: медицина, авиастроение, информационные технологии, микроэлектроника, биохимия, производство автокомпонентов, строительных материалов и оборудования, пищевая промышленность.

Одним из важнейших направлений выделили поддержку строительного сектора. А также финансирование создания инфраструктуры индустриальных парков, технопарков, технополисов, в том числе в рамках проектов, получивших поддержку федерального бюджета, более того разработка механизмов комплексного развития промышленных зон.

С производителями импортных товаров планируется заключать долгосрочные государственные контракты, одним из условий которых станет создание и развитие производства соответствующей продукции в Москве.

При этом возникает спрос импортозамещающих предприятий на отечественные разработки, в т.ч. Москвы и МО.

В МО просматриваются конкретные направления и география импортозамещения, один из них г. Химки. Инвестиционный проект ООО «Куранты», Производство порошковых композиций (фидстоков) с повышенными физико-механическими свойствами, а также металлических и керамических изделий сложной формы. Для реализации потребуется 377,4 млн. руб. Экспертный совет фонда одобрил выделение займа на сумму 280 млн. руб. Использование фидстоков необходимо для производства стрелкового оружия, поэтому международные компании ограничили поставки, вызвав дефицит на гражданских предприятиях. Благодаря инвестиционному

проекту появятся дополнительно 18 рабочих мест. А первая промышленная партия будет готова к 2018 г.

Следующий проект компании ООО "Ниармедик Плюс", Москва и Калужская область.

Общая сумма инвестиций превышает 300 млн руб. Реализация проекта позволит создать 24 рабочих места.

Компания рассчитывает, что заем Фонда развития промышленности в размере 202 млн. руб. позволит ей отвоевать большую часть отечественного рынка молекулярно-генетической идентификации личности и установления родства, снизив зависимость государственных экспертных лабораторий от зарубежных поставщиков с 98% до 20-30%.

Кроме того, потребители смогут экономить на закупках реагентов до 42% за счет более низкой цены отечественной продукции. Компания создает первое в России производство полного цикла по технологии, обладающей значительными конкурентными преимуществами перед зарубежными аналогами. Производиться реагенты будут на двух площадках – в Москве и Обнинске.

Области применения продукции - геномная регистрация и идентификация, криминалистическая и судебно-медицинская экспертиза по ДНК-маркерам человека, определение родства и другие виды генетических исследований.

Среди потенциальных потребителей МВД РФ, ФСБ РФ, Министерство обороны РФ, Министерство здравоохранения РФ, Следственный комитет РФ, которые являются основными потребителями наборов для ДНК-анализа в России. Коммерческие продажи продукции планируется начать в 2017 г.

Пока наша экономика является сырьевой, а главный доход идет от продажи нефти, необходимо срочно организовывать более глубокую переработку сырья, увеличивая добавочную стоимость и выпуск сопутствующих товаров. Один из таких проектов представляет ОАО «Башнефть» совместно с Правительством Москвы.

Московское предприятие планирует завершить разработку и наладить к концу 2018 г. работу модульной установки утилизации сероводородного газа в элементарную серу на нефтеперерабатывающем предприятии ОАО АНК "Башнефть".

Проект станет пилотным и впоследствии позволит создать отечественную технологию производства элементарной серы с

возможностью тиражирования установок на объектах нефтегазового комплекса страны. Элементарная сера – необходимый элемент для химической, целлюлозно-бумажной, горнодобывающей, металлургической отраслей промышленности. Особенно широко применяется в производстве сельскохозяйственных удобрений.

Общественная полезность разработки московского предприятия заключается в возможности перерабатывать отходы нефтегазового производства – токсичный сероводородный газ – в безопасный продукт. На последующих этапах проекта предполагается превышение параметров признанных мировых технологий, что создаст высокий экспортный потенциал отечественной разработки.

Расходы проекта запланированы на уровне 765 млн. руб., из которых заем фонда, одобренный экспертным советом, может составить 500 млн. руб. Реализация проекта позволит создать 42 рабочих места.

Помимо планируемых проектов, существует много реализованных. Один из таких является Лианозовский молочный комбинат.

Для увеличения производства молочной продукции в целях импортозамещения для населения Москвы и Московской области проведена модернизация Лианозовского молочного комбината.

В результате произошло увеличение объемов выпуска за счет увеличения количества поточных линий, за последние два года запускается 3я поточная линия, при этом производство молочной продукции произошло на основе отечественного молока. Среднесуточный объем производства составляет 1050 тонн готовой продукции (180 ассортиментных позиций в 20 продуктовых категориях). Сегодня комбинат является крупнейшим молокоперерабатывающим предприятием в России и Восточной Европе.

Выпускается продукция под марками "Домик в деревне", BioMax, "Чудо", "Веселый молочник", "Агуша" и другими. Комбинат использует молоко из местных ферм - 25% из хозяйств Подмосковья и 75% - Рязанской, Вологодской, Калужской и Тульской областей.

Основным потребителем продукции комбината традиционно являются Москва и Московская область, на которые приходится порядка 60% от общего объема продукции. Часть продукции экспортируется в страны СНГ, а также в Грузию и Монголию.

Модернизация "Лианозовского молочного комбината" - реальный пример успешного импортозамещения в Москве, сообщил мэр столицы Сергей Собянин.

Москва успешно реализует планы по импортозамещению молочной продукции. "В Москве завершается процесс импортозамещения молока и молочной продукции. Сегодня уже на рынки поставляется 90% именно отечественной продукции.

Подводя итог, можно сделать следующие выводы, что без содействия со стороны всех уровней государства по организации импортозамещения решить проблему в короткий срок и в настоящее время почти невозможно. У государства должно быть в руках сопровождение проблем несогласованности партнеров по организации производства импортозамещающей продукции. Необходимо наладить четкую работу производителей и покупателей, создать благоприятную обстановку для создания новых технологий, поощрять качественные и эффективные проекты, а также противодействовать коррупции.

Литература

1. Вопросы региональной экономики №3 (24) 2015
2. Вопросы региональной экономики №4 (21) 2014
3. Электронный ресурс: http://www.garant.ru/article/630000/ (дата обращения 29.01.2016)
4. Электронный ресурс: http://www.customs.ru/index2.php?(дата обращения 28.01.2016)
5. Электронный ресурс: http://rg.ru/2014/12/04/(дата обращения 01.02.2016)
6. Электронный ресурс: http://mosreg.ru/multimedia/novosti (дата обращения 01.02.2016)
7. Электронный ресурс: http://www.engineering-info.ru/фонд-развития-промышленности-поддер-2/ (дата обращения 29.01.2016)
8. Электронный ресурс: http://importozamechenie.ru/tag/investicii/ (дата обращения 28.01.2016)

ИННОВАЦИОННАЯ СРЕДА РОССИЙСКОЙ ФЕДЕРАЦИИ

Клевцов Павел Олегович, Богданов Александр Валерьевич,
студенты 2 курса кафедры Экономики
Научный руководитель: **Рыжкова Татьяна Васильевна**, к.э.н.,
доцент кафедры Экономики

Статья посвящена исследованию одной из самых многозначительных для развития страны теме – инновационной среде. Изучена сущность инновационной среды, ее состав и структура, состояние инновационной среды в Российской Федерации, а также предложены методы ее оценки и возможные пути развития.

Инновационная среда, факторы инновационной среды, проблемы инновационной среды, показатели оценки инновационной среды.

INNOVATIVE ENVIRONMENT OF THE RUSSIAN FEDERATION

Klevtsov Pavel, Bogdanov Aleksandr, 2nd year students of the
Department of economics
Scientific adviser: **Ryzhkova Tatyana,** Candidate of Economic Sciences,
Assistant Professor of the Department of economics

In this article investigated one of the most meaningful themes for the development of the country - innovative environment. Was investigated the essence of the innovation environment, its composition and structure, was analyzed state innovation environment in the Russian Federation, as well was proposed methods of assessment this. On the basis of the study were identified possible ways of developing innovative environment in Russian Federation.

Innovative environment, factors innovative environment, problems innovative environment, performance evaluation of the innovation environment.

Роль инноваций в мировом развитии неоспорима, и сейчас их разумно связывать не с отдельным сектором экономики, а с концепцией устойчивого развития страны, с перспективами развития общества. Именно поэтому в сложных текущих условиях России особенно важно с помощью инноваций и развития инновационной

деятельности выйти из кризиса и занять достойное место в мировом распределении труда.

Но что означает «инновационная среда»? По сути это то, что позволяет появляться инновациям и, самое главное, помогает им развиваться.

Инновационная среда – это сложившаяся определенная внешняя и внутренняя - социально - экономическая, организационно - правовая и политическая среда, обеспечивающая или тормозящая развитие инновационной деятельности. Компонентами инновационной среды принято считать определенные стратегические зоны хозяйствования: рынок новшеств, рынок чистой конкуренции нововведений (инноваций), рынок капитала (инновационных инвестиций), звенья административной системы, с которыми непосредственно связаны участники инновационного процесса, звенья инновационной инфраструктуры, обслуживающие инновационную деятельность [1].

В.Д. Секерин утверждает, что инновационная среда представляет собой меру готовности к реализации инновационного проекта или программы инновационных преобразований и, следовательно, внедрению инноваций [10].

Также инновационную среду можно рассматривать, как совокупность всех социально-экономических подсистем, обеспечивающих доступ к различным ресурсам и оказывающих ту или иную поддержку участникам инновационной деятельности.

Под инновационной средой нужно понимать совокупность тех систем, которые являются фундаментальным ядром, формирующим инновационную деятельность, исходя из классической теории инноваций Й. Шумпетера. В общем виде инновационную среду России можно представить в качестве совокупности подсистем (рисунок 1):

- исследовательской и образовательной, обеспечивающих разработку и научное сопровождение инновационных процессов (интеллектуальный потенциал территории);
- хозяйствующих предприятий и организаций, занятых в инновационном производстве (реализация инновационных проектов);
- информационной сети, которая функционирует на базе действующих информационных ресурсов;
- специализированных инновационных структур (система трансферта инновационных технологий);

- структуры подготовки инновационной восприимчивости потребителем;
- системы институционального и политического обеспечения;

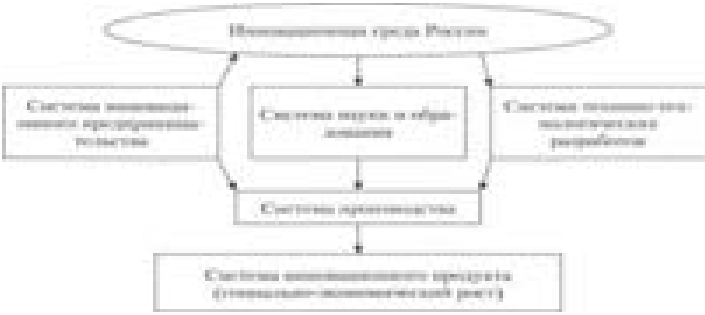


Рисунок 1 – Структура системы инновационной среды

- сферы инвестиционного обслуживания, финансовой, в том числе предприятий венчурной индустрии и специализированных фондов [6, 7].

Инновационная среда определяется факторами, которые непосредственно или косвенно влияют на инновационную систему. Непосредственно влияющие на инновационную систему факторы могут быть как экзогенными - социально-экономическими и институциональными, так и эндогенными - инновационная инфраструктура, инновационный потенциал. К косвенным факторам относятся: технологическое развитие страны и технологическая структура экономики [12].

Инновационная экономика – это экономика, основанная на знаниях. И она имеет свои законы, отличные от тех, которые работают в традиционных рыночных системах. Установил и продемонстрировал это лауреат Нобелевской премии по экономике Брайен А. (США). В экономической литературе утверждается, что фирмы, работающие в одной области, будучи близко расположенными, мешают друг другу. Их следует разнести либо территориально, либо по номенклатуре выпускаемой продукции. Однако, по словам А. Брайена, пример противоположного демонстрирует Кремниевая долина в США – мировой центр компьютерной и инновационной индустрии. Именно там взаимодействие соседних фирм имеет положительный характер. Это объясняется кооперирующим синергетическим эффектом, связанным с созданием единой информационно-технологической среды,

возможностью обмена идеями, знаниями и квалифицированными кадрами [2].

В процессе изучения текущего состояния инновационной системы в научном исследовании были выявлены следующие проблемы развития инновационной среды в Российской федерации.

Первая и самая существенная проблема в том, что разорванным оказался воспроизводственный цикл создания и внедрения инноваций, который является фундаментом всей инновационной среды.

В условиях социализма цикл выглядел следующим образом: высшая школа и академия наук проводили фундаментальные исследования. Результаты этих исследований воплощались в прикладные разработки отраслевыми институтами, на основе которых в НИИ и КБ проводили опытно-конструкторские работы, создавали опытные образцы и передавались на предприятия соответствующих отраслей экономики для серийного и массового производства. Создаваемая техника увеличивала производительность труда либо предоставляла новые возможности стране. Это позволяло направить часть финансовых ресурсов на дальнейшие фундаментальные разработки. Данный круг замыкался [2].

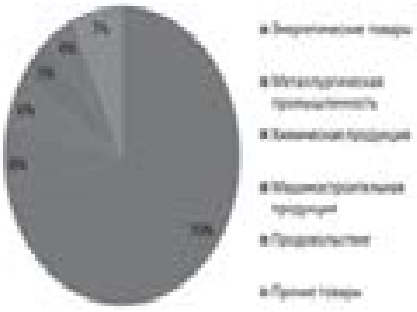


Рисунок 2 – Структура экспорта товаров из России за 2014 г.

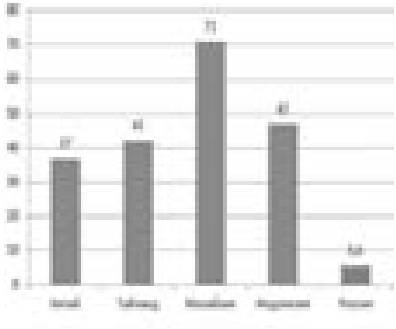


Рисунок 3 – Доля высокотехнологических товаров в Экспорте

Вторая проблема состоит в том, что российские товары оказались вытесненными с внешних рынков высокотехнологичной продукции зарубежных производителей (рисунок 3), и, что еще более опасно, многие виды продукции оказались неконкурентоспособными и на внутренних рынках. Пример тому компания «Аэрофлот», вынужденный закупать самолеты фирмы «Боинг», в то время как

отечественные производители не имеют заказов и, таким образом, неизбежно деградируют. Это усиливает зависимость отечественной экономики от первичного и энергетического сырья (рисунок 2).

Экономика Россия не производит необходимого объёма потребительских и продовольственных товаров и многих товаров высокотехнологичных отраслей, имеет сырьевую ориентацию. Поэтому отказаться от импорта многих товаров в такой ситуации, несмотря на активный процесс импортозамещения, невозможно. Поток импортных товаров уравновешивается в первую очередь экспортом нефти, газа и ряда других невосполнимых минеральных ресурсов.

Важной проблемой российской экономики характеризует состояние образовательной системы, которая определят научный потенциал страны, а значит и развитие инновационной среды в долгосрочном периоде. Инновационную экономику часто называют экономикой, «основанной на знаниях» или «экономикой знаний». Европейский опыт показывает, что стратегический потенциал развитой страны определяется не общим массовым образованием, как это было ранее, а творческим креативным потенциалом населения, уровнем организационно-политической и научно-технической элиты. Большое значение имеет не только уровень финансирования образования, но и направления использования денежных средств. К сожалению, в настоящее время, в базисных ценах затраты на образование падают (рисунок 4) даже несмотря на улучшение общей структуры образования населения в целом (рисунок 5). Однако количество еще не является показателем качества.

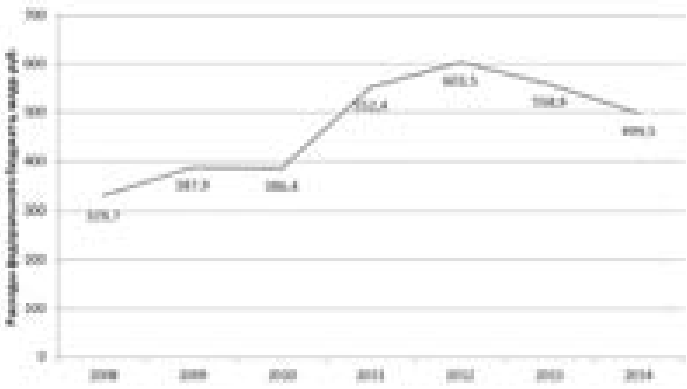


Рисунок 4 – Расходы на образования, млрд. руб.

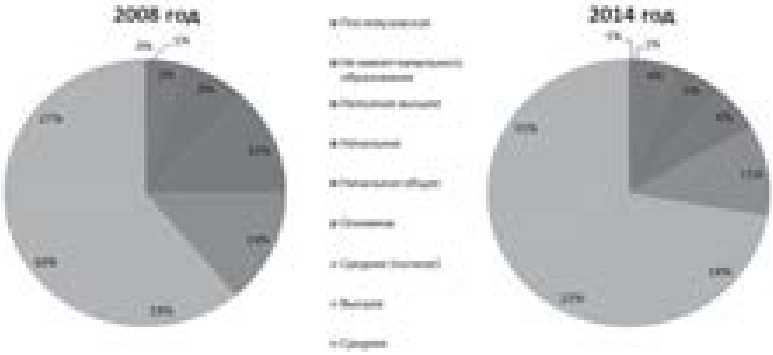


Рисунок 5 – Структура образования населения

Для оценки инновационной среды страны в мировой практике используют показатель числа поданных международных заявок на патенты, характеризующий уровень инноваций и интеллектуального развития стран мира. По абсолютному числу заявок на патенты США по-прежнему являются безоговорочным лидером. Только в 2014 г. изобретателями США было подано 44855 заявок, что значительно выше, чем в следующих за ней странах Японии, Германии, Китае и Южной Корее. Россия в 2014 г. зарегистрировала всего 560 международных заявок на патенты - самый низкий показатель за последние пять лет. В 2010 г. было зарегистрировано 677 патентов, в 2011 – 703. Россия опережают лишь такие страны, как Ирландия (431), Турция (406), Новая Зеландия (285), Бразилия (459 заявок), и значительно превосходит Латвию (28) и Литву (24), Белоруссию (13 заявок), Казахстан (19) (рисунок 6) [5].

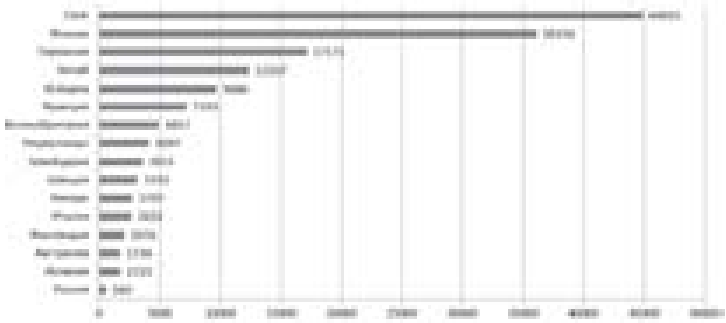


Рисунок 6 – Число поданных международных заявок на патенты (на 1.000.000 человек)

Кроме того, в оценки инновационной среды, помимо числа поданных международных заявок на патенты, целесообразно использовать такие показатели, как удельный вес организаций, осуществляющих технологические инновации, в общем количестве организаций; интенсивность затрат на технологические инновации; объем товаров (продукции, работ, услуг), приходящийся на рубль затрат на технологические инновации [8,9].

Удельный вес организаций, осуществляющих технологические инновации, в общем количестве организаций, характеризует уровень инновационной активности, т.е. разработки и внедрения новых или же усовершенствованных товаров, работ, услуг, технологических процессов или способов производства услуг и иных видов инновационной деятельности, в течение определенного периода времени.

Затраты на технологические инновации - выраженные в денежной форме фактические расходы, связанные с разработкой и внедрением технологических инноваций, выполняемых в масштабе организации (отрасли, региона, страны). В них учитываются расходы на различные виды инновационной деятельности, как выполненные собственными силами организации, так и расходы на оплату работ, услуг сторонних организаций.

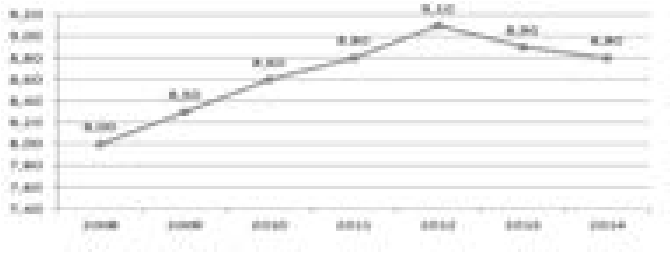


Рисунок 7 – Удельный вес организации, осуществлявших технологические инновации, в общем числе организаций

Затраты на технологические инновации включают текущие и капитальные затраты, осуществленные организацией в отчетном году. При этом не имеет значения, на какой стадии находится инновационный процесс - завершающей, когда уже налажено производство и выпускаются товары (работы, услуги), или на начальной, промежуточной стадии (например, когда выпуск товаров (работ, услуг) еще не налажен, а осуществляется лишь подготовка к их производству) [5].

Этот показатель отражает желание и возможности организаций и предприятий в данной стране (отрасли, регионе) финансировать свою инновационную деятельность или инновационную деятельность сторонних организаций (рисунок 8).

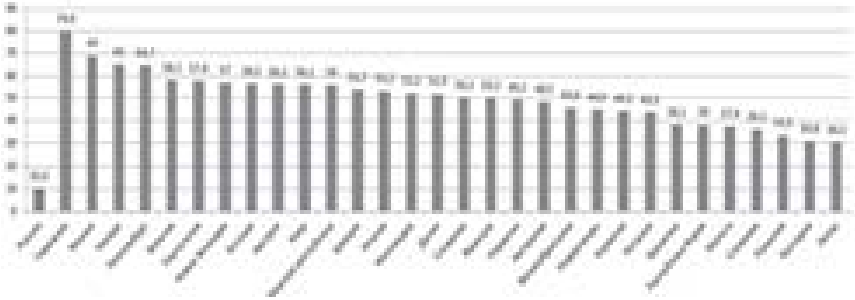


Рисунок 8 – Интенсивность затрат на технологические инновации

Показатель объема товаров приходящийся на рубль затрат на технологические инновации, выражается в виде стоимости полученных товаров за счет затрат на технологические инновации (рисунок 9). Значение показателя характеризует эффективность затрат на инновационную деятельность, как в краткосрочном, так и в долгосрочном периодах.

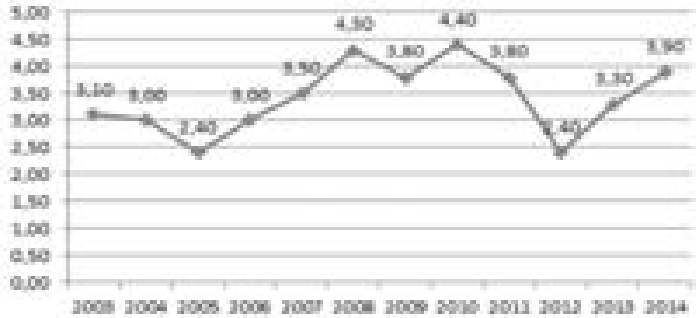


Рисунок 9 – Объем инновационных товаров, работ, услуг на рубль затрат на технологические инновации

Для преодоления проблем, существующих в инновационной среде, необходимо предпринять необходимые меры, среди которых основными являются:

- разработка государственной программы по поддержанию и улучшению инновационной среды;

• стимулирование инновационной политики предприятий на основе использования финансово-кредитных и денежно-фискальных инструментов;

• возрождение цикла создания и внедрения инноваций;

• изменение приоритетов экономики в направлении производства и экспорта высокотехнологичных товаров.

Решение поставленных задач потребует больших затрат, на которые государство в текущей кризисной экономико-политической ситуации практически неспособно. Однако в случае откладывания решения этой проблемы на более поздние сроки не сможет вернуть Россию в число стран – мировых лидеров.

В работе определены и исследованы показатели, характеризующие степень инновационности мировой экономики и место России в инновационном процессе. Анализ показал, что за последнее почти 10 лет уровень инновационности страны не изменился, и она находится на крайне низкой стадии развития, несмотря на некоторые успехи и видимый прогресс в оборонной промышленности. Без разработки и реализации срочных мер, направленных на улучшению ситуации, страна окончательно проиграет конкуренцию передовым странам в научной и технологической сферах.

Литература

1. ГОСТ Р 54147-2010: Стратегический и инновационный менеджмент.

2. Инновационная экономика России. Реалии и перспективы [Электронный ресурс]: - Режим доступа: http://do.gendocs.ru/docs/index-127156.html (дата обращения: 29.11.2015)

3. Иващенко, Н.П. и др. Экономика инноваций [Текст] / Н.П. Иващенко, А.А. Энговатова, М.С. Шахова, М.С., М.С. Антропов, И.И. Коростылева // М.: Макс Пресс. – 2014. – 348 с.

4. Основные факторы построения инновационного промышленного производства [Электронный ресурс]: - Режим доступа: http://www.pandia.ru/805473/ (дата обращения: 24.12.2015)

5. Показатели затрат на инновации [Электронный ресурс]: - Режим доступа: http://1aya.ru/referat6/textbook-14617.php (дата обращения: 14.01.2016)

6. Рыжкова, Т.В., Колесниченко, К.В. Венчурное предпринимательство в системе инновационного развития экономики

[Текст] / Т.В. Рыжкова, К.В. Колесниченко // Вестник Московского государственного университета леса - Лесной вестник. – 2010. – № 2(71). – С.164-169.
7. Рыжкова, Т.В., Колесниченко, К.В. Методы оценки венчурных предприятий [Текст] / Т.В. Рыжкова, К.В. Колесниченко // Вестник Московского государственного университета леса - Лесной вестник. – 2011. – №6(82). – С. 161-164.
8. Рыжкова, Т.В. Теоретические аспекты экономической оценки эффективности деятельности предприятий [Текст] / Т.В. Рыжкова // Вестник Московского государственного университета леса – Лесной вестник. – 2013. – № 4(96). – С. 201-205.
9. Рыжкова, Т.В. Планирование инновационного развития экономики. Сборник статей открытой научно-практической конференции преподавателей кафедры экономики: Инновационное развитие экономических систем: тенденции и перспективы. Ярославль-Королёв: ФТА, «Канцлер». – 2014. – С. 41-50
10. Секерин, В.Д., Горохова, А.Е. Инновационная среда как фактор эффективности коммерциализации инноваций [Текст] / В.Д. Секерин, А.Е. Горохова, А.Е. // Известия МГТУ. – 2014. – №2 (20). – С. 39-43.
11. Структура и содержание инновационной среды [Электронный ресурс]: - Режим доступа: http://studme.org/44992/investirovanie /struktura_soderzhanie innovatsionnoy_sredy (дата обращения: 17.12.2015)
12. Суслов, В.И. Толковый словарь «Инновационная деятельность». Термины инновационного менеджмента и смежных областей (от А до Я). 2-е изд., доп. Новосибирск: Сибирское научное издательство. – 2008. – 18 с.

ОЦЕНКА РЕСУРСНОГО ПОТЕНЦИАЛА ПРЕДПРИЯТИЯ

Махова Мария Николаевна, студентка 3 курса кафедры Экономики
Научный руководитель: **Рыжкова Татьяна Васильевна**, к.э.н., доцент кафедры Экономики

В статье представлены результаты исследования теоретических и методологических положений оценки ресурсного потенциала предприятия. Выявлены факторы, влияющие на величину, динамику, уровень и эффективность использования РПП, систематизированы существующие подходы и методы оценки потенциалов предприятия в структурно-элементном разрезе.

Ресурсный потенциал предприятия, оценка РПП, методы оценки, факторы, влияющие на РПП.

EVALUATION OF THE RESOURCE POTENTIAL OF THE ENTERPRISE

Mahova Maria, 3rd year student of the Department of economics
Scientific adviser: **Ryzhkova Tatyana,** Candidate of Economic Sciences, Assistant Professor of the Department of economics

Research of theoretical and methodological bases of an assessment of the resource potential of the enterprise, factors influencing the size, dynamics, level and efficiency using the resource potential of the enterpriseis presented in article. Also the existing estimates of the enterprise's potential for each one are systematized.

The resource potential of the enterprise, approaches of an assessment, the assessment methods, factors influencing the size, dynamics, level and efficiency using the resource potential of the enterprise.

Изучение ресурсного потенциала, подходов и методов его оценки важно как для предприятия, так и для экономики страны в целом. Отсутствие всеобщей, универсальной, официально признанной и принятой системы взглядов на изучение, формирование, анализ, оценку, планирование, организацию использования и управление РПП определяет актуальность этой проблемы [13].

Принятие любого управленческого решения о производстве продукции или услуг основывается, в первую очередь, на возможностях имеющегося ресурсного потенциала предприятия. Отсюда вытекает необходимость измерения его величины, а, следовательно, изучения методологии оценки ресурсного потенциала предприятия и выявления способов повышения его уровня и эффективности использования.

Ресурсный потенциал и его структурные элементы были определены в предыдущем исследовании темы.

Ресурсный потенциал – это обеспечивающая эффективное использование ресурсов, устойчивое стратегическое развитие предприятия, его конкурентоспособность на рынке система всех структурных элементов потенциала предприятия, включая имеющиеся и возможные, а также сложившиеся экономические и

политические условия на рынке товаров и услуг, формирующаяся под воздействием внешних и внутренних факторов [определение автора и научного руководителя].

Таблица 1 – Состав ресурсного потенциала предприятия

	Элементы РП	***Составляющие***
РПП	Осязаемый потенциал	• Технический потенциал • Финансовый потенциал • Кадровый потенциал • Материальный потенциал
	Неосязаемый потенциал	• Технологический • Инфраструктурный • Организационный • *Маркетинговый* • Управленческий • Имиджевый • *Интеллектуальный* • Информационный • *Инновационный*

Перед тем, как погрузиться в исследуемую проблему, особое внимание следует уделить определению таких понятий, как методология, метод и методика исследования.

Методология есть система принципов и способов организации, построения теоретической и практической деятельности, а также учение об этой системе.

Метод исследования – это совокупность определенных правил, приемов, способов, норм познания и действия.

Методика – описание объекта и процедур изучения, способов фиксации и обработки полученных данных. На основе определенного метода может быть создано множество методик [1, С.3-4].

Следует отметить, что, несмотря на многочисленные знания, труды и большой опыт ведения аналитической и оценочной деятельности величин, значений, событий, процессов, явлений в разных областях науки и практики единой позиции в отношении определения сути анализа и оценки пока не сформировано. В таблице 2 представлены определения анализа и оценки как экономических категорий, сформулированные авторами, занимающимися изучением данного вопроса.

Обзор определений термина «оценка» позволил выявить ряд недостатков, основным среди которых является отождествление большинством авторов понятий «анализ» и «оценка», что недопустимо, поскольку оценка представляет собой только часть анализа. Считаем необходимым, ввести в оборот определение оценки, как процедуры, состоящей в рассмотрении каждого показателя,

полученного в результате анализа, с точки зрения соответствия его уровня нормальному или заданному значению; в выявлении факторов, обусловивших величину показателя, и возможных его изменений под воздействием того или иного фактора; в установлении необходимого перспективного значения показателя и способов достижения этой величины.

Таблица 2 — Определения анализа и оценки

Авторы	*Определения*
Райзберг Б. А.	«Информационной основой анализа и оценки ресурсного потенциала любой организации служит их отчетность, содержащая сведения, данные об изменении состояния организации за отчетный период»
Батова Т. Н., Васюхин О. В., Павлова Е. А., Сажнева Л. П.	«Анализ и оценка имеют одинаковое значение при определении уровня ресурсного потенциала предприятия»
Шеремет А. Д., Негашев Е. В, Гаврилова А. Н., Попов А. А., Фридман А. М.	«Оценка – есть часть анализа, поскольку цель анализа не только как оценки состояния прошлой деятельности на момент анализа, но и оценки будущего потенциала предприятия, то есть прогнозной оценки»
Скрынник Е. Е.	«Анализ – есть часть оценки состояния потенциала предприятия. Является методом проведения оценки при выполнении необходимых расчетов»
Николаева Т. П.	«Оценка как вид анализа»

Поскольку оценка РПП выполняет измерительную, регулирующую и стимулирующую функции, ее целью является повышение эффективности текущего управления предприятием при купле-продаже, инвестировании, реструктуризации, кредитовании, страховании, налогообложении и др. случаях.

Оценка РПП должна соответствовать определенным требованиям и критериям, среди которых обязательным условием должна быть актуальность, полнота, объективность, системность, комплексность, независимость, поэтапность, поэлементность [11, 12]. На первом этапе оценки РПП осуществляется постановка задачи и анализ объекта исследования, после чего проводится сбор исходной информации, которая в дальнейшем подвергается анализу и первичной обработке. По результатам анализа отбираются факторы, определяющие объект исследования, строится экономико-математическая модель, решение и экономико-математический анализ полученных результатов. На основе полученной информации оценивается РПП.

Для управления величиной и оптимизации РПП особое внимание при его изучении и оценке следует уделить факторам, определяющим величину, динамику, уровень и эффективность

использования РП, и определить те из них, которые оказывают наиболее существенное влияние на эти процессы.

В ходе исследования нами установлены и сгруппированы факторы уровня, динамики, уровня и эффективности РПП (рисунок 1).

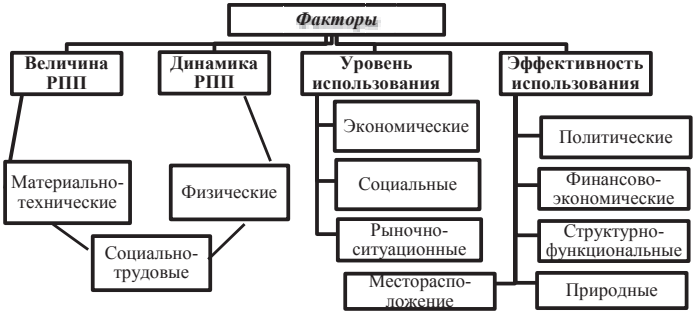


Рисунок 1 – Классификация факторов

Таблица 3 – Подходы к оценке РПП

Подход	Характеристика	Примечание
Затратный подход	Основан на предположении, что затраты на становление предприятия, насыщения его ресурсами являются приемлемым ориентиром для определения стоимостной оценки совокупного ресурсного потенциала предприятия.	Применяется на стадии зарождения производства (происходит насыщение производства ресурсами - формирование, становление предприятия)
Доходный подход	Включает в себя метод капитализации доходов (прямая капитализация), в основе которого лежит расчет текущей стоимости будущих доходов, полученных от использования сбалансированных элементов ресурсного потенциала.	Применяется на стадии роста (происходит быстрое развитие предприятия и период роста доходов от его функционирования)
Сравнительный (рыночный) подход	Основан на сопоставлении анализа текущей стоимости оценки ресурсного потенциала и затрат связанных с формированием сбалансированного ресурсного потенциала при изначальном становлении предприятия.	Применяется на стадии стабильности (в период равновесия - стабильные доходы, сформировавшийся рынок сбыта продукции, создание инфраструктуры и т.д.)
Частный подход	Оценка эффективности использования ресурсного потенциала определяется по одному показателю.	Каждый из этих показателей, независимо от степени деятельности предприятия, характеризует лишь один из аспектов экономической деятельности.

продолжение таблицы 3

Универсальный подход	Нахождение показателя, который бы достаточно полно отражал эффективность использования ресурсного потенциала предприятия и ее изменение за счет объединения определенного количества частных показателей.	Трудности с получением такого показателя из-за количественного состава самих показателей и их сопоставимости.
Ситуационный подход	В качестве критерия эффективности использования ресурсного потенциала при этом подходе выступает выполнение поставленных целей за тот или иной период деятельности.	Сложности с определением показателя из-за различия целей предприятия на разных этапах деятельности.
Результативный подход	Учет перспектив деятельности и развития предприятия как целостного земельно-имущественного и социально-организационного комплекса, исходя из прежнего опыта, достигнутых результатов и сложившихся рыночных условий.	В аналитических расчетах используется прогнозная (вероятностная), а не фактическая хозяйственная информация;аналитические процедуры формирования ставок дисконтирования и капитализации имеют субъективный характер.

Так, величину и динамику РПП определяют материально-технические, физические и социально-трудовые факторы. Уровень использования РПП зависит от экономических, социальных и рыночно-ситуационных факторов. Эффективность использования РПП складывается под воздействием политических, финансово-экономических, структурно-функциональных, природных факторов, а также месторасположения предприятия.

По поводу выбора и использования того или иного подхода к оценке РПП - затратного, доходного, рыночного, частного, универсального, ситуационного или результативного среди ученых сложились разные мнения. Их обзор представлен в таблице 3. Несмотря на все многообразие основными из них принято считать затратный, сравнительный и результативный подходы [9, 10].

Объяснением тому служит наличие или сравнительно небольшие сроки получения информации для оценки РПП наиболее востребованными на практике подходами.

Что касается методов оценки РПП, представленных в таблице 4, пока сложно определить, какой из них более качественно выполняет свои функции и какой именно следует использовать [14].

Таблица 4 – Методы оценки РПП

Методы оценки	Преимущества	Недостатки
Традиционные финансовые показатели	— Простота внедрения — Простота при использовании в системе материального стимулирования	— Не учитывает факторы внешней среды и последствия принимаемых решений — Отсутствие гибкости системы — Трудности при применении в прогнозировании
Стоимостные оценки (DCF)	— Интегральный показатель – стоимость предприятия — Простота при использовании в системе материального стимулирования	— Неполный охват уровней организации (трудности при учете нефинансовых факторов) — Используемые показатели дублируют информацию
Системы сбалансированных показателей	— Охватывает все уровни организации — Логически взаимосвязанная система показателей — Гибкая система показателей	— Отсутствие интегрального показателя (большое количество разных показателей) — Трудности при применении в системе материального стимулирования — Трудности при внедрении (значительное временные затраты на разработку и проверку значимости показателей системы)
Процессно-ориентированный анализ рентабельность	— Охватывает все уровни организации — Связи между показателями определяются бизнес-процессами — Получение четких сигналов о необходимых изменениях	— Эффективность внедрения системы на предприятиях зависит от количества вспомогательных и общехозяйственных процессов — Трудности при применении в системе материального стимулирования для вспомогательных подразделений
Системы сбалансированных показателей на основе факторов стоимости	— Охватывает все уровни организации — Логически взаимосвязанная система показателей — Интегральный показатель – стоимость предприятия — Простота при использовании в качестве компенсации — Гибкая система показателей	— Трудности при внедрении (значительные временные затраты на разработку и проверку значимости показателей системы) — Отсутствие интегрального показателя (большое количество разных показателей)
Методика объективной интегральной оценки РП на базе математического моделирования	— Существует алгоритм расчета индекса ресурсного потенциала (4 этапа) — Охватывает все уровни организации — Сформирована система показателей оценки рациональности использования ресурсного потенциала.	— Эффективность внедрения системы на предприятиях зависит от количества вспомогательных и общехозяйственных процессов — Используемые показатели дублируют информацию

Оценка на основе построения корреляционно-регрессионной модели	— Позволяет определить структуру каждого вида ресурсов, а именно его удельный вес — Разнообразие показателей, включаемых в корреляционно-регрессионную модель.	— Взаимозависимость между суммами потраченных ресурсов и объемами выпускаемой продукции имеет нелинейный характер
Метод, основанный на цепочке ценностей М. Портера	— Анализ РП проводится по показателям цепочки ценностей, определяющей деятельность, функции и процессы по разработке, производству, продвижению, доставке и поддержке продукта или услуги — Позволяет определить пути повышения конкурентоспособности фирмы по издержкам.	— Получить информацию об издержках других компаний всегда довольно сложно, так как она является конфиденциальной — равнение информации по издержкам не всегда возможно из-за того, что конкурирующие компании стараются использовать отличные друг от друга методы учета для определения затрат.

В рамках основных подходов на практике при оценке РПП используют методы, представленные на рисунке 2.

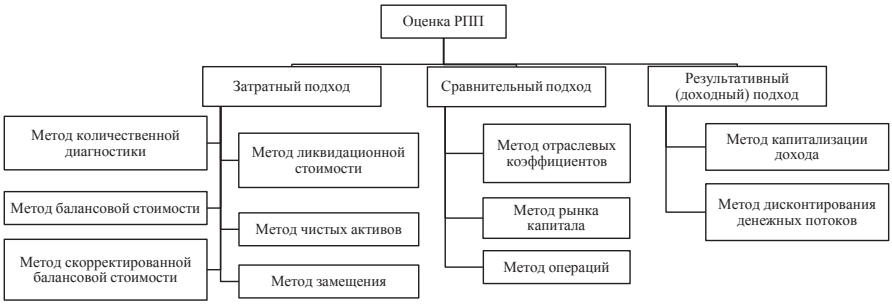


Рисунок 2 – Методы оценки РПП

В зависимости от полученных результатов оценки величины РПП выделяют:

— *высокий* уровень РПП, соответствующий стабильной доле рынка и устойчивому положению на рынке;

— *средний* уровень РПП, соответствующий ситуации, когда произведенная продукция продается, доля рынка не стабильна, но в среднем за период наблюдения поддерживается на определенном уровне;

— *низкий* уровень РПП, характеризуется проблемами с обеспечением предприятия основными производственными фондами,

сырьем, материалами, трудовыми ресурсами, неэффективным их использованием.

Изучая условия и возможности всесторонней оценки использования РПП указанными методами, нами установлено, что только в ходе комплексного исследования каждого элемента ресурсного потенциала предприятия в отдельности, можно полноценно определить уровень и эффективность его использования, а также установить причины, снижающие эффективность предпринимательской деятельности, и выявить резервы его повышения [10].

В процессе выполнения научной работы нами выявлены и систематизированы методы, которые используются для оценки структурных элементов РПП, представленные в таблице 5 [15]. Их насчитывается 14. При оценке научно-технического потенциала предприятия используют 4 метода –пятиблочный, коэффициентный, экспертный и балльный. Тремя методами пользуются при оценке финансового, кадрового и инфраструктурного потенциалов. Организационный, маркетинговый, интеллектуальный и управленческий потенциалы оценивают двумя методами. В оценке материального, технологического, инфраструктурного, имиджевого и информационного потенциалов используют всего один метод.

В оценке шести потенциалов применяется экспертный метод. Комплексный метод, по составляющим и по единичному показателю используют в оценке 3-х потенциалов, балльным методом оценивают 2 потенциала и 9 потенциалов пытаются оценить каким-либо одним методом.

Из чего можно сделать вывод о том, что система оценки РПП является довольно сложным делом, пока имеет фрагментарный характер, находится в стадии разработки, математически не оформлена и, таким образом, представляет собой большое поле деятельности, как для начинающих, так и для маститых ученых.

Кроме того, методы оценки РПП были апробированы на материалах двух предприятий, принадлежащим разным сферам деятельности, что также позволило получить интересную информацию. Несмотря на кажущееся большое разнообразие методов оценки РПП, они не являются универсальными, т.е. не каждый из них позволяет качественно оценить все до одного потенциала, практически ни один из них по разным причинам в полной мере не

отвечает предъявляемым требованиям. Следовательно, и в этом направлении можно продолжать движение.

Таблица 5 – Методы оценки потенциалов предприятия

Методы / ***Потенциал***	Пятибалочная система	Коэффициентный	Экспертный	Бальный	Комплексный	Интегральный	Общенаучные	Оценочные показатели	По составляющим	По единич. показателю	Поэтапный	Качественные	Количественные	Комбинированные
Научно-технический	+	+	+	+										
Финансовый			+		+	+								
Кадровый			+		+		+							
Материальный								+						
Технологический									+					
Инфраструктурный										+				
Инновационный												+	+	+
Организационный									+	+				
Маркетинговый				+							+			
Управленческий			+							+				
Имиджевый			+											
Интеллектуальный			+						+					
Информационный					+									

Можно предположить, что не должно быть стандартной методики для оценки любого элемента РПП, и каждый потенциал необходимо рассматривать отдельно.

Литература

1. Бронникова, Т.С., Котрин, В.В. Развитие методологии формирования рыночного потенциала предприятия [Текст] / Т.С. Бронникова, В.В. Котрин // Монография. – Королёв. – 2012.
2. Ильченко, А.Н., Абрамова, Е.А. Оценка инфраструктурного потенциала [Текст] / А.Н. Ильченко, Е.А. Абрамова // Современные наукоемкие технологии. Региональное приложение. – 2010. – С 28-35.
3. Колесник, Е.Н. Оценка и развитие маркетингового потенциала предприятий [Текст] / Е.Н. Колесник // Диссертация к.э.н. – Код специальности: 08.00.05 «Экономика и управление народным хозяйством». Тольятти. – 2014.
4. Королёв, О.Л. Методика оценки информационного потенциала предприятия [Текст] / О.Л. Королёв // Ученые записки Таврического национального университета имени В.И. Вернадского. – 2011. – С 109-113.
5. Кузнецов, В.В. Организационный потенциал предприятия [Текст] / В.В. Кузнецов // Учебное пособие. Ульяновск. – 2007.

6. Лаптева, Е.А. Развитие методов оценки инновационного потенциала промышленных предприятий [Текст] / Е.А. Лаптева // Диссертация к.э.н. – Код специальности: 08.00.05 «Экономика и управление народным хозяйством». Саратов. – 2014.
7. Мироседи, С.А., Щедрина, А.В. Методы оценки кадрового потенциала предприятия [Текст] / С. А. Мироседи, А.В. Щедрина // Волжский политехнический институт. – 2013.
8. Морозова, Л.Э., Бортник, О.А. Экспертные методы и технологии комплексной оценки экономического и инновационного потенциала предприятий [Текст] / Л.Э. Морозова // Учебное пособие. Москва. – 2009.
9. Окорокова, Л.Г. Методология и принципы эффективного использования и формирования ресурсного потенциала промышленных предприятий [Текст] / Л.Г. Окорокова // Диссертация д.э.н. – Код специальности: 08.00.05 «Экономика и управление народным хозяйством». Москва. – 2003.
10. Попов, М.С., Лутовинов, П.П. Использование категорий потенциала в системе принятия решений по управлению производственно-инновационной деятельностью предприятия [Текст] / М.С. Попов, П.П. Луговинов // Вестник ЮУрГУ. – 2010. – №20. – С. 57-62.
11. Рыжкова, Т.В., Колесниченко, К.В. Венчурное предпринимательство в системе инновационного развития экономики [Текст] / Т.В. Рыжкова, К.В. Колесниченко // Вестник Московского государственного университета леса - Лесной вестник. – 2010. – № 2(71). – С.164-169.
12. Рыжкова, Т.В., Колесниченко, К.В. Методы оценки венчурных предприятий [Текст] / Т.В. Рыжкова, К.В. Колесниченко // Вестник Московского государственного университета леса - Лесной вестник. – 2011. – №6(82). – С. 161-164.
13. Рыжкова, Т.В. Теоретические аспекты экономической оценки эффективности деятельности предприятий [Текст] / Т.В. Рыжкова // Вестник Московского государственного университета леса – Лесной вестник. – 2013. – № 4(96). – С. 201-205.
14. Свободин, В.А. Вопросы определения и эффективности производственного потенциала [Текст] / В.А. Свободин // АПК: экономика определении, управление. – 2006. – №3. – С. 27-30.
15. Стексова, С.Ю. Ресурсный потенциал строительного предприятия и оценка эффективности его использования [Текст] /

С.Ю. Стексова // Диссертация к.э.н. – Код специальности: 08.00.05 «Экономика и управление народным хозяйством». С–Пб. – 2011.
16. Тертышник, М.И. Оценка производственного потенциала предприятия и научно-технического уровня производства [Текст] / М.И. Тертышник // Известия ИГЭА. – 2012. – №1 (81). –С. 98-102.
17. Шатрова, А. П. Алгоритм внедрения методики оценки ресурсного потенциала предприятия сферы услуг [Электронный ресурс]: Режим доступа: http://www.m-economy.ru/art.php?nArtId (дата обращения 30.11.2014)
18. Шевченко, А.А. Оценка финансового потенциала при определении способности предприятия к модернизации [Текст] / А.А. Шевченко // Юго-Западный государственный университет. Курск. – 2011.

РАЗРАБОТКА БИЗНЕС-ПЛАНА ИНВЕСТИЦИОННОГО ПРОЕКТА ПО ПРОИЗВОДСТВУ СУХОГО МОЛОКА В ВИДЕ ПРОДУКТА ИМПОРТОЗАМЕЩЕНИЯ

Метёлкина Кристина Геннадьевна, студентка 4 курса кафедры Экономики
Научный руководитель: **Бронникова Тамара Семеновна**, к.э.н., доцент кафедры Экономики

На фоне санкций на ввоз в Россию молока и молочных продуктов со стороны ЕС, США, Австралии, Норвегии и Канады отечественный рынок претерпел серьёзные изменения. Остро ощущается потребность восполнить отсутствующие на отечественном рынке товары, которые ранее Российская Федерация импортировала. В данной статье рассматривается предложение бизнесу для производства импортозамещающего товара как разработка бизнес-плана на примере производства сухого молока и доказывается эффективность данной идеи при определённых исходных данных.

Импортозамещение, инвестиционный проект, бизнес план.

BUSINESS PLAN OF THE INVESTMENT PROJECT FOR THE PRODUCTION OF MILK POWDER IN THE FORM OF IMPORT-SUBSTITUTION PRODUCT

Metelkina Kristina, 4rd year student of the Department of economics

Scientific adviser: **Bronnikova Tamara**, Candidate of Economic Sciences, Associate Professor of the Department of economics

The domestic market has undergone major changes against the background of the sanctions on the import of milk and milk products from the EU, US, Australia, Norway and Canada by Russia. There is a great need to make up for the missing items in the domestic market that were previously imported by Russian Federation. This article discusses the business proposal for the production of import-substituting goods as the development of a business plan as an example the production of milk powder and proved the effectiveness of this idea under certain input data.

Import-substitution, investment project, business plan.

Бизнес-план – это общепринятая в мировой практике форма представления деловых предложений и проектов, содержащая развёрнутую информацию о производственной, сбытовой и финансовой деятельности предприятия и оценку перспектив, условий и форм сотрудничества на основе баланса собственного экономического интереса инициатора проекта и партнеров, инвесторов, потребителей и конкурентов в достижении социально-экономических целей бизнес - проектов [4, С.16].

Бизнес-план представляет собой взаимосвязанную совокупность видов планов: стратегического, тактического и оперативного, так как на первый год составляется с помесячной детализацией, а на второй – с поквартальной [5].

За год с момента введения запрета на ввоз в Россию молока и молочных продуктов из США, ЕС, Австралии, Норвегии и Канады [1], отечественный рынок серьёзно изменился. Объемы импорта масла, сухого молока и сыра значительно снизились, так как именно по этим молокоёмким категориям Россия была наиболее импортозависима. За период с июля 2013 года по июль 2014 года было ввезено 8,5 тыс. т. сухого цельного молока, а за тот же период 2014-2015 гг. - всего 2,4 тыс.т, что в 3,5 раза меньше; сухого обезжиренного молока - в 6,3 раза меньше (45 и 7,1 тыс. т соответственно) [7].

Наибольший объем от общего производства сухих молочных продуктов приходится на сухое цельное молоко распылительной сушки и его разновидности. К основным видам сухих молочных продуктов относятся: молоко коровье цельное сухое 20 и 25%-ной

жирности, молоко сухое, молоко коровье обезжиренное сухое, сливки сухие, сливки сухие высокожирные, продукты сухие кисломолочные. Сухим молочным продуктом может называться молочный продукт, из которого удалена влага до значений массовой доли сухих веществ 96,0% и более.

Сухие молочные продукты по структуре относятся к сыпучим порошкам. Они вырабатываются из нормализованного пастеризованного сгущенного цельного или обезжиренного молока, сливок, пахты высушиванием на распылительных или вальцовых сушилках. Массовая доля влаги в сухих продуктах колеблется от 2 до 7%. Структура и размер частиц сухих молочных продуктов зависит от способа сушки.

Сухое молоко распылительной сушки состоит из агломерированных частиц. Для пленочного молока, высушенного на вальцовых сушилках, структура в виде измельченных пленок (чешуек).

Сухое молоко употребляется в качестве напитка, для изготовления которого сухой порошок разводится кипяченой водой. Готовый продукт обладает теми же полезными свойствами, что и свежее пастеризованное молоко, и применяется в основном для приготовления кулинарных блюд, является составным ингредиентом детского питания, а также применяется для изготовления косметических средств, для изготовления хлебобулочных изделий, при консервировании и т.д.

Таким образом, производство сухого молока (растворимого порошка, получаемого в результате технологической обработки пастеризованного коровьего молока) является перспективным направлением развития бизнеса.

Производство и реализация сухого молока имеют большой спрос в определенных производственных сферах. Более того, производство сухого молока обладает перспективой развития в молочный комбинат, который будет производить весь ассортимент продукции: йогурты, ацидофилин, кефир, ряженку, простоквашу, сгущенное молоко, сыр, сметану, сливочное масло, сливки и т.д. В последние годы увеличивается производство сухих смесей для мороженого, сухих сливок с пищевыми наполнителями. Расширяется ассортимент сухих молочных продуктов детского и диетического питания.

Так же велики и перспективы расширения производства сухого молока и выхода на международный рынок.

Бизнес по производству сухого молока совершенно не требует крупных капиталовложений, сырье для производства в большинстве своем весьма дешево, а требования ГОСТ и других регламентирующих документов вполне лояльны.

Производство сухого молока на рынке России достаточно стабильно и постепенно наращивает свои объемы. Исследования последних 5 лет показывают увеличение спроса на сухое молоко на 1,4% [7], что стимулирует
развитие предпринимательства по его производству, так как данное предпринимательство является сейчас достаточно выгодным делом.

Для того, чтобы не быть голословным в том, что производство сухого молока может быть прибыльным делом, в конце статьи на базе теоретических основ экономики и управления инновационным развитием предприятия [6] и методологии бизнес-планирования [4], подтверждена эффективность предложения бизнесу по созданию инновационного предприятия по производству сухого молока.

В статье рассмотрены важнейшие разделы бизнес-плана, описывающие все виды деятельности от анализа рынка, разработок планов маркетингового, производственного, организационного, инвестиционного, финансового до оценки эффективности инвестиций в бизнес-проект [2, С.34].

Для начала проводится анализ рынка и разработка плана маркетинга. Это и является первыми разделами бизнес-плана. Для того, чтобы выяснить, нужен ли потребителем подобный товар, пользуются ли потребители сухим молоком при производстве молочной продукции, в каком объеме они готовы приобрести товар, необходимо сделать оценку конкурентоспособности продукта.

Для оценки конкурентоспособности товара было проведено анкетирование потенциальных потребителей [3]. Более 70% респондентов заинтересованы в данной продукции. Ранее они использовали иностранные товары, но готовы покупать отечественный, так как для них не имеет значения страна производителя. Данный вид продукции привлекает потребителя, так как отмечается недостаточно широкий ассортимент молочной продукции и молочные сухие смеси являются альтернативой.

Молочных заводов и фабрик в России насчитывается 71. В большей степени потенциальными покупателями сухого молока

могут стать более половины заводов и фабрик. Данные заводы, благодаря многолетнему опыту работы в нише, прекрасно знают, как именно работать с продукцией и в каком количестве её закупать.

Оценка конкурентоспособности (таблица 1) осуществлена относительно одного из лучших продуктов, имеющихся на рынке сухого молока на данный момент, а именно «Сухое молоко» Распак.

Таблица 1 – Оценка конкурентоспособности продукта

Показатель	Ед. изм.	Весовой коэффициент, bj	M1 (новая)			M2 (конкурент)		
			Значение показателя					
			Количественное	Балльное	Средневзвешенное	Количественное	Балльное	Средневзвешенное
				aij	bij		Aij	bij
Органолептические показатели								
Вкус и запах (Свойственный свежему пастеризованному молоку при распылительной сушке и перепастеризованному (кипяченому) молоку при пленочной сушке, без посторонних привкусов и запахов)	Балльная шкала 1-10	0,15	-	10	1,5	-	9	1,35
Консистенция (мелкий сухой порошок или порошок, состоящий из гломерированных частиц сухого молока)	Балльная шкала 1-10	0,15	-	9	1,35	-	9	1,35
Цвет (белый, с легким кремовым оттенком для распылительного молока; кремовый для пленочного молока)	Балльная шкала 1-10	0,15	-	10	1,5	-	9	1,35
Физико-химические показатели								
Массовая доля влаги,	%	0,07	3	10	0,7	4	9	0,63
Массовая доля жира,	%	0,07	20	10	0,7	20	10	0,7
Массовая доля белка,	%	0,07	23	10	0,7	23	10	0,7
Индекс растворимости	$см^3$	0,1	0,2	10	1	0,3	9	0,9
Микробиологические показатели								
Количество мезофильных аэробных и факультативно анаэробных микроорганизмов в 1,0 г сухого молока	КОЕ	0,14	50 000	10	1,4	50 000	10	1,4
Средняя цена за 1 кг	Руб.	0,1	42	10	1	68	9	0,9
Сумма средневзвешенных балльных оценок		1,0			9,85			9,28

Анализ результатов (таблица 1) показал, что сухое молоко по органолептическим, физико-химическим, микробиологическим и

ценовым показателям является конкурентоспособным относительно лучшего представителя сухого молока конкурента. Сумма средневзвешенных бальных оценок продукта конкурента равняется 9,28, а продукта данного проекта – 9,85 единиц, что подтверждает его конкурентоспособность.

Следующим этапом оценки конкурентоспособности продукта является поиск и оценка наиболее выгодного для компании поставщика сырья для производства сухого молока. В качестве сырьевой базы для производства сухого молока, как правило, используется наиболее недорогое маложирное молоко (переводить хороший продукт на сухое просто нецелесообразно), а требования ГОСТ и других регламентирующих документов вполне умеренные и нежёсткие. Таким образом, интерес представляют молочные фермерские хозяйства Московской области, способные удовлетворить все потребности на выгодных условиях. В ходе исследования были выявлены три лучших варианта. Оценка поставщиков осуществлялась по следующим критериям:

- Цена за единицу товара (1 литр молока);
- Стоимость доставки;
- Качество товара [2].

Результаты анализа показали, что «Фермерское хозяйство Сергиев-Посад» является наиболее выгодным поставщиком маложирного сырого молока, используемого для производства сухого обезжиренного молока (СОМ) и цельного сухого молока (ЦСМ).

Целевой аудиторией производимой продукции будут предприятия пищевой промышленности, производящие мороженое, кондитерские изделия, сгущенное молоко, детские сухие смеси, ритейлеры, расположенные в регионе функционирования предприятия.

Произведя расчёты по поставкам и производственным мощностям оборудования предприятия, сделан вывод о том, что максимальные объемы производства составят 1,2 тонны СОМ в сутки, потенциальный объем спроса на продукт в первый год запуска производства составит 135 тонн в месяц, во второй – 230 тонн в месяц, в третий – 270 тонн в месяц.

В России цены на сухое молоко достаточно низки: примерно от 40 до 62 тыс.руб. за тонну.

На первых этапах цены не будут существенно отличаться от цен конкурентов, однако будут немного снижены, что необходимо для привлечения клиентов при выходе на рынок.

Для оптовых покупателей предусматриваются акции и собственная система скидок, а в дальнейшем для постоянных потребителей будут установлены специализированные цены.

После проведения маркетингового исследования организация получит информацию относительно того, что продавать и кому, а также о том, как продавать и как стимулировать продажи. Это имеет решающее значение для достижения конкурентных преимуществ. Результаты исследования могут предопределить изменение целей и стратегий деятельности организации в целом.

Основным направлением маркетингового плана является проведение рекламы. Для начала следует установить щит в месте, где происходит большое скопление нашей целевой аудитории. Так же продукция должна быть представлена на выставке. И в дальнейшем предприятие рекламирует свой товар посредством проведения промо-акций, дегустаций, конкурсов, не забывая о том, что основной источник информации для потребителей – это СМИ и Интернет.

Следующий этап бизнес-плана - план производства [4].

Приняты следующие исходные данные: производственная площадь состоит из производственного цеха, складского и офисных помещений. Площадь производственного цеха – 500 кв.м., площадь склада – 500 кв.м., площадь офиса – 100 кв.м. Производство осуществляется на оборудовании – Вакуум-выпарная установка для молока и сыворотки.

Определена мощность и годовая производственная программа выпуска продукции - мощность – 270 тонн в месяц, а годовой выпуск продукции равен 3240 т/год.

Для изготовления 1 т сухого молока необходимо 2,2 т сырого молока, водоснабжение, электричество и тара. На основе этих данных определена сумма затрат на годовую производственную программу. Таким образом, для изготовления 3240 т сухого молока в год необходимо 115894800 руб. на приобретение оборотных средств.

По результатам расчета на оплату труда сотрудникам, занятым в производстве сухого молока, потребуется 12090 тыс. руб.

Расчет себестоимости затрат на годовую программу производства, выполненный калькуляционным методом представлен в таблице 2 [3].

Таблица 2 – Калькуляция себестоимости

№ п/п	Шаг расчета, год	1		2		3		4		5	
	Наименование статей затрат	З-ы на год. программу	З-ы на ед.	З-ы на год. программу	З-ы на ед	З-ы. на год. программу	З-ы на ед	З-ы на год. программу	З-ы на ед	З-ы на год. программу	Затраты на единицу
1	Прямые мат.затты	109635,05	35,77	115894,80	35,77	115894,80	35,77	115894,80	35,77	115894,80	35,77
2	Фонд оплаты труда ОПП	7917,92	2,58	8370,00	2,58	8370,00	2,58	8370,00	2,58	8370,00	2,58
3	Социальный взнос	2375,38	0,78	2511,00	0,78	2511,00	0,78	2511,00	0,78	2511,00	0,78
4	Накладные расходы	12426,02	4,21	13138,50	4,21	13124,85	4,20	13112,42	4,20	11010,60	4,20
5	Амортизационные отчисления	180,00	0,06	165,00	0,05	151,35	0,05	138,92	0,04	127,61	0,04
6	Себестоимость без амортизации	121881,07	39,92	128868,30	39,93	128868,30	39,93	128868,30	39,93	126777,79	39,93
7	Себестоимость с амортизацией	122061,07	39,98	129033,30	39,98	129019,65	39,97	129007,22	39,97	126905,40	39,97
8	Условно-постоянные издержки	2132,73	0,70	2257,50	0,70	2243,85	0,69	2231,42	0,69	129,60	0,69
9	Условно-переменные издержки	119928,34	39,13	126775,80	39,13	126775,80	39,13	126775,80	39,13	126775,80	39,13

На основе данных об общих (годовых) условно-постоянных издержках, средних условно-переменных издержках (на 1 тонну сухого молока), и годовой выручки от реализации сухого молока, построен график точки безубыточности.

Аналитический расчет и графический метод оценки точки безубыточности показывают, что в первый год точка безубыточности наступит при объеме производства (реализации) сухого молока в количестве 748,82 т (рисунок 1).

Коэффициент устойчивости проекта составляет 23,11%, что намного меньше предельно допустимого значение, равного 70%, а это означает, что данный проект имеет высокую устойчивость.

Следующий раздел бизнес-плана – это организационный план. Организационный план начинается со списка членов руководящей группы, их кратких биографических справок и предполагаемого круга обязанностей каждого.

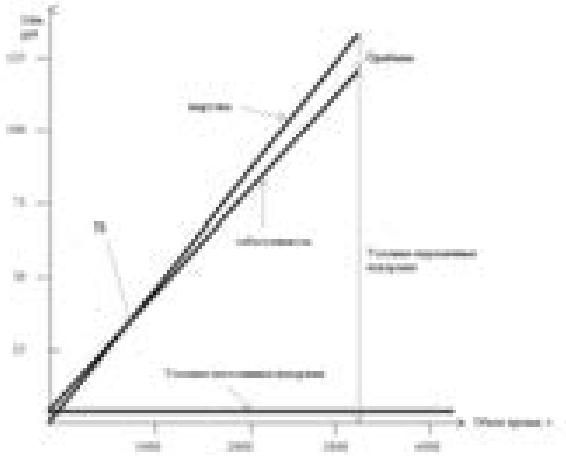


Рисунок 1− График точки безубыточности проекта

Для четкого определения круга обязанностей каждого сотрудника предприятия составляются должностные инструкции.

Организационно-правовая форма собственности данного предприятия – общество с ограниченной ответственностью. ООО – это учрежденное одним или несколькими юридическими и/или физическими лицами хозяйственное общество, уставный капитал которого разделён на доли; участники общества не отвечают по его обязательствам и несут риск убытков, связанных с деятельностью общества, в пределах стоимости принадлежащих им долей или акций в уставном капитале общества.

Планируемое предприятие «Королёвская Молочная Компания СухМол» (сокращенно «КМК СухМол») действует согласно типовой форме устава, принятой законодательством РФ.

Все решения принимаются генеральным директором предприятия с учетом предложений и пожеланий работников предприятия и являются обязательными к выполнению. Планируется трёхсменный режим работы и повременная система оплаты труда.

Исходной информацией для определения размеров инвестиций в бизнес-проект принимаются стоимость основных средств и прирост оборотного капитала [2]. Данный бизнес-план не предусматривает наличие собственного капитала, а все расчеты инвестиционных издержек, формы и источники их финансирования осуществляются с использованием заёмных средств, которые в составляют – 12 299 тыс. руб.

В отчете о финансовых результатах деятельности определена выручка по годам реализации проекта, себестоимость продукции, балансовая прибыль, налоги и обязательные отчисления в бюджет, чистая прибыль и нераспределенная прибыль.

При расчете денежных потоков для оценки коммерческой эффективности проекта определены коэффициенты дисконтирования по годам реализации проекта. Основным экономическим нормативом, используемым при дисконтировании, является норма дисконта E (Rate of Discount), выражаемая в долях единицы или процентах в год [3, С.155].

Для данного бизнес-проекта принята норма дисконта, равная 18% (E = 0,18), исходя из действующей на момент разработки бизнес-плана ключевой ставки ЦБ РФ – 11%.

Эффективность – это категория, отражающая соответствие проекта целям и интересам его участников. Осуществление эффективных проектов увеличивает поступающий в распоряжение общества внутренний валовой продукт (ВВП), который затем делится между участвующими в проекте субъектами – предприятиями, акционерами и работниками, банками, бюджетами разных уровне и прочее. Поступлениями и затратами этих субъектов определяются различные виды эффективности проекта [2].

В международной практике обоснования инвестиционных проектов используется несколько показателей, позволяющих подготовить решение о целесообразности (нецелесообразности) вложения средств [4].

Значение показателя внутренней нормы доходности (Евн) определено методом подбора такой нормы дисконта, при которой чистый дисконтированный доход (ЧДД) за экономический срок жизни инвестиций (5 лет) будет равен нулю [1]. Внутренняя норма дисконта (ВНД) в данном бизнес-плане проекта равна 110 %.

На рисунке 2 приведен график финансового профиля проекта. На этом графике представлены с учётом срока экономической жизни инвестиций (5 лет) денежные потоки проекта без учёта дисконтирования (кривая ЧДП); с учётом дисконтирования при E= 0,18 (кривая ЧДД) и кривая ЧДД при значении внутренней нормы доходности - Евн =1,1.

Анализ значений показателей подтверждает экономическую эффективность предлагаемого бизнес - проекта по производству сухого молока КМК «СухМол» в городе Королёве.

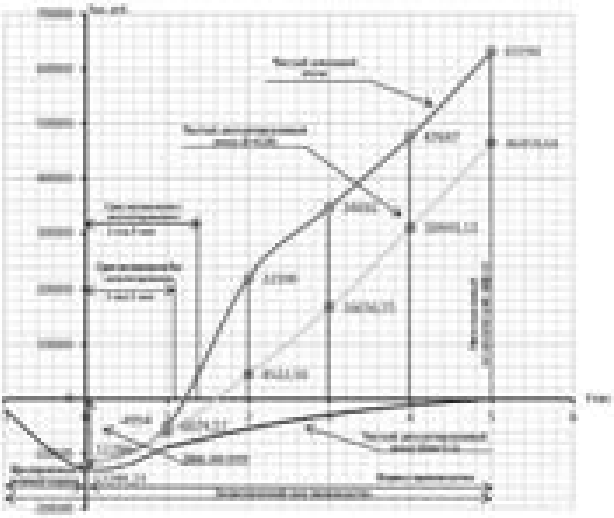


Рисунок 2- График взаимосвязи финансовых показателей проекта (финансового профиля)

Литература

1. Постановление Правительства Российской Федерации от 7 августа 2014 г. N 778 г. Москва "О мерах по реализации Указа Президента Российской Федерации от 6 августа 2014 г. N 560 "О применении отдельных специальных экономических мер в целях обеспечения безопасности Российской Федерации""
2. Бронникова Т.С. Учебно-методическое пособие для выполнения курсового проекта (работы) [Текст] / Бронникова Т.С.: учебно-методическое пособие, «Канцлер» - Королёв, 2014 – 80 с.
3. Бронникова, Т.С. Развитие методологии формирования рыночного потенциала предприятия [Текст] / Т.С. Бронникова, В.В. Котрин: монография, - Королёв, ФТА. 2012 - 134 с.
4. Бронникова Т. С., Разработка бизнес-плана проекта. [Текст] / Т.С. Бронникова: учебное пособие, "Инфра-М" 2016 – 224 с.
5. Попов, В.М. Сборник бизнес-планов. С рекомендациями и комментариями [Текст]/ В.М.Попов, С.И.Ляпунов, С.Г.Млодик: учебно-методическое пособие - КНОРУС, 2007.
6. Старцева Т.Е., Бронникова Т.С. Экономика и управление инновационным развитием предприятия: методологический инструментарий: монография/ Т.Е. Старцева, Т.С. Бронникова.− М.: РУСАЙНС, 2016. – 202 с.

7. Электронный ресурс «Рынок сухого молока и сливок. Текущая ситуация и прогноз 2016-2020гг»: http://alto-group.ru/otchot/marketing/346-rynok-suxogo-moloka-i-slivok-tekushhaya-situaciya-i-prognoz-2014-2018-gg.html (дата обращения: 11.11.2015)

ОРГАНИЗАЦИЯ СТАРТАПОВ В РОССИИ

Мясоедов Сергей Витальевич, Иванов Михаил Алексеевич,
студенты 4 курса кафедры Экономики
Научный руководитель: **Бронникова Тамара Семеновна**, к.э.н.,
доцент кафедры Экономики

В статье рассмотрены понятие, роль, значение стартапов и этапы их создания. Приведены примеры стартапов России в 2015 году. Показаны успехи студентов «МГОТУ» в разработке инновационных проектов. Предложено широко развивать в студенческой среде творческий подход к использованию знаний, поиску и созданию новых инновационных проектов.

Стартап, проект, инновации.

ORGANIZATION OF START-UPS IN RUSSIA

Myasoedov Sergey, Ivanov Mikhail, 4th year students of the Department of economics
Scientific adviser: **Bronnikova Tamara,** Candidate of Economic Sciences, Associate Professor of the Department of economics

The article examines the concept, role, importance of startups and the stages of their creation. The examples of Russian startups in 2015. Shows the progress of the students PHOTO in the development of innovative projects. Proposed widely to develop the student's creative approach to the use of knowledge, creation of new innovative projects.

Startup, project, innovation.

Стартап – представляет инновационную идею, в которой задействуются финансовые, маркетинговые, материальные, производственные и другие ресурсы, для дальнейшей реализации идеи и получении максимальной выгоды. Для того чтобы идея была успешной, нужно уметь чётко ставить цели и создать все условия для её реализации, вложив и задействовав все имеющиеся ресурсы.

Следует отметить, что стремительному развитию стартапов в мире способствует увлечённость идеей и объектом исследования, упорный труд и молодость стартаперов.

Основной причиной создания и успешного развития стартапов является их мобильность при внедрении новых, востребованных потребителями идей, обеспечивающих высокую конкурентоспособность продукции, услуг по сравнению с крупными компаниями.

В последнее время увеличилось количество новых инновационных проектов, не имеющих аналогов, в которые предприниматели вкладывают большие суммы инвестиций.

Для потенциальных стартаперов, в частности студентов «МГОТУ», в данной статье рассматривается структура создания стартапа, представленная на рисунке 1.

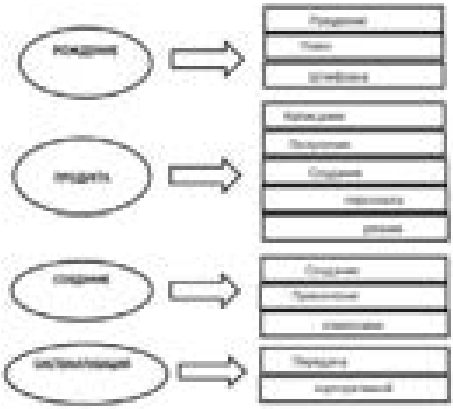


Рисунок 1− Этапы создания стартапа [11]

Рассмотрим краткое содержание каждого этапа.

1. Рождение

Появление компании можно считать с момента, когда появилась конкретная идея. Сюда относится сама идея, её обсуждение, а также шлифовка идеи.

Появление идеи. Существует много способов поиска новых идей. Любой бизнес всегда должен начинаться с идеи, но не всегда даже самая хорошая идея может служить гарантом того, что бизнес будет успешным, так как это сложный и многофакторный процесс.

Розыск сторонников. Под этим пунктом подразумевается поиск сотрудников, которые будут задействованы в ходе создания стартапа,

и вместе с главой проекта обсуждать новые идеи и пути реализации, а также выполнять дополнительные функции.

Обработка идеи (шлифовка). Главный смысл состоит в том, что любая идея не является совершенной и всегда нуждается в доработке, если взглянуть на неё под разными углами. Поэтому на этом этапе происходит доведении идеи до окончательного, финального состояния, улучшения экономических и технологических путей реализации.

Для того чтобы привести идею в конечное, окончательно сформированное состояние, должен быть создан коллектив, который будет объективно смотреть на неё и предлагать своё видение. Поэтому успешный стартап чаще всего это продукт, созданный двумя индивидами, которые вкладывали и способствовали либо зарождению, либо окончательному формированию идеи.

Во время доведения идеи до конечного состояния нужно понимать и знать проблемы, возникающие при принятии решений группой. К недостаткам группового мышления относятся:

1. Иллюзия неуязвимости;
2. Ложная рациональность;
3. Стереотипы- то, что мешает объективно оценивать потенциальных конкурентов;
4. Самоцензура это внутреннее решение соблюдать «групповой консенсус», из-за чего совершается отказ от устверждения сомнений;
5. Привратничество это предохранение друг друга от отрицательной информации, которая может сломать веру группы.

Результатом недостатков группового мышления приведенных выше могут быть приняты не очень качественные решения и введена невыполнимая бизнес-идея, для осуществления которой будет сложно подобрать инвесторов. Обычно, найти инвестора просто почти под каждую обработанную идею. Но нереально почти под любую необработанную.

2. Создание продукта

На данном этапе создатель стартапа начинает реальную подготовку - проводит анализ состояния рынка, а также, обеспеченность ресурсами. Затем привлекаются финансы и люди, включаются связи компании и она выходит на работу в тестовом режиме. После завершения данного этапа продукция будет готова к продаже, а стартап будет готов выйти на рынок.

Разберём основные ступени этого этапа.

Разработка бизнес-плана. Бизнес-план – обязательно письменный документ, суммирующий деловые возможности и перспективы и разъясняющий, как эти возможности могут быть реализованы имеющейся командой. Нужно уделить грамотному бизнес плану достаточно много времени потому что, это главный документ для инвесторов.

Получение инвестиций. Наиболее популярные варианты получить стартовые деньги:

- вложить собственные средства предпринимателя;
- использовать частный венчурный капитал инвестора (бизнес-ангела);
- использовать заемные средства (кредит);
- получить безвозмездные субсидии (гранты).

Любой из представленных вариантов имеет как плюсы, так и минусы:

- собственных средств, в большинстве случаях, практически не хватает;
- для того, чтобы найти бизнес-ангелов обычно нужны знакомства, связи;
- кредит вероятнее получить только под хорошее обеспечение;
- для получения гранта - существует большое число государственных программ, нужно только располагать информацией о них и передать достойный проект.

Получение кредита связано с необходимостью знать показатели, на которые банки концентрирует своё внимание:

- прибыль;
- отчет о поступлении финансов;
- показатель эффективности проекта;
- показатель рентабельности;
- присутствие залога;
- присутствие маркетингового изучения рынка проекта.

Из этого следует, что нужно довольно большое число документов, отдельные из них стартап - компания не может предоставить.

Субсидия (грант) предоставляется лицу среднего или малого предпринимательства на основе конкурса при условии, что конкурсант прошел кратковременное обучение (не менее сорока часов), предоставил бизнес-план и отвечает следующим критериям:

- реализовывает свою деятельность не более чем 1 год, при условии подтверждения, расходов на государственную регистрацию ИП, либо юридического лица, покупает основные фонды и оборудование, предназначенное для производства, обеспечение получения франшизы – договор франчайзинга, набор благ и бизнес-модели предоставляющего франшизу, для права пользования брендом, а также других благ необходимых для создания и ведения бизнеса.

Создание офиса (обеспечение помещением). Начинается подбор наиболее подходящего помещения, на основе таких критериев как: стоимость, качество, предназначение стартап-компании. После приобретения в аренду наиболее целесообразного помещения его нужно обставить, исходя из назначения, провести и подключить интернет, установить телефон и другие коммуникации. После этого офис будет готов к поступлению новых работников, покупателей и клиентов.

Наём сотрудников. Набор сотрудников - трудная и кропотливая работа, которая требует основательного и серьезного подхода. Чтобы принять на работу наиболее подходящих сотрудников нужно ясно описать себе требования к потенциальному работнику. Помимо ваших требований следует учесть некоторые критерии:

-наличие вредных привычек, а точнее их отсутствия;

-хорошее отношение к коллективу;

-наличие лидерских качеств;

-проявление активности;

-присутствие положительных отзывов.

Существуют разные методы набора сотрудников, которые нужно знать организатору стартапа.

Работа в тестовом режиме. В создание и формирования товара включается разработка продукта или услуги, создание прототипа-работающую модель (опытный образец). Затем может быть понадобиться внедрение отдельных дополнений, следовательно, необходимо испытать несколько образцов продукта.

Дальше стартует работа с первыми клиентами, анализ недочетов и работа над ошибками, потом работа с основными партнерами, совершенствование механизмов результативного сотрудничества.

3. Создание рынка

Наработка клиентской базы. На данной стадии осваиваются алгоритмы наработки клиентуры, балансируются расходы на привлечение покупателя, прогнозируются и утверждаются расходы на рекламу бизнес-проекта, которая дает гарантию привлечение клиентов, использование результатов маркетинговых исследований прошедшего периода. вступает в силу стадия расширения рынка и агрессивных продаж.

Раскручивание бренда компании. К данной стадии относится создание образа компании, который будет поддерживать имидж компании, а конкретно создание: названия, слогана, логотипа. Чтобы объективно оценить создаваемый имидж компании нужно координировать свои шаги для его развития при помощи таблицы “направления репутационного аудита" (таблица 1):

Таблица 1− Направления репутационного аудита

№ п/п	Направления репутационного аудита	Составляющие
1.	Репутация компании	Успешность, информационная политика, кадровый потенциал
2.	Репутация руководителя компании	Успешность, навыки общения и тп
3.	Активность компании в информационном поле	Индекс цитирования, количественный анализ позитивных и негативных упоминаний
4.	Эффективность работы с отдельными каналами коммуникации	Работа со СМИ, интернет, реклама.
5.	Эффективность работы со СМИ	Качественный анализ эффективности
6.	Оценка реального достижения поставленных задач и целей	Динамика развития имиджа.

Руководствуясь таблицей 1 и составляющими бренда, можно сформировать полноценный положительный образ стартап - компании, который будет притягивать покупателей.

Работа с партнерами. Данная стадия включает в себя поиск возможных партнеров, образование надежных партнерских связей.

Реклама. Этот этап позволяет стартап-компании приобретать своих первых клиентов, которые делятся на 2 группы: восторженные и скептические. Основная задача этого этапа переход клиентов из группы восторженных в постоянные, а замечания группы скептически настроенных – использовать как маркетинговую информацию для усовершенствования качества продукта.

4. Систематизация (системное управление предприятием)

Передача полномочий. Основная доктрина данного пункта очень проста – компания развивается и происходит рост самой

компании и, если все решения будут на одном руководителе, то создатель стартапа не даст развиваться бизнес-проекту. Существуют пути снятия с основателя стартапа различных дел и передачи управления под чужой контроль:

- Делегирование полномочий;
- Передача некоторых полномочий сторонней компании (аутсорсинг)
- консультирование руководителей в различных сферах (консалтинг).

Формирование организационной культуры. В самом начале развития стартапа руководством бизнес-проекта занимаются несколько человек, которые в основном опираются на своего лидера. Со временем в компании появляются новые работники, происходит расширение предприятия, но еще довольно долгое время, корпоративная культура будет формироваться, ориентируясь на лидера и основных работников, благодаря их личностным качествам. Базовые виды корпоративной культуры характерные стартап проектам:

- Партисипативный

Имеет развитие на предприятиях с демократичным типом управления. Для таких организаций характерно: добросовестное выполнение обязанностей, сотрудники работают в команде для достижение общей цели, равное участие в принимаемых решениях и прикладывание равных усилий. Данный вид корпоративной культуры подходит для творческих компаний и всегда будет эффективным.

- Предпринимательский

Основной особенностью таких компаний является руководство, которое ценит в своих сотрудниках: самостоятельность, умение достигать поставленных целей, индивидуальность, активность.

Основным рычагом управления выступает здесь карьера сотрудника и финансовое вознаграждение за труд.

- Авторитарный

В компании с данным типом управления основное место занимает культура власти, которая подразумевает принятие всех решений лично руководителем организации и соблюдение на предприятии строгой иерархической структуры.

С момента создания и развития стартапа существуют два пути формирования внутренней культуры:

1.Трансформация компании из авторитарной в коллективную (органическую), по сути своей в семью, где руководитель компании будет отцом семьи.

2.Обладание руководителем диктаторских черт. Все решения руководитель предприятия принимает лично, но проявляет очень тяжелое давление на своих работников, становится еще более строже по отношению к своим сотрудникам, и намного чаще применяет к ним санкции. Формируется централизация в управлении предприятием и создается жесткая иерархическая организационная культура.

Каждая из представленных видов культур обладает своими преимуществами и недостатками, и результативна для разного типа компаний. Обычно практика показывает, что компании и ее лидерам стоит руководствоваться “подходу по ситуации”, а именно использовать те методы, рычаги управления, и руководство компанией, подходящие, для конкретной ситуации. Первым делом для руководителя нужно выбрать наиболее эффективную культуру конкретно для его компании, чтобы способствовать интенсивному развитию и максимизации прибыли. Обзор успешных стартапов в России в 2015 году приведён в таблице 2 [8].

В данном обзоре представлены разработки проектов из областей IT, высоких технологий, пищевой промышленности, медицины, которые показывают возможности роста и развития в самых разных сферах деятельности - именно в тех отраслях, в которых их авторы являются профессионалами.

Рассмотрим успехи студентов Технологического университета в развитии инновационной деятельности.

Студенты «МГОТУ» в 2015 году приняли участие в проекте «Сколково» Russian Startup Tour 2015 (Московская область).

Магистрант Амежнова Евгения Дмитриевна представила проект «Defence Assistant «Автоматизированное средство анализа уязвимостей объектов и субъектов информационных систем».

Программа «У.М.Н.И.К.» – «Участник молодежного научно-инновационного конкурса», организованного Фондом содействия развитию малых форм предприятий в научно-технической сфере, стартовала в 2007-м году. В Российской академии наук конкурсы по Программе проводятся с 2008-го года. Целью Программы является выявление молодых учёных, стремящихся самореализоваться через инновационную деятельность, и стимулирование массового участия

молодежи в научно-технической и инновационной деятельности путем организационной и финансовой поддержки инновационных проектов [10].

Таблица 2 – Примеры стартапов 2015 года в России

Название стартапа	Направление стартапа
1.Здравпринт	Стартап, родившийся на стыке двух, как могло показаться, совершенно разных направлений: медицины и 3D-печати.Суть состоит в том, что в изготовлении персональных ортезов и фиксаторов для разных частей тела средствами 3D-моделирования и объемной печати. - быстро, точно и с особой эстетикой каждого изделия.
2. HaptonCreek	Майонез без яиц –на свет появился один из самых успешных стартап проектов в пищевой промышленности (майонез Mayo от HaptonCreek). Данный продукт показал, что многие люди стремятся к здоровому, диетическому и правильному питанию!
3.Aerogreen	"Аэрогрин" – один из чисто российских стартапов, громко заявив о себе на международном рынке технологий имеет большие перспективы. Иркутский инженер Юрий Крулин с создателями компании в 2008 году выпускают в свет инновационные ветряные трубы, которые гораздо эффективней, чем трёхлопастные генераторы.
4.AmpStrip	AmpStrip имеющий устройство Band-Aid. Это небольшое устройство(гаджет), которое крепится в виде пластыря на любую часть тела, происходит отслеживание многих показателей организма человека во время тренировок. Несмотря на то, что у Band-Aid много аналогов, в отличии от других гаджетов его можно использовать при любой физической нагрузке (плавание, бег, культуризм, многоборье, игровые виды спорта) и самое главное, что вы никогда не заметите его присутствия.
5.Panorics	Стартапы основанные на технологии пространственной съемки и дополненной реальности, по отдельности имели огромные успехи на рынке технологий. Но компания Panorics (Москва) первая среди них совершила прорыв, создав один из перспективнейших стартапов в России, в котором объединила эти два направления.

Победителями программы «УМНИК» в 2015 году стали проекты студентов «МГОТУ»:

1.Проект «Разработка паропоршневого двигателя для котельных» студента Пахомова Данилы Владимировича.

2.Проект «Разработка и исследование углепластикового КМ на основе полиэфирэфиркетона» магистранта Перевезенцева Владимира Андреевича.

Предлагается широко внедрять в студенческой среде «МГОТУ» для создания стартапов методологический инструментарий,

представленный в работе [5] для поиска новых инновационных идей и создания стартапов.

Литература

1. Гундарин М.В. книга руководителя отдела PR: практические рекомендации.М.2-е изд., дополненное.- СПб.: Питер, 2009.;
2. Дейл Карнеги. Как завоевывать друзей и оказывать влияние на людей. Общ. Ред. Зинченко В.П., Жукова Ю.М., Хасхачих М.И., М., ПРОГРЕСС, 1989г;
3. И. Манн, А. Турусина. Маркетинговая машина. Менеджер становится директором. - 3-е изд.- М.: Манн. Иванов и Фербер, 2010;
4. М. Рыбаков. Как навести порядок в своем бизнесе. Практикум., М., ИКАР, 2011;
5. Старцева Т.Е., Бронникова Т.С. Экономика и управление инновационным развитием предприятия: методологический инструментарий: монография/ Т.Е. Старцева, Т.С. Бронникова.− М.: РУСАЙНС, 2016. – 202 с.
6. Шудра В. Ф., Беличко А.Н., Как подготовить успешный бизнес-план. VOCA, Киев, 1990;
7. Эффективный менеджер. Взгляды и иллюстрации. Хрестоматия: пер. с англ./ Подгот. Дж. Билсберри.- 5-е изд., стер- Жуковский: МИМ ЛИНК, 2001;
8. Электронный ресурс http://bankirf.mirtesen.ru/blog/43438105491/7-uspeshnyih-startapov-2015-goda:-gotovyie-idei-dlya-biznesa
9. Электронный ресурс http://tomtunguz.com/startup-growth-rate-all-time-high
10. Электронный ресурс http://umnik-ras.ru/about_programm.html
11. Электронный ресурс http://knowledge.allbest.ru/management/2c0a65625a2bc78a5d43a89421316d27_0.html.

ИСТОРИЯ РАЗВИТИЯ И ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ САМОРЕГУЛИРУЕМЫХ ОРГАНИЗАЦИЙ

Обухова Екатерина Вадимовна, студентка 4 курса кафедры Экономики
Научный руководитель: **Курдюкова Наталья Олеговна**, к.э.н., доцент кафедры Экономики

В данной статье рассмотрена история развития саморегулирования в мире, а так же основные цели, задачи и

принципы функционирования саморегулируемых организаций в Российской федерации на примере строительной сферы. Приведен анализ состава и распределения СРО в строительстве по субъектам РФ, в том числе более подробный анализ по Москве и Московской области. На основе проанализированной информации сделаны выводы о положительном и отрицательном влиянии введения саморегулирования на экономику России.

Саморегулируемые организации, саморегулирование, лицензирование.

HISTORY OF DEVELOPMENT AND OPERATION OF SELF-REGULATORY ORGANIZATIONS

Obukhova Ekaterina, 4th year student of the Department of economics
Scientific adviser: **Kurdyukova Natalia**, Candidate of Economic Sciences, Associate Professor of the Department of economics

This article is about the history of the development of self-regulation in the world, as well as the main goals, objectives and principles of operation self-regulatory organizations in the Russian Federation on an example of the construction sector. An analysis of the composition and distribution of the SRO in the construction of the subjects of the Russian Federation, including a more detailed analysis in Moscow and the Moscow region.

Self-regulatory organizations, self-regulation, licensing.

Первыми саморегулируемыми профессионалами, по сути, были врачи. Клятва Гиппократа — это реальный кодекс поведения и качества оказания услуг как предтеча современного саморегулируемого общества (далее СРО). Исторически саморегулирование восходит к западноевропейским цехам, объединявших под собой работников одной профессии, таким образом, очевидно, что свое регулирование участники рынка строили без участия государства, без участия власти, институтов потребителей. В средние века ремесленники близких профессий объединялись для создания определенных стандартов деятельности.

Наиболее ярким и показательным примером становления СРО стала система регулирования рекламы в Соединенных Штатах Америки. Низкое качество, отсутствие этики, недостоверность – все

это приводило к негодованию потребителей, в результате чего в 1912 году в Америке сформировались комитеты бдительности, действующие в сфере рекламы.

В российской действительности о СРО можно говорить с 1864 года, когда сформировались коллегии адвокатов, адвокатуры. Также прообразом современных саморегулируемых организаций можно назвать Московскую биржу, созданную в 1870 году. Защита интересов сообщества биржи перед государственными и общественными органами лежала на представительном органе – биржевом комитете. В 20 веке о саморегулировании вспомнили при оформлении принципов деятельности и контроля профессиональных участников рынка ценных бумаг. Также этот процесс коснулся оценщиков.

Затем последовал период перестройки, когда начали внедряться отдельные элементы делегирования полномочий по регулированию экономики от государственных органов к трудовым коллективам. В 1990-е годы начали создаваться и функционировать бизнес-сообщества в некоторых отраслях, перенявшие от государства часть контрольно-регулирующих функций. С 2010 года в связи с отменой государственного лицензирования строительства началась «новая эра» саморегулирования в России и организациям, деятельность которых связана с инженерными изысканиями, строительством и проектированием, нужно в обязательном порядке вступить в саморегулируемые организации и получить допуск СРО для осуществления указанных работ. Полномочия контроля над работой профильных компаний от государственных органов перешли к саморегулируемым организациям.

Во многих странах мира структуры саморегулирования и соответствующие частные организации сложились естественным образом в ходе исторического развития и на сегодняшний день успешно используются в качестве альтернативы государственному управлению, в России же этот процесс еще не завершен.

Сегодня в строительной отрасли в России ситуация такова: если ваша компания не входит в профильную СРО, то у вас нет разрешения на осуществление профессиональной деятельности, и тогда любые действия организации подлежат уголовному преследованию за незаконное предпринимательство. Все СРО не только устанавливают свои стандарты и обязательные правила профессиональной деятельности, но и контролируют их исполнение

всеми членами саморегулируемой организации. А главное, каждая СРО обеспечивает гражданскую ответственность всех своих членов (согласно ст. 55.16 гл. 6.1 Градостроительного Кодекса РФ) перед потребителями произведенных работ (услуг) и иными лицами.

Саморегулируемые организации — некоммерческие организации, объединяющие субъекты предпринимательской деятельности, работающие в определенной отрасли производства товаров (работ, услуг), либо объединяющие субъекты профессиональной деятельности определенного вида.

Основная идея СРО — переложить контрольные и надзорные функции за деятельностью субъектов в определённой сфере с государства на самих участников рынка. При этом с государства снимаются явно избыточные функции и, как следствие, снижаются бюджетные расходы, а фокус собственно государственного надзора смещается с надзора за деятельностью в сторону надзора за результатом деятельности, то есть иными словами вместо бесчисленного количества строительных компаний государство контролирует лишь официально зарегистрированные СРО.

Основная цель создания — дебюрократизация российской экономики и формирование новых гражданско-правовых институтов, направленных на укрепление практики ответственного ведения хозяйственной деятельности.

В настоящее время статус саморегулируемых организаций могут получить объединения предприятий, функционирующие по принципу некоммерческого партнерства. Если деятельность таких организаций отвечает всем требованиям, регламентированным в Градостроительном Кодексе и прочим нормативным актам.

К началу 2012 года в Российской Федерации федеральным законодательством было установлено обязательное членство в саморегулируемых организациях для участников профессиональной или предпринимательской деятельности в 10 сферах деятельности:

- деятельность арбитражных управляющих;
- аудиторская деятельность;
- кредитная кооперация;
- оценочная деятельность;
- деятельность ревизионных союзов сельскохозяйственных кооперативов;
- инженерные изыскания;
- архитектурно-строительное проектирование;

• строительство;

• деятельность в области энергетического обследования;

• теплоснабжение.

Основными целями СРО в России согласно Градостроительному кодексу РФ, глава 6.1, статья 55.1:

• предупреждение причинения вреда жизни или здоровью физических лиц, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений, объектам культурного наследия (памятникам истории и культуры) народов Российской Федерации (далее - вред) вследствие недостатков работ, которые оказывают влияние на безопасность объектов капитального строительства и выполняются членами саморегулируемых организаций;

• повышение качества выполнения инженерных изысканий, осуществления архитектурно-строительного проектирования, строительства, реконструкции, капитального ремонта объектов капитального строительства.

Присвоение статуса саморегулируемых организаций и их введение обеспечивает прозрачную деятельность и эффективную координацию различных государственных структур.

Общий обзор СРО в России говорит об улучшении картины дел в строительстве. По данным портала «Реестр СРО» на декабрь 2015 года в России насчитывалось 511 (для сравнения в декабре 2013 года – 454) саморегулируемых организаций (в строительстве, проектировании и инженерных изысканиях) Из них:

• СРО в строительстве – 277 организаций (13г. - 249);

• СРО в проектировании – 194 организации (13г. – 171);

• СРО в инженерных изысканиях – 40 организации (13г. – 34);

Саморегулируемые организации в соответствии с федеральным законодательством объединены по видам деятельности в такие национальные СРО, как:

• Национальное объединение строителей (НОСТРОЙ);

• Национальное объединение проектировщиков (НОП) и Национальное объединение изыскателей (НОИЗ) были объеденены в Национальное объединения проектировщиков и изыскателей (НОПРИЗ) 24 ноября 2014г.

В таблице 1 приведено территориальное распределение СРО и их структура по субъектам Российской Федерации.

Таблица 1 – Территориальная структура СРО в России

Федеральный округ	СРО							
	В строительстве		В проектировании		В изысканиях		ВСЕГО	
	кол-во	%	кол-во	%	кол-во	%	кол-во	%
Центральный	132	47,6	93	47,9	17	42,5	210	41,1
Северо-Западный	50	18,1	36	18,6	12	30,0	83	16,2
Приволжский	30	10,8	24	12,4	4	10,0	55	10,8
Южный+респ.Крым	11+1	4,3	10+1	5,7	3	7,5	25	4,9
Северо-Кавказский	8	2,9	3	1,5	0	0	8	1,6
Уральский	13	4,7	9	4,6	2	5,0	23	4,5
Сибирский	21	7,6	13	6,7	2	5,0	36	7,0
Дальневосточный	11	4,0	5	2,6	0	0	15	2,9
ИТОГО	277	100	194	100	40	100	511	100

Наибольшее число СРО образовано в Центральном федеральном округе (47,6% от всех организаций), за ним по убыванию следуют Северо-Западный (18,1%) и Приволжский (10,8%). Наименее развит институт СРО Северо-Кавказском (2,9%) и Дальневосточном федеральных округах (4,0%).

Структура СРО по видам деятельности (строительство, проектирование, изыскания) повторяет общую картину. Однако по данным на декабрь 2015 в Северо-Кавказском и Дальневосточном федеральных не было ни одного СРО в изысканиях. Компаниям из этих регионов для получения соответствующих допусков к работе рекомендуется обратиться в саморегулируемые организации других округов.

Характерное для СРО деление на региональные (объединения компаний в пределах одного региона или города) и межрегиональные (распределение компаний по всей России) имеет значительные преимущества. Получая заказы федерального уровня, компания-интегратор может привлекать из регионов субподрядчиков, входящих в одну СРО с едиными нормами квалификационного контроля и высоким уровнем взаимного доверия и надежности.

Если проводить обзор СРО по городам России, то здесь уверено лидирует Москва. На ее территории зафиксировано 159 саморегулируемых организаций или 34,6% от их общего числа. Далее с большим отрывом идет Санкт-Петербург – 67 СРО (или 14,8% от всех организаций), Екатеринбург – 11 СРО (2,4%). В остальных городах не более 10 саморегулируемых организаций. Если рассматривать московскую область, то картина выглядит следующим образом: Прудно (1), Долгопрудный (1), Домодедово (1), Одинцово

(1), Пушкино (2), Электросталь (1), Зеленоград (1), итого – 8 СРО что составляет 1,6%.

Многообразие различных СРО в каждом регионе обусловлено распределением спроса в единой сфере деятельности между игроками рынка. Несмотря на единую законодательную базу и обширную представленность в регионах все они очень отличаются друг от друга:

- по отраслевой направленности;
- по составу и территориальному охвату;
- по особенностям индивидуального подхода;
- по внутренним требованиям и нормативам.

На сегодняшний день по подсчетам аналитиков действительное число СРО в строительной области значительно превышает официальные данные. Создается множество коммерческих СРО, деятельность которых крайне негативно сказывается на репутации самого механизма саморегулируемых сообществ. Недальновидные клиенты, покупаясь на низкие требования и небольшие денежные взносы, вступают в ряды таких СРО. В результате сами же и страдают от этого, покрывая ущерб, нанесенный многими недобросовестными партнерами, которые беспрепятственно вступили в СРО без соблюдения необходимых требований.

Нередки случаи расформирования СРО после проверок, признания недействительными их свидетельств или, что еще хуже, внезапного исчезновения таких СРО с полным компенсационным фондом и членскими взносами. Ростехнадзор реализует программу по выявлению недобросовестных коммерческих СРО. Одним из инструментов против коммерциализации СРО предлагается введение рейтинговой системы.

Позитивными моментами введения системы СРО в строительство и другие сферы хозяйственной деятельности России являются:

1. Вступление в СРО позволяет избежать бюрократических проволочек и коррупции со стороны чиновников при получении лицензий.

2. Качество оказываемых российскими компаниями строительных и проектных услуг должно повыситься в связи с введением СРО в строительстве и СРО в проектировании. Это связано с тем, что к компаниям, желающим вступить в СРО, предъявляется ряд серьезных требований, соответствие которым должно гарантировать качество оказываемых ими услуг.

3. Вступление в СРО защищает фирмы от возникновения всевозможных форс-мажорных ситуаций, поскольку при форс-мажорах участникам СРО выплачиваются компенсации из страховых средств и дополнительного компенсационного фонда саморегулируемой организации. В 2010 году было осуществлено несколько таких страховых выплат. Это наглядно продемонстрировало пользу саморегулируемых организаций в данном аспекте.

4. Кроме того открытие СРО увеличивает количество рабочих мест в субъектах РФ что способствует увеличению занятости населения.

Но введение системы СРО в строительство в нашей стране имеет и ряд существенных недостатков, которые на данном этапе пытается устранить правительство:

1.На данном этапе развития бизнес в нашей стране не готов к работе в рамках саморегулируемых организаций. Вследствие печального опыта предприниматели в нашей стране стараются работать на краткосрочную, а не на долгосрочную перспективу. Поэтому для них ежегодная выплата крупных членских взносов просто для того, чтобы иметь возможность продолжить работу, оказалась непосильной.

2.Вступление в СРО, обязательное для всех, должно было очистить рынок от недобросовестных предприятий и фирм однодневок. Но на деле это привело к появлению коммерческих СРО в строительстве (и СРО в проектировании), предъявляющих заниженные требования к своим членам.

Анализ состояния строительной отрасли в России показывает, что динамика ее улучшений во многом обусловлена введением в 2010 году саморегулируемых организаций. Всю ответственность за получение лицензий на строительную деятельность государство фактически переложило на сами строительные организации. Чтобы стать членом СРО, всем строительным предприятиям необходимо сначала доказать свою компетентность. Несмотря на критические заявления некоторых аналитиков нововведения в целом качество строительных услуг значительно улучшилось. Причина тому – перераспределение ответственности: за любые недобросовестные работы каждого члена СРО отвечают все входящие в организацию участники. Это способствовало очищению строительной отрасли от

фирм-однодневок и организаций, некачественно выполняющих работы.

Но тут оказалось не все так просто как оказалось. Да, в какой-то степени саморегулирование оказалось неплохим инструментом управления и контроля во многих сферах, он его введение было не столь однозначным.

Без введения системы саморегулируемых организаций Россия не смогла бы вступить в ВТО. Саморегулируемые организации уже давно и успешно функционируют в Европе и Америке и зарекомендовали себя в качестве эффективной альтернативы государственному регулированию предпринимательской деятельности. Чтобы достичь таких же результатов, России потребуется время. Но, безусловно, введение системы СРО поспособствовало вступлению России в ВТО.

Литература

1. Градостроительный кодекс РФ. Статьи 55.1-55.20: Саморегулирование в области инженерных изысканий, архитектурно-строительного проектирования, строительства, реконструкции, капитального ремонта объектов капитального строительства.
2. Федеральный закон от 1 декабря 2007 г. № 315-ФЗ «О саморегулируемых организациях».
3. Постановление Правительства Российской Федерации от 29 сентября 2008 г. № 724 «Об утверждении порядка ведения государственного реестра саморегулируемых организаций».
4. Государственный реестр саморегулируемых организаций Российской Федерации «Федеральной службы по экологическому, техническому и атомному надзору» Режим доступа: http://sro.gosnadzor.ru/ (дата обращения 10.02.2016).

ОПРЕДЕЛЕНИЕ ОБЪЕМА И СТРУКТУРЫ ПОТРЕБНОСТИ ЛОКАЛЬНЫХ РЫНКОВ ТРУДА МОСКОВСКОЙ ОБЛАСТИ В ТРУДОВЫХ РЕСУРСАХ

Райляну Андриана Юрьевна, студентка 4 курса кафедры Экономики
Научный руководитель: **Лучкина Вероника Вячеславовна**, к.э.н., доцент кафедры Экономики

Внутрирегиональная маятниковая трудовая миграция призвана смягчать территориальные различия и более эффективно задействовать трудовые ресурсы. Для разработки эффективных мер необходимо обладать информацией о детерминантах внутренней миграции в городах и районах Московской области. Перераспределение трудовых ресурсов по территории Московской области является необходимым условием для обеспечения социально-экономического развития региона.

Трудовая миграция, трудовые ресурсы, внутренняя миграция.

DETERMINATION OF VOLUME AND STRUCTURE OF LABOUR MARKET NEEDS LOCAL MOSCOW REGION IN THE LABOR FORCE

Raileanu Andriana, 4th year student of the Department of economics
Scientific adviser: **Luchkina Veronica**, Candidate of Economic Sciences, Associate Professor of the Department of economics

Intraregional floating labor migration should mitigate the territorial differences and utilize efficiently the labor resources. The quality of research in the determinants of internal migration to cities and districts of the Moscow region affects the policies. The redistribution of labor resources in the region has influence on the socio-economic development.

Labor migration, labor force, internal migration.

По результатам мониторинга, общая потребность предприятий и организаций городов и районов Московской области в трудовых ресурсах в 2011 году составила 18,8 тысячи человек, в 2012 году спрос на рабочую силу снизился до 16,2 тысяч человек. Снижение общей потребности организаций в рабочей силе объясняется тем, что на большинстве предприятий не формируется даже среднесрочная

перспектива по развитию и восполнению кадрового потенциала. Замещение вакантных рабочих мест в 2011 году составило 89,2%, в 2012 году – 89,7% [1, 2].

Источники обеспечения необходимыми трудовыми ресурсами организаций и предприятий распределились следующим образом: местные трудовые ресурсы -56,7% (2012 год – 58,8%), в том числе выпускники образовательных учреждений начального и среднего профессионального образования – 9,13%, (2012 год – 9,1%), российские граждане из других субъектов РФ - 17,4% (2012 год - 11%), иностранная рабочая сила - 16,6% (2012 год - 13%).

Однако каждая четвертая вакансия замещается иностранными работниками. Полностью за счет иностранной рабочей силы заполняются вакантные рабочие места по профессиям, не требующим квалификации (уборщик производственных помещений, разнорабочий, дворник и т.д.). Объемы подготовки и переподготовки кадров за счет внутрифирменной подготовки составляют 4,4% в 2011 году, в 2012 году – 4,7%, что, в первую очередь, связано с отсутствием мастеров производственного обучения на предприятиях.

В табл. 1 представлена потребность предприятий и организаций Московской области в трудовых ресурсах в разрезе основных видов деятельности.

Таблица 1 - Потребность в трудовых ресурсах в разрезе отраслей производства и социальной сферы Московской области

	Наименование показателей	Численность, чел.		Удельный вес, %		Отклонение %
		2011 год	2012 год	2011 год	2012 год	
1	2	3	4	5	6	7
1	Потребность в рабочей силе,	18849	16154			
	в том числе					
	работающие (замещенные рабочие места)	10136	9419			
	дополнительная потребность (вакантные рабочие места)	8713	6735	100	100	
Лесное хозяйство						
2	Потребность в рабочей силе, всего	47	47			
	в том числе					
	работающие (замещенные рабочие места)	36	38			

Здравоохранение						
4	Потребность в рабочей силе,	952	848			
	в том числе					
	работающие (замещенные рабочие места)	360	286			
	дополнительная потребность (вакантные рабочие места)	592	562	6,8	8,3	-1,6
Торговля						
5	Потребность в рабочей силе,	805	591			
	в том числе					
	работающие (замещенные рабочие места)	35	43			
	дополнительная потребность (вакантные рабочие места)	770	548	8,8	8,1	0,7
Сельское хозяйство						
6	Потребность в рабочей силе,	2541	1596			
	в том числе					
	работающие (замещенные рабочие места)	1900	1301			
	дополнительная потребность (вакантные рабочие места)	641	295	7,4	4,4	3,0
Транспорт и связь						
7	Потребность в рабочей силе,	6767	6768			
	в том числе					
	работающие (замещенные рабочие места)	6196	6402			
	дополнительная потребность (вакантные рабочие места)	571	366	6,6	5,4	1,1
Наука						
8	Потребность в рабочей силе,	677	555			
	в том числе					
	работающие (замещенные рабочие места)	100	66			
	дополнительная потребность (вакантные рабочие места)	577	489	6,6	7,3	-0,6
Строительство						
9	Потребность в рабочей силе,	2101	1721			
	в том числе					
	работающие (замещенные рабочие места)	470	412			
	дополнительная потребность (вакантные рабочие места)	1631	1309	18,7	19,4	-0,7
Жилищно-коммунальное хозяйство						
10	Потребность в рабочей силе,	10429	10429			

	в том числе					
	работающие (замещенные рабочие места)	9066	9239			
	дополнительная потребность (вакантные рабочие места)	1363	1190	15,6	17,7	-2,0
Промышленность						
11	Потребность в рабочей силе,	10440	8140			
	в том числе					
	работающие (замещенные рабочие места)	5832	4968			
	дополнительная потребность (вакантные рабочие места)	4608	3172	52,9	47,1	5,8
Финансы и управление						
12	Потребность в рабочей силе,	69	66			
	в том числе					
	работающие (замещенные рабочие места)	25	31			
	дополнительная потребность (вакантные рабочие места)	44	35	0,5	0,5	0,0
Образование и культура						
13	Потребность в рабочей силе,	2249	2136			
	в том числе					
	работающие (замещенные рабочие места)	1784	1697			
	дополнительная потребность (вакантные рабочие места)	465	439	5,3	6,5	-1,2

Исходя из анализа представленных данных, можно сделать следующие выводы:

1) рост потребности организаций Московской области в рабочей силе наблюдается в таких сферах экономической деятельности как: промышленность, транспорт и связь, торговля, сельское хозяйство;

2) снижение потребности отмечено в таких видах, как здравоохранение, наука, строительство, жилищно-коммунальное хозяйство, образование и культура.

Промышленность. По данным мониторинга - промышленность составляет более 20% от отраслевой численности работающих. В 2011 году представленная организациями потребность в кадрах составила 10429 человек, при этом текущий спрос удовлетворен на 89,2%. В 2012 году произошло увеличение потребности в рабочей силе на 3,1%.

Источники обеспечения промышленных предприятий в 2011 году распределились следующим образом (рис. 1.):

Рисунок 1 - Источники обеспечения потребности организаций промышленной отрасли высококвалифицированными кадрами, чел.

-привлечение рабочей силы: за счет местных трудовых ресурсов – 60,3%, из других регионов России – 16,4%, за счет иностранных граждан – 10,7%. В 2012 году произошло сокращение объемов привлечения рабочей силы за счет российских граждан из других регионов нашей страны и составило 7,5% и местных трудовых ресурсов и составило 62,3%. Параллельно с этим, происходило увеличение объемов привлечения рабочей силы за счет иностранных граждан на 2,4%;

-приток выпускников начальных и средних профессиональных заведений на производство в 2011 году составляет 6,6%, в 2012 году этот показатель вырос на 9,7%.

Жилищно-коммунальное хозяйство. Предприятия жилищно-коммунального аккумулируют около 28% от отраслевой численности работающих. По состоянию на 2011 год представленная организациями потребность в кадрах составила 10429 человек, при этом текущий спрос был удовлетворен на 88,5%. В 2012 году дополнительной потребности в рабочей силе не возникло.

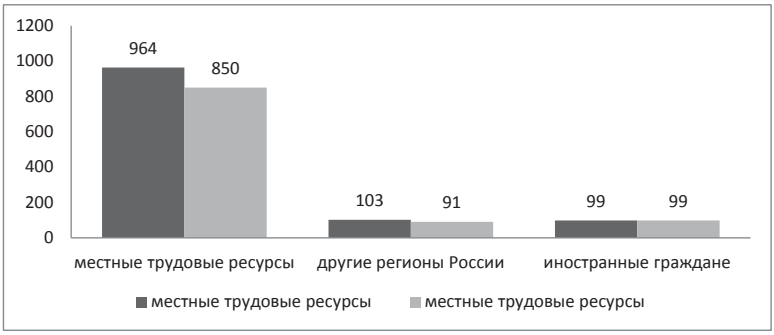


Рисунок 2 - Источники обеспечения потребности организаций ЖКХ высококвалифицированными кадрам

Источники обеспечения предприятий жилищно-коммунального хозяйства трудовыми ресурсами распределились следующим образом (рис. 2):

-за счет местных трудовых ресурсов – 70,7%, из других регионов России – 7,6%, за счет иностранных граждан – 7,3%.

В 2012 году произошло сокращение объемов привлечения рабочей силы за счет местных трудовых ресурсов на 11,8%, из других регионов России на 11,7%. Параллельно с этим, не изменился объем привлечения рабочей силы за счет иностранных граждан.

Приток выпускников начальных и средних профессиональных заведений на производство в 2011 году составляет 0,4%, как и в 2012 году.

Транспорт и связь. Транспортные предприятия и предприятия связи аккумулируют 18,3% от совокупной отраслевой численности работающих региона. В 2011 году представленная предприятиями потребность в кадрах составила 6767 человек, при этом текущий спрос был удовлетворен на 99%. Однако в 2012 году рост потребности в рабочей силе снизился на 5%.

Источники обеспечения предприятий, занимающихся деятельностью, связанной с транспортом и связью, распределились следующим образом (рис. 3):

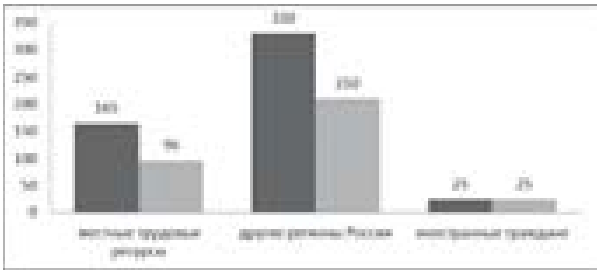


Рисунок 3 - Источники обеспечения потребности организаций транспорта и связи высококвалифицированными кадрами

-привлечение рабочей силы: за счет местных трудовых ресурсов – 28,9%, из других регионов России – 57,8%, за счет иностранных граждан – 4,4%. В 2012 году произошло сокращение объемов привлечения рабочей силы за счет местных трудовых ресурсов на 41,8%, из других регионов России на 36,4%. Одновременно с этим процессом объем привлечения рабочей силы иностранных граждан не изменилось. Приток выпускников начальных и средних профессиональных заведений в организации в 2011 году составляет

5,4%, 2012 год этот показатель немного возрос.

Таким образом, наибольшую потребность в трудовых ресурсах испытывают отрасли промышленного производства – 28,2% от совокупного уровня потребности в трудовых ресурсах предприятий и организаций Московской области, 28,1% от совокупного уровня потребности приходится на предприятия и организации ЖКХ. Более 15% - на транспорт и связь, далее в рейтинге следуют по отраслям сельского хозяйства уровень потребности в трудовых ресурсах составляет около 7% от совокупного уровня потребности в кадрах, образование и культура – 6,1%, строительство – 5,7%, здравоохранение - около 2,6% (рис. 4).

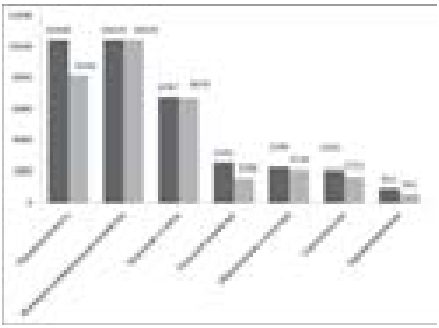


Рисунок 4 - Потребность в трудовых ресурсах на предприятиях и организациях Московской области в разрезе видов экономической деятельности в 2011-2012 гг.

Наибольшая доля потребности в трудовых ресурсах восполняется за счет местного экономически активного населения региона в следующих отраслях:

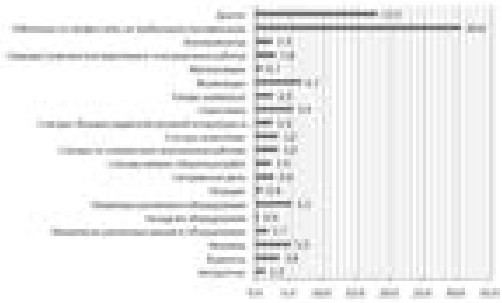


Рисунок 5 - Потребность организаций Московской области в рабочей силе по профессиям (специальностям) в 2012 году

- жилищно-коммунальное хозяйство - более 90%;
- наука и научное обслуживание - 89,3%;
- транспорт и связь - 87%;
- сельское хозяйство - около 80%;
- промышленность - более 50%.

Наиболее остро на предприятиях и организациях Московской области ощущается потребность в высококвалифицированных кадрах рабочих профессий (рис. 5).

Далее рассмотрим потребность в трудовых ресурсах в разрезе городов и районов Московской области по следующим параметрам:

- по уровню потребности в трудовых ресурсах;
- по уровню возмещения потребности в трудовых ресурсах за счет внутрирегиональной трудовой миграции.

Ранжирование по уровню потребности в трудовых ресурсах позволило выделить основные 4 группы территориальных образований (табл. 2):

- с высоким уровнем потребности в трудовых ресурсах (от 3% до 11% от общей численности экономически активного населения);
- со средним уровнем потребности в трудовых ресурсах (более 2% от общей численности экономически активного населения);
- с низким уровнем потребности (от 1% до 2%);
- уровнем потребности менее 1% от общей численности экономически активного населения), т.е. практически полностью возмещающим потребность в трудовых ресурсах за счет собственного населения).

По уровню возмещения потребности в трудовых ресурсах за счет маятниковых внутренних трудовых мигрантов группировка территорий Московской области выглядит следующим образом:

- 1 группа - с высоким уровнем возмещения потребности в трудовых ресурсах за счет внутрирегиональных трудовых мигрантов. Города и районы, привлекающие от 15% до 35% экономически активного населения из других районов и городов Московской области для покрытия потребности отраслей экономики в трудовых ресурсах;
- 2 группа - города и районы, привлекающие от 8% до 13% экономически активного населения из других районов и городов Московской области;
- 3 группа - города и районы, привлекающие от 5% до 8%

экономически активного населения из других районов и городов Московской области;

• 4 группа - с низким уровнем возмещения потребности в трудовых ресурсах за счет внутрирегиональных трудовых мигрантов,

Таблица 2 - Ранжирование городов и районов Московской области по уровню потребности, %

№	ГОРОДА И РАЙОНЫ МОСКОВСКОЙ ОБЛАСТИ	Ранг	
1	Одинцовский район	1	От 3% до 11%
2	Дмитровский район	2	
3	г. Электросталь	3	
4	г. Королёв	4	
5	Истринский район	5	
6	Клинский район	6	
7	Рузский район	7	
8	Наро-фоминский район	8	
9	г. Ивантеевка	9	
10	Люберецкий район	10	
11	Домодедовский район	11	
12	Ленинский район	12	Более 2%
13	Солнечногорский район	13	
14	Озерский район	14	
15	г. Реутов	15	
16	г. Лобня	16	
17	Балашихинский район	17	
18	Серпуховской район	18	
19	г. Жуковский	19	
20	г. Орехово-Зуево	20	Более 1%
21	г. Пущино	21	
22	г. Красноармейск	22	
23	Мытищинский район	23	
24	Ногинский район	24	
25	г. Дзержинский	25	
26	Коломенский район	26	
27	Лотошинский район	27	Менее 1%
28	г. Щербинка	28	
29	Волоколамский район	29	
30	г. Климовск	30	
31	Щелковский район	31	
32	г. Дубна	32	
33	Павлово-Посадский район	33	
34	Воскресенский район	34	
35	Каширский район	35	
36	Подольский район	36	
37	Чеховский район	37	
38	Серебряно-Прудский район	38	

• привлекающие от 1% до 3% экономически активного населения из других районов и городов Московской области для покрытия потребности отраслей экономики в трудовых ресурсах.

Таким образом, перераспределение трудовых ресурсов по территории Московской области является необходимым условием для обеспечения социально-экономического развития региона. Внутрирегиональная маятниковая трудовая миграция населения, призванная смягчать существующие территориальные различия и более эффективно задействовать дефицитные трудовые ресурсы региона. В свою очередь, для разработки эффективных мер внутрирегиональной миграционной стратегии необходимо обладать информацией о детерминантах внутренней миграции в городах и районах Московской области.

Литература

1. Официальный сайт Комитета по труду и занятости населения Московской области [Электронный ресурс] - http://old.ktzn.mosreg.ru/kadr_potencial/ (даты обращения: 01.12.15 - 15.02.16)
2. Филимоненко, И.В. Управление локальными рынками региона как факторами экономического роста [Текст] / Е.В. Белякова, О.В. Иванов / ООО «Проспект», электронная версия книги», 2015. - С. 146-149

КОРРУПЦИЯ КАК ФАКТОР, СДЕРЖИВАЮЩИЙ РАЗВИТИЕ РОССИИ

Савельев Андрей Валерьевич, Иванова Ангелина Станиславовна, студенты 2 курса кафедры Экономики
Научный руководитель: **Рыжкова Татьяна Васильевна**, к.э.н., доцент кафедры Экономики

В статье исследуется одна из самых актуальных проблем современной России - коррупция. Рассмотрены виды, причины коррупции, определены ее последствия. Представлены методы борьбы с коррупцией и предпринята попытка оценки ее масштабов. Проанализированы подходы и дана оценка методам борьбы с коррупцией. Предложены меры борьбы с коррупцией.

Виды, причины, последствия, масштабы коррупции, методы и результаты борьбы с коррупцией.

CORRUPTION AS A FACTOR CONSTRAINING THE DEVELOPMENT OF RUSSIA

Savelyev Andrey, Ivanova Angelina, 2nd year students of the Department of economics
Scientific adviser: **Ryzhkova Tatyana,** Candidate of Economic Sciences, Assistant Professor of the Department of economics

This article examines one of the most actual problems of modern Russia - corruption. Considered the types and reasons of corruption, defined its consequences. Presents methods the fight against corruption and attempt to assess its scope. Analyzed approaches and assessed the methods of struggle against corruption. The proposed measures to combat corruption.

Types, causes, consequences, the scale of corruption, methods and results of the fight against corruption.

Коррупция является серьезной и трудно преодолимой проблемой современной России. Она имеет массовый характер и затрагивает все сферы жизни общества. Коррупция разрушает государственное устройство, препятствует развитию страны, негативно отражается на жизни каждого гражданина и экономике в целом. Несмотря на то, что эта проблема постоянно обсуждается на всех уровнях власти, определяются и реализуются различные направления и методы борьбы с коррупцией, существенно снизить ее уровень не удается.

Что же такое «коррупция»? Коррупция является сложным социальным явлением, поэтому его сложно определить, отразив в одном предложении все аспекты сущности. В источниках термин «коррупция» описывается по-разному. В одних говорится, что коррупция – это злоупотребление служебным полномочием, в других указываются ее конкретные виды и формы проявления. Если сложить воедино мысли авторов, то *коррупцию* можно определить как использование должностным лицом своего служебного положения в целях личного обогащения, как правило, сопровождающееся нарушением законности, которая имеет форму взяток, злоупотребления по службе, превышения должностных полномочий и других противозаконных действий.

Коррупция, как многоплановое явление, имеет множество проявлений. Она поражает все уровни государственных органов и

сферы общественной деятельности, различается по территории своего распространения, отличается характером воздействия на регулируемые отношения (рисунок 1).

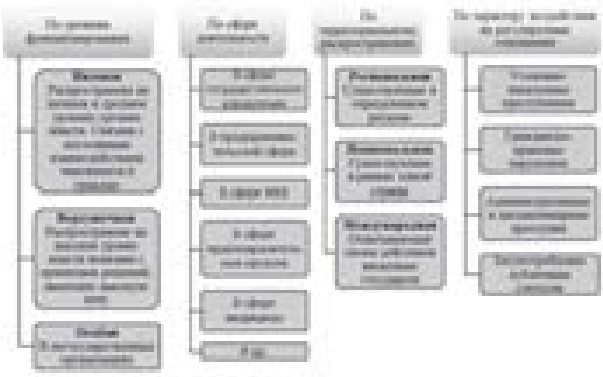


Рисунок 1 – Классификация видов коррупции [14]

По уровням формирования различают низовую, верхушечную и особую коррупцию. Низовая коррупция распространена на низшем и среднем уровнях органах власти и связана с постоянным взаимодействием чиновников и граждан. Верхушечная - имеет распространение на высшем уровне власти и связана с принятием решений, имеющими высокую цену. Особая коррупция проявляется в негосударственных организациях.

Коррупция способна проникнуть во все сферы жизни общества. Она существует в сфере государственного управления, в предпринимательской сфере, в сфере правоохранительных органов и других.

По размеру и масштабам распространения различают региональную, национальную и международную коррупцию.

Группировка коррупционных событий по характеру воздействия на регулируемые отношения содержит уголовно-наказуемые преступления, гражданско-правовые нарушения, административные и дисциплинарные проступки и злоупотребления, имеющие публичный статус. Получение, дача взятки и некоторые другие правонарушения, связанные с незаконным получением благ и преимуществ, являются уголовно-наказуемыми. Административные и дисциплинарные проступки, создающие условия для коррупции, относятся гражданско-правовым нарушениям. Злоупотребления публичным

статусом – это действия, которые не влекут за собой никакой ответственности.

Коррупция существует в форме взяточничества, растраты, вымогательства, незаконных операций с ценными бумагами, кумовства, фаворитизма, мошенничества, злоупотребления служебным положением [3].

Распространению коррупции способствует ряд условий, основное из которых – несовершенство законодательства. Другими коррупции являются чрезмерное государственное вмешательство в экономику, низкий уровень развития гражданского общества, отсутствие контроля над распределением государственных ресурсов, неадекватные меры наказания за коррупционные сделки, относительно низкая оплата труда служащих и многие другие [7].

Последствия коррупции можно разделить на три типа (таблица 1):

Таблица 1 – Последствия коррупции [9]

Экономические	Социальные	Политические
Расширение сектора теневой экономики;	Несправедливое перераспределение средств в пользу узких олигархических групп;	Снижение доверия к власти у населения;
Нарушение механизма функционирования рыночной конкуренции;	Отвлечение колоссальных средств от целей общественного развития;	Падение престижа страны на международной арене;
Неэффективное использование бюджетных средств;	Инструментом регулирования экономики и жизни общества служат не законы, а деньги.	Угроза политической и экономической изоляции страны.

Коррупция наносит непоправимый ущерб экономике. Под ее воздействием расширяется сектор теневой экономики, нарушается механизм функционирования рыночной конкуренции, использование бюджетных средств становится неэффективным. Социальные последствия коррупции заключаются в несправедливом перераспределении средств в пользу узких олигархических групп, колоссальные средства отвлекаются от целей общественного развития. Таким образом, инструментом регулирования экономики и жизни общества служат не законы, а деньги. Коррупция имеет не только экономические и социальные последствия, но и политические результаты - снижение доверия к власти у населения и падение престижа страны на международной арене, что может привести к ее экономической и политической изоляции.

Несмотря на массовый характер и широкие масштабы коррупция в России, она сложно поддается количественной оценке и практически не измерима. Так как коррупция обычно не влечет за собой никаких негативных последствий для непосредственных участников данного процесса, факты коррупции не разглашаются, определить ее размер методами прямого счета невозможно. Немногие готовы признаться в том, что давали или получали взятку. Оценить уровень коррупции можно лишь косвенными методами (рисунок 2).

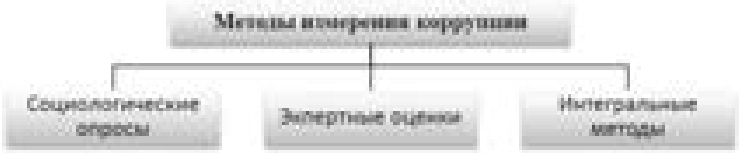


Рисунок 2 – Классификация методов оценки коррупции [13]

К первой группе таких методов оценки относятся социологические опросы. Они связаны с изучением общественного мнения по вопросу восприятия коррупции и опыту столкновений с ее проявлениями. Социологические опросы проводятся с помощью личных, телефонных или сетевых интервью с гражданами различных профессий и возрастов.

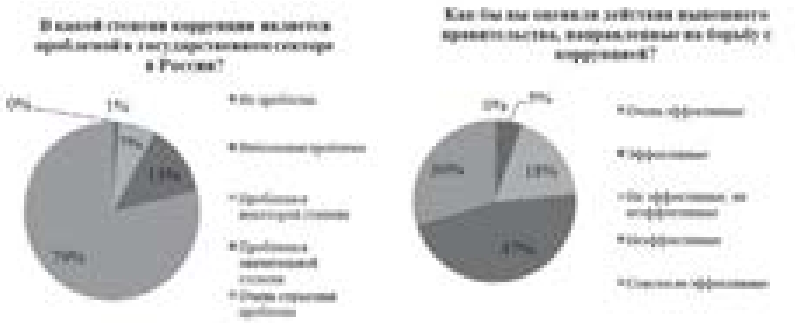


Рисунок 3 – Результаты опроса россиян в рамках исследования «Барометр мировой коррупции»

Одним из таких опросов является «Барометр мировой коррупции», проводимый международной неправительственной организацией Transparency International, который проводит исследование в 107 странах мира и изучает мнение более 110 000 участников. Респондентам задаются вопросы, связанные с проявлениями коррупции в их стране. Как показывают результаты

опроса, практически все россияне считают коррупцию весьма серьезной проблемой. Большинство россиян высказали мнение, что правительство проводит неэффективно антикоррупционную политику (рисунок 3).

Двум третям опрошенных россиян предлагали взятку. На вопрос «Отказались ли они от дачи взятки?» утвердительно ответило 87% процентов участников. Скорее всего, многие скрывают эти факты (рисунок 4).

Рисунок 4 – Результаты оценки уровня взяточничества [12]

Другим видом социологического опроса, проводимого Всемирным банком и посвященного изучению коррупции, является «Индекс качества государственного управления». Показателем уровня коррумпированности экономики является индекс сдерживания коррупции государственными органами. Эксперты Всемирного банка присваивают каждой стране индекс от 0 до 100. Чем ближе индекс к максимальному значению, тем выше качество государственного управления и противодействие коррупции.

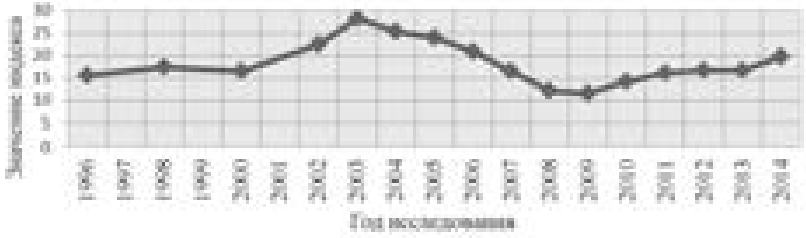


Рисунок 5 - Качество государственного управления в области коррупции в России [11]

На протяжении многих лет сдерживание коррупции государством в России находится на очень низком уровне, не превышая 30 (рисунок 5). Рост рейтинга в 2003 г. обусловлен сменой

президента и правительства и началом новой власти борьбы с коррупцией, которой не занимались в 90-ых гг. Однако эффективность предпринятых мер - очень низка. Увеличение рейтинга в 2008 году связано с принятием Федерального закона «О противодействии коррупции» и принятие национального антикоррупционного плана.

Социологические опросы, связанные с изучением распространения коррупции, проводятся ВЦИОМ. Респондентам было предложено выбрать сферы общественной жизни, наиболее подверженные коррупции. На основании их ответов составлен рейтинг коррумпированности (рисунок 6).

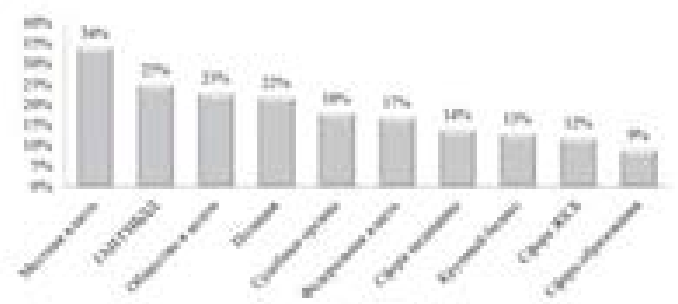


Рисунок 6 - Сферы жизни России, наиболее подверженные коррупции (данные опроса ВЦИОМ, 2015 год) [8]

Вторую группу методов оценки коррупции образуют экспертные оценки. Их основу составляют опросы ученых, экспертов в области политики и экономики, а также представителей бизнеса разных стран мира. Эти методы оценок позволяют получить более точные результаты, по сравнению с методами опроса населения.

Экспертные оценки под названием «Индекс взяткодателей» проводит компания Transparency International. Исследование посвящено коррупционным практикам компаний стран-экспортеров. В ходе исследования опрашиваются представители бизнеса, каждому из которых задаются вопросы об опыте работы со странами-экспортерами и их компаниями, определяя, насколько часто они прибегают к подкупу (0 - всегда, 10 - никогда). По данным этого исследования российские компании являются самыми коррумпированными и наименее привлекательными для сотрудничества (таблица 2).

Таблица 2 – Индекс взяткодателей [12]

Ранг	Страна / Территория	Балл Индекса взяткодателей
1	Нидерланды	8,8
1	Швейцария	8,8
3	Бельгия	8,7
4	Германия	8,6
4	Япония	8,6
…	…	…
26	Мексика	7,0
27	Китай	6,5
28	***Россия***	***6,1***

Другим видом экспертной оценки является рейтинг «Нации в транзите» компании Freedom House. Исследование предназначено для оценки развития демократии в 29 бывших странах восточной Европы и СССР. Оценки выставляется учеными и другими компетентными экспертами представителями местного сообщества. Чем ближе оценка к 1, тем выше уровень демократии и ниже уровень коррупции в стране. Максимальная оценка, равная 7, означает авторитарность режима и высокую коррупцию. Коррумпированность России, по мнению экспертов, имеет максимальное значение и продолжает расти (рисунок 7).

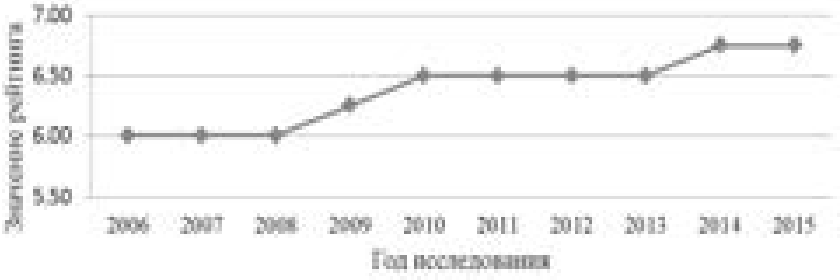


Рисунок 7 - Отчет неправительственной организации Freedom House о состоянии коррупции в России [11]

Еще одним методом оценки коррупции являются интегральные оценки, получаемые агрегированием рейтингов коррупционности различных организаций. Самая известная из интегральных оценок – «Индекс восприятия коррупции» от Transparency International.

Индекс восприятия коррупции – ежегодный составной индекс, измеряющий уровень восприятия коррупции в государственном секторе различных стран. Эксперты компании Transparency International агрегируют и оценивают различные коррупционные

исследования. На основе собранной информации страны ранжируются по шкале от 0 до 100 баллов. 0 означает самый высокий уровень восприятия коррупции, 100 – наименьший.

Восприятие коррупции в России находится на высоком уровне, принимая значения от 20 до 30 баллов из 100 возможных, постоянно занимая место во второй сотне списка (рисунок 8). Стоит отметить, что в прошлом году уровень восприятия коррупции стал наиболее низким относительно всех рейтингов предыдущих лет. По мнению вице-президента Transparency International Елены Панфиловой, это вызвано объективной реальностью сокращения коррупционной «кормовой базы» в силу текущей экономической ситуации, а также введения в правовое поле целого ряда обременительных для публичных должностных лиц ограничений, в части декларирования имущества, доходов, владения зарубежной собственностью.

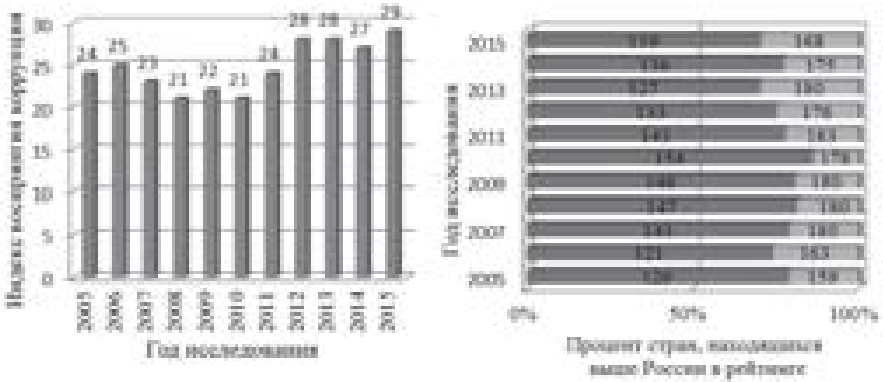


Рисунок 8 – Индекс восприятия коррупции в России [12]

Таким образом, результаты всех рассмотренных оценок позволяют сделать вывод о высоком уровне коррупции в стране. Ввиду специфики коррупционных преступлений, которая заключается в их скрытности, их сложно определить количественно. Однако СМИ и участники антикоррупционных организаций периодически представляют информацию о состоянии российской коррупции (таблица 3).

Так, по оценке Национального Антикоррупционного Комитета, объем рынка коррупции составляет более 300 млрд. долларов, что соответствует 20-30% ВВП. Средний размер взяток увеличился в 3 раза по сравнению с прошлым годом и составил 613 тыс. руб. (данные на сентябрь 2015 года).

Таблица 3 – Масштабы коррупции в России

Более 300 млрд. долларов	Объем рынка коррупции, по оценке Национального Антикоррупционного Комитета.
20-30%	ВВП страны составляет рынок коррупции.
613 тысяч рублей	Средний размер взятки в России на сентябрь 2015 года.
29 млн. взяток	Примерное количество взяток в России за год.
65%	Коррупционный охват в России по данным Transparency International.

На основе поступающих во Всероссийскую антикоррупционную общественную приемную «Чистые руки» жалоб, самой коррумпированной сферой являются судебные органы. Среднюю величину взятки по уголовным делам эксперты оценивают в 3 млн. руб., по гражданским — в 650 тыс. руб. Наибольшее количество жалоб, связанных с коррупцией, поступает из Москвы (27,5%), Московской области (15,6%) и Краснодарского края (5,62%).

Следует отметить, что в России разрабатываются и реализуются меры противодействия коррупции, которые в соответствии с их содержанием можно разделить на 3 группы:

- направленные на предупреждение коррупции, в том числе на выявление и последующее устранение причин коррупции;
- направленные на выявление, предупреждение, пресечение, раскрытие и расследование коррупционных правонарушений;
- направленные на минимизацию и (или) ликвидацию последствий коррупционных правонарушений [4].

Противодействие коррупции регулируется нормативно-правовыми актами и международными договорами, ратифицированными Россией. В целях уголовно-правового обеспечения противодействия коррупции УК РФ устанавливает ответственность за совершение коррупционных преступлений - за получение взятки (ст.290), дачу взятки (ст.291), коммерческий подкуп (ст.204), злоупотребление должностными полномочиями (ст.285) и другие преступления [5]. КоАП РФ определяет ответственность за противоправные действия, связанные с коррупцией, в частности за нецелевое использование бюджетных средств и средств государственных внебюджетных фондов (ст.15.14), за использование незаконной материальной поддержки при финансировании избирательной кампании, кампании референдума (ст.5.19) [2]. Ответственность лиц за гражданские правонарушения, которые обладают признаками коррупции, но не являются преступлениями, введены ГК РФ. Статья 575 ГК РФ содержит запрет на дарение, за

исключением обычных подарков, государственным служащим в связи с их должностным положением или в связи с исполнением ими служебных обязанностей, стоимость которых не превышает 3 тыс. руб. [1].

Основным законом, который определяет принципы и систему мер противодействия коррупции, является Федеральный закон "О противодействии коррупции" (№ 273-ФЗ от 25.12. 2008 г.), устанавливающий обязанности, ограничения и запреты, связанные с прохождением государственной и муниципальной службы [4].

Каждые 2 года президент утверждает Национальный план противодействия коррупции, направленный на развитие нормативно-правовой базы федеральных государственных органов, субъектов Российской Федерации и муниципальных образований по противодействию коррупции; организацию работы кадровых служб федеральных органов исполнительной власти по профилактике коррупционных и иных правонарушений; проведение социологических исследований уровня коррупции и эффективности, антикоррупционных мер; обучение федеральных государственных служащих, в должностные обязанности которых входит участие в противодействии коррупции [6].

В 2006г. Россия подписала и ратифицировала Конвенцию ООН «Против коррупции», целью принятия которой является поощрение, облегчение и поддержка международного сотрудничества и оказание технической помощи в предупреждении коррупции и борьбе с ней [3].

Россия обладает широким спектром средств по противодействию коррупции, однако, само по себе существование и многообразие средств еще не обеспечивает реальных результатов. Масштабы коррупции не уменьшаются, а ее уровень продолжает расти. Строгость закона компенсируется его неисполнением. У органов государственной власти не сформирована потребность и ответственность искоренения коррупции, и борьба с ней носит характер имитации. Функция борьбы с коррупцией возложена на правоохранительные органы, которые сами поражены ей. Очевидно, что необходимы более совершенные и радикальные методы и меры противодействия коррупции, требуется создание специальных структур, которые смогли бы осуществлять борьбу эффективно.

Предупреждение и противодействие коррупции должно быть системным. Для снижения уровня коррупции считаем целесообразным принять меры, направленные:

-на повышение ответственности государственных служащих за преступления, связанные с коррупцией;

-на усиление контроля доходов и расходов государственных служащих и членов их семей, конфискация имущества, полученного незаконным путем;

-на обеспечение полной независимости СМИ и судебной системы;

-на обеспечение избирательности чиновников всех уровней власти;

-на формирование у населения антикоррупционного мышления;

-на внедрение ЕГАИС и подобных ей систем по учету продаж в различных отраслях экономики;

-на введение системы поощрений для людей, которые сообщают о коррупционных правонарушениях.

Уровень коррупции в стране крайне высок. Россия является одним из мировых лидеров по этому показателю. Проблема является комплексной и оказывает негативное влияние на все сферы жизни общества. Как сложное социально-экономическое явление коррупция трудно поддается оценке, ее масштабы и динамика оцениваются лишь на основе косвенных признаков. Реализуемые государством меры борьбы с этой проблемой носят формальный характер и неэффективны. Борьба с коррупцией должна иметь системный характер с использованием самых разных методов ее предупреждения и устранения. Объединение усилий государства и общества, а также соблюдение всех необходимых принципов способны снизить уровень коррупции в нашей стране.

Литература

1. Гражданский кодекс Российской Федерации (часть вторая) от 26.01,1996 №14-ФЗ (ред. От 29.06.2015) //Российская газета. - 06.02.1996. № 23, 07.02.1996. № 24, 08.02.1996. №25, 10.02.1996. № 27.

2. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ (ред. от 30.03.2016) // Российская газета. - 31.12.2001. № 256.

3. Конвенция Организации Объединенных Наций против коррупции (подписана Российской Федерацией 9 декабря 2003г.,

ратифицирована Федеральным законом от 8 марта 2006 г. №40-ФЗ) // Российская газета. 2006.
4. О противодействии коррупции: Федеральный закон от 25.12.2008 № 273- (ред. от 15.02.2016)// Российская газета. 2008. №266.
5. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 30.03.2016)// Собрание законодательства РФ. 1996. № 25.
6. Указ Президента РФ от 11.04.2014 N 226 (ред. от 15.07.2015) "О Национальном плане противодействия коррупции на 2014 - 2015 годы"// Российская газета. 5 августа 2008 г. № 4721.
7. Братановский, С. Н. Противодействие коррупции в системе исполнительной власти в Российской Федерации: административно-правовые аспекты: монография [Текст] / С. Н. Братановский, М. Ф. Зеленов. - М.: Директ-Медиа, 2014. - 433 с.
8. Борьба с коррупцией: миссия выполнима? [Электронный ресурс]: исследование ВЦИОМ - Режим доступа: http://infographics.wciom.ru/theme-archive/politics/internal-policy/corruption/article/borba-s-korrupciei-missija-vypolnima.html (дата обращения: 19.12.2015)
9. Доклад «Россия и коррупция: кто кого» [Электронный ресурс] // Проекты фонда ИНДЕМ, 1998. – Режим доступа: http://indem.ru/russian.asp
10. Исследование Всемирного банка «Качество государственного управления» [Электронный ресурс]: - Режим доступа: http://info.worldbank.org/governance/wgi/index.aspx#home (дата обращения: 29.11.2015)
11. Исследование Freedom House «Нации в транзите» [Электронный ресурс]: - Режим доступа: https://freedomhouse.org/(дата обращения: 14.12.2015)
12. Исследования Transparency International [Электронный ресурс] - Режим доступа: http://transparency.org.ru/(дата обращения: 10.12.2015)
13. Редакция журнала «Отечественные записки». Методики измерения коррупции [Электронный ресурс] // Отечественные записки, 2012. Режим доступа: http://www.strana-oz.ru/2012/2/metodiki-izmereniya-korrupcii (дата обращения: 18.11.2015)
14. Толкачев, В.В. Понятие и виды коррупции [Электронный ресурс]: - Режим доступа: http://www.sartraccc.ru/i.php?oper (дата обращения: 21.12.2015)

БИЗНЕС-ИНКУБАТОР В УНИВЕРСИТЕТАХ - БАЗА НАУЧНЫХ ИССЛЕДОВАНИЙ И РАЗРАБОТОК ДЛЯ БИЗНЕСА

Санина Анастасия Евгеньевна, студентка 4 курса кафедры Управления
Научный руководитель: **Бронникова Тамара Семеновна,** к.э.н., доцент кафедры Экономики

Система бизнес-инкубаторов является частью структурной, социально-экономической и инновационной политики, которая поддерживает и способствует развитию малого предпринимательства, в том числе носящего инновационный характер. Малый и средний инновационный бизнес играют одну из ключевых ролей в экономике. Это подталкивает правительства стран к реализации мер государственной политики по развитию системы бизнес-инкубирования.

В статье проанализированы результаты функционирования бизнес-инкубаторов в вузах России и предложено развивать это направление для связи научного взаимодействия университета и бизнеса.

Бизнес-инкубатор, инновации, университет.

BUSINESS INCUBATOR IN UNIVERSITIES - BASE OF SCIENTIFIC RESEARCH AND DEVELOPMENT FOR BUSINESS

Sanina Anastasia, 4rd year student of the Department of management
Scientific adviser: **Bronnikova Tamara**, Candidate of Economic Sciences, Associate Professor of the Department of economy

The system of business incubators is a part of the structural, social, economic and innovation policy that supports and promotes to development of small business, including business of the innovative character. The realization that the small and medium business innovation play a key role in the economy. This encourages governments to implement public policies for the development of business incubation.

The article analyzes the results of functioning of business incubators in the universities of Russia and proposed to develop this area to communicate scientific interaction between University and business.

The business-incubator, innovation, University, startups.

Современная ситуация в мире показывает, что Россия не сможет достичь значимых результатов в ближайшие годы и в отдаленной перспективе без высоких технологий, поэтому у нашей страны нет другого выбора, как развиваться в инновационном направлении.

Распоряжением от 6 марта 2015 года премьер-министром РФ было подписано распоряжение о реализации в 2015-2016 годах «Стратегии инновационного развития России на период до 2020 года». Так, в рамках первого этапа реализации Стратегии (2011-2013 годы) проводилась реструктуризация сектора высшего образования.

Для решения задач второго этапа Стратегии (2014-2020 годы) утвержден план ее реализации в 2015–2016 годах. Он предусматривает меры представленные в таблице.

Таблица 1 – План реализации второго этапа Стратегии инновационного развития России на период 2015− 2016 гг.

№	Направления плана по реализации 2 этапа Стратегии
1	Совершенствование системы образования;
2	Популяризация научной, научно-технической и инновационной деятельности;
3	Формирование системы поддержки научного и технического творчества детей и молодежи государством;
4	Обеспечение эффективной реализации программ инновационного развития компаний с государственным участием;
5	Формирование механизмов стимулирования спроса на инновации, модернизации структуры сектора исследований и разработок;
6	Развитие финансовой инфраструктуры инновационной деятельности;
7	Создание механизмов поддержки правовой охраны результатов перспективных коммерческих разработок российских инновационных компаний;
8	Повышение степени интеграции России в мировые процессы создания и использования инноваций;
9	Реализация программ развития инновационных территориальных кластеров.

Выполнение плана данной Стратегии будет способствовать развитию основополагающих элементов поддержки инновационной деятельности в России, а также динамичному формированию социально ориентированной инновационной экономики [4].

Для реализации направления Стратегии – по совершенствованию системы образования и поддержки создания стартапов в ведущих российских университетах планируется осуществлять всестороннюю помощь в организации бизнес-инкубаторов.

Начиная с 2005 года поддержка развития бизнес-инкубаторов становится частью государственной политики, поэтому на создание

их базовой инфраструктуры средства выделяются из бюджетных источников.

Немаловажным вопросом в развитии инновационной системы в России является поддержка регионов, путем государственного субсидирования. Для этих целей Минэкономразвития выделили более 1,6 миллиарда рублей на поддержку малого бизнеса в субъектах РФ, в том числе 276 миллионов рублей Московской области [5].

Отметив необходимость инновационного развития страны и готовность государства к финансовой поддержке подобных проектов, рассмотрим сущность и роль бизнес-инкубаторов в университетах. Итак, бизнес-инкубатор — это организация, которая оказывает всестороннюю поддержку проектов молодых предпринимателей на всех этапах его развития.

Бизнес-инкубаторы играют все большую роль в развитии экономики региона и социальной сферы. Данный факт можно объяснить с нескольких точек зрения.

Во-первых, эти структуры благотворно влияют на рост количества малых предприятий. Именно в бизнес-инкубаторах создаются наиболее приемлемые условия для старта и первоначального развития малого предприятия. Согласно статистике, выживает не более 30% малых предприятий, рискнувших начать свою деятельность самостоятельно, в то время как в бизнес-инкубаторе выживает около 80%. Кроме того, они более приспособлены к деятельности в современных рыночных условиях.

Во-вторых, решается проблема занятости населения, это способствует значительному снижению социальной напряженности и росту экономической активности на внутреннем рынке.

В-третьих, при создании бизнес-инкубаторов определенного вида и фиксации условий предоставления услуг и поддержки, решаются экономические и социальные проблемы региона, путем направления деятельности малых предприятий в приоритетные для региона и муниципальных образований сферы деятельности.

В-четвертых, выращивание в бизнес-инкубаторах малых технологических фирм способствует повышению инновационной активности бизнеса в регионе, внедрению новых технологий, использованию инноваций для решения проблем в различных важных сферах, за решение которых ответственны региональные структуры власти.

Таким образом, бизнес-инкубаторы дают возможность решать многие актуальные проблемы, как на уровне отдельных муниципальных образований, так и на уровне региона в целом. Они являются важным элементом стратегии развития региона в инновационном направлении [3].

Наиболее значимая роль бизнес-инкубаторов наблюдается в наукоградах и других муниципальных образованиях, где особенно развит научно-производственный комплекс. Высокая концентрация научного потенциала, наличие большого количества разработок, готовых для промышленного использования, делают создание организаций инновационной инфраструктуры объективной необходимостью.

По замыслу администраций наукоградов инновационная инфраструктура призвана обеспечивать весь процесс движения научной разработки – от научно-исследовательских и опытно-конструкторских разработок до массового производства. Исходя из этого, в наукоградах строится последовательная цепочка предприятий, имеющих инновационную направленность: бизнес-инкубатор – технопарк – муниципальная промышленная зона. Каждая из этих структур играет свою роль в создании инновационного бизнеса. Такой подход уже успешно реализуется в Обнинске и Дубне.

Организация бизнес-инкубаторов в стенах университетов приобретает всё большую популярность во многих регионах. Потребность в подобном виде бизнес-инкубаторов объясняется тем, что именно в высших учебных заведениях имеется высокий потенциал актуальных идей и научных разработок, которые нуждаются в организационной и финансовой помощи [7].

В 2010 году известный журнал «Forbes» выбрал пять наиболее эффективных бизнес-инкубаторов России, которые работают в университетах или тесно сотрудничают с ними [6]. Рассмотрим основные характеристики университетских бизнес-инкубаторов, которые вот уже многие годы не уступают своих лидерских позиций.

1) Бизнес-инкубатор Академии народного хозяйства

Бизнес-инкубатор при Академии народного хозяйства был открыт 27 мая 2010 года. Особенностью данного бизнес-инкубатора является возможность организации личных встреч с лидерами соответствующей индустрии. Например, фонд гражданских исследований и развития «CRDF» организовал образовательную программу в стенах бизнес-инкубатора, которая позволила

участникам прорабатывать свои стартапы с наставниками из Кремниевой долины.

Дополнительно бизнес-инкубатор берет на себя привлечение потенциальных инвесторов; материальное обеспечение проекта при участии в отраслевых выставках; оплату патентования и регистрации юридического лица; финансирование исследований.

Бизнес-инкубатор при Академии народного хозяйства связан более чем со 120 стартапами. Непосредственно в стенах инкубатора каждый год должны быть размещены семь стартапов. Одним из самых перспективных проектов данного инкубатора считается проект ePythia, сервис, позволяющий с помощью смартфона, привязывать задачу к месту на карте.

2) Бизнес-инкубатор ГУ-ВШЭ

Бизнес-инкубатор ГУ-ВШЭ был открыт 1 декабря 2006 года. Отличительной особенностью бизнес-инкубатора ГУ-ВШЭ является широкий спектр программ, таких как: лаборатория бизнеса с Дмитрием Молчановым, социальное предпринимательство, летний образовательный лагерь, английский разговорный клуб и многие другие.

Кроме того, данный бизнес-инкубатор обеспечивает финансирование стартапов за счет ГУ-ВШЭ, а также связи с общественностью и продвижение проектов инкубатора на различных выставках.

Среди самых популярных и востребованных выпускников инкубатора можно назвать следующие: пенсионный навигатор Pensiamarket.ru; онлайновая система по продаже цветов b2b flowers; Skillopedia — интернет-сервис, предназначенный для обучения интернет-пользователей посредством видео; roomix — программа, позволяющая каждому пользователю выбирать мебель и товары для ремонта из каталогов различных магазинов, тем самым создавая в интернете уникальный дизайн интерьера по своему вкусу.

3) Бизнес-инкубатор МГУ

Становление современного бизнес-инкубатора при МГУ началось с программы «Формула успеха», запущенной в 2004 году. Бизнес-инкубатор МГУ поддерживается Британским советом и Фондом содействия развитию малых форм предприятий в научно-технической сфере. Из дополнительных услуг можно отметить доступные тематические вебинары.

В год инкубатор выпускает 5 жизнеспособных проектов. Среди которых — ООО «Молекулярные технологии», которое позволяет с помощью компьютера смоделировать лекарственные вещества, проект «Стереоник», занимающийся выпуском флуоресцентных наноскопов.

4) Инкубатор РЭУ им. Плеханова

Инкубатор РЭУ им. Плеханова был открыт в июне 2009 года**.** Преимущества инкубатора — это тесное сотрудничество с частными и корпоративными инвесторами, технопарками, а также с инкубаторами физико-технических вузов. В дополнение к этому бизнес-инкубатор продвигает услуги и продукцию стратапов; занимается маркетинговой и исследовательской деятельностью, проведением опросов и экспертиз; внедряет в учебный процесс университета инновационные образовательные технологии, прошедших апробацию в РЭУ.

Ежегодно инкубатор объединяет вокруг себя 40-45 эффективных проектов. Например: студенческое рекламное агентство milkshake, компании LemonTree (занимается аксессуарами для мобильных устройств) и BinConnect (работа с облачными сервисами).

Следует отметить, что современный этап рыночной экономики в России характеризуется созданием теоретических основ и методологического инструментария перехода предприятий на инновационный путь развития и как подтверждают авторы в работе [8, С. 39], что «ядром инновационной деятельности оказывается университет».

Организация бизнес-инкубатора на территории нашего города полностью оправдана, ведь именно Королёв является неофициальной космической столицей России, здесь сосредоточенно большое количество крупных научно-производственных предприятий ракетно-космической промышленности, конструкторских бюро и исследовательских центров.

Подводя итог вышесказанному, можно смело заявить, что у «МГОТУ» есть все шансы стать эффективным бизнес-инкубатором для перспективных стартапов. Доказательствами тому являются:

1) Стремительное развитие университета; Пройдя длинный путь от института до университета всего лишь за 18 лет, «МГОТУ» значительно опередил многие образовательные учреждения, которые тратят на это десятилетия.

2) Хорошее материальное обеспечение; В распоряжении ВУЗа имеются три функционирующих здания бывшей Академии, два здания колледжа и техникума, а также новое здание на этапе строительства. Аудитории в корпусах университета отремонтированы и оборудованы современными компьютерными технологиями, что позволяет сделать учебный процесс высокотехнологичным и удобным для восприятия. Кроме того, в университете работают высококвалифицированные специалисты, способные стать ответственными наставниками, для помощи начинающим предпринимателям в развитии их стартапов.

3) Студенты готовы к открытию собственного бизнеса, т.к. опрос показал, что об открытии собственного дела задумывались 47 % респондентов, 35% - заинтересованы, и всего лишь 18% считают, что это не их сфера деятельности. Анализ результатов опроса дает основания полагать, что в нашем учебном заведении есть достаточное количество потенциальных предпринимателей из числа студентов, которые смогут работать и обучаться в студенческом бизнес-инкубаторе «МГОТУ» [1, С.101-108].

4) Имеется опыт создания бизнес-инкубатора в 2009 г. В этот период в КИУЭС планировалось создание при кафедрах бизнес-центров по оказанию услуг планируемым к созданию малым предприятиям, соответствующим профилю кафедр. Было создано 7 малых предприятий. Они получили всестороннюю поддержку со стороны руководства вуза, то есть начинающим предпринимателям были доступны льготы на использование помещений, рекламу, бесплатное пользование оборудованием, информационными и консультационными услугам. Кроме того, был обеспечен доступ к интеллектуальному потенциалу университета, полезным связям с органами власти и ведущими предприятиями города. В частности, одно из них ООО «Транслит» эффективно функционирует, оказывая услуги по техническому переводу на английский, немецкий, французский, китайский и другие языки.

Таким образом, на современном этапе создание студенческого бизнес-инкубатора на базе «МГОТУ» даст возможность решить следующие важные задачи на местном и региональном уровне [2]:

1) Увеличивать количество новых рабочих мест.

2) Стимулировать экономическую активность в регионе.

3) Способствовать структурной перестройке экономики, развитию малого и среднего предпринимательства, росту количества новых предприятий малого бизнеса.

4) Повышать эффективность производства традиционных товаров и осваивать качественно новые виды предпринимательской деятельности.

5)Развивать отдельные отрасли промышленности и диверсифицировать местную экономику.

6) Повысить занятость среди молодежи, безработных, инвалидов и других социальных групп населения, нуждающихся в поддержке.

7) Проводить обучение и повышать квалификацию предпринимателей, общий уровень экономического образования клиентов, предпринимательскую способность населения региона в целом;

8) Повышать уровень конкурентоспособности местной продукции на внутреннем рынке с возможностями вывода её на внешние рынки.

9) Повышать инновационный потенциал региона.

Литература

1. Бронникова Т.С. Инновационные методы в образовательном процессе вузов России /Перспективы, организационные формы и эффективность развития сотрудничества ВУЗов стран Таможенного союза и СНГ [Текст] / сборник научных трудов международной научно-практической конференции: Королёв МО: ФТА, 2013

2. Волошина Л.А. Бизнес-инкубирование в условиях университета как форма малого предпринимательства и способ обеспечения конкурентоспособности образовательного учреждения // Теоретическая и прикладная экономика. — 2015. - № 2. - С.13-27.

3. Медведева Т.Ю. Бизнес-инкубаторы в региональных инновационных системах. Электронный ресурс. Режим доступа:http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/6c7ad944306287a3c3257441004a1eca (дата обращения: 23.12.2015).

4. Медведев в день выступления Путина в ООН и встречи с Обамой вышел на международную арену через Google по вопросу инноваций Электронный ресурс. Режим доступа: http://hitech.newsru.com/article/29sep2015/medvedev(дата обращения: 04.01.2016).

5. Минэкономразвития РФ выделил деньги регионам на обустройство бизнес-инкубаторов Электронный ресурс. Режим

доступа:http://www.1obl.ru/news/o-lyudyakh/chelyabinskaya-oblast-poluchila-pochti-3-milliona-rubley-na-podderzhku-malogo-biznesa/(дата обращения: 25.12.2015).
6. Пять лучших российских бизнес-инкубаторов. Электронный ресурс. Режим доступа:http://www.forbes.ru/svoi-biznes/startapy/59358-pyat-luchshih-rossiiskih-biznes-inkubatorov (дата обращения: 15.01.2016).
7. Седаков Д. М. Государственное финансирование бизнес-инкубаторов в России // Интернет-журнал «НАУКОВЕДЕНИЕ» Выпуск 2, март – апрель 2014 Электронный ресурс. Режим доступа: http://naukovedenie.ru/PDF/158EVN214.pdf(дата обращения: 25.12.2015).
8. Старцева Т.Е., Бронникова Т.С. Экономика и управление инновационным развитием предприятия: методологический инструментарий: монография/ Т.Е. Старцева, Т.С. Бронникова.− М.: РУСАЙНС, 2016. – 202 с.

МАРКЕТИНГОВАЯ ПОЛИТИКА ПРЕДПРИЯТИЯ: ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЙ АСПЕКТ

Торосян Надя Татуловна, Шатохина Виктория Олеговна,
студенты 2 курса кафедры Экономики
Научный руководитель: **Рыжкова Татьяна Васильевна**, к.э.н.,
доцент кафедры Экономики

Статья посвящена комплексному исследованию содержания и принципов формирования маркетинговой политики предприятия в современных условиях хозяйствования, совершенствование её теоретико-методологических положений. В статье приведен анализ определений маркетинговой политики предприятия, а также обобщены материалы по исследуемой проблеме. Вводятся в научный оборот процесс разработки маркетинговой политики предприятия, ее модель и показатели оценки. Данная проблема мало изучена и требует дальнейших исследований.

Маркетинговая политика предприятия, модель МПП, структура, концепция.

MARKETING POLICY OF ENTERPRISE: THEORETICAL AND METHODOLOGICAL ASPECT

Torosyan Nadya, Shatokhina Victoria, 2nd year students of the Department of economy
Scientific adviser: **Ryzhkova Tatyana,** Candidate of Economic Sciences, Assistant Professor of the Department of economy

The article is about complex research on content and the way of working marketing policy of enterprise out in contemporary conditions of economy, updating its theoretical and methodological knowledge. The article consists of analysis of definitions of marketing policy of enterprise and complex knowledge about it. The process of creating marketing policy, its scheme and estimations are generalized. Marketing policy is poor in developing and requires to be done more research Marketing policy, efficiency, image of enterprise.

Marketing policy of enterprise, model of marketing policy, structure, conception.

Изучение маркетинговой политики предприятия обусловлено значением маркетинга, как концепции управления рынком, в деятельности предприятия в условиях свободной конкуренции и рыночной системы хозяйствования, а также слабой проработанностью научного знания о маркетинговой политике и важностью осмысления теоретических положений маркетинговой политики, как элемента организационно-экономического механизма управления предприятием. Цели и задачи научного исследования представлены в таблице 1.

Таблица 1 – Цели, задачи, объект и предмет исследования МПП

Цели научной работы	исследование практики реализации маркетинговой политики предприятия в современных условиях хозяйствования,
	совершенствование её теоретико-методологических положений.
Задачи исследования	провести обзор знаний о маркетинговой политике предприятия;
	исследовать сущность содержание маркетинговой политики в её теоретическом и практическом аспектах;
	выявить роль маркетинговой политики в деятельности предприятия;
	определить цели, задачи, функциональное назначение, виды МПП;
	определить ее место в экономической политике предприятия;
	установить соотношение маркетинговой стратегии и маркетинговой политики предприятия;
	разработать алгоритм формирования МПП;
	систематизировать факторы, определяющие ее содержание и структуру.

продолжение таблицы 1

Объект исследования	маркетинговая политика предприятия.
Предмет исследования	степень разработанности проблемы.

Маркетинговая политика предприятия (МПП), как сложная экономическая категория, в трудах ученых представлена в виде взаимоотношения агентов, масштабного плана, рыночного механизма, курса поведения на рынке (таблица 2) . Процесс формирования понятия является не завершенным и само понятие МПП определено недостаточно качественно.

Термин МПП упоминается в Налоговом кодексе РФ. Практики предлагают разрабатывать маркетинговую политику в качестве официального документа предприятия и закреплять его локальным нормативным актом. В настоящий момент маркетинговая политика отражает и фиксирует вопросы разработки товарного ассортимента, ценообразования, стимулирования сбыта товаров и организационные меры [3, 8].

Таблица 2 – Оценка определений МПП

Автор	Определение	Оценка определения
В.А. Костецкий	Маркетинговая политика это совокупность взаимоотношений, складывающихся в итоге целенаправленного взаимодействия групп с целью завоевания, удержания и использования конкурентоспособных преимуществ для осуществления своих интересов.	Маркетинговая политика – взаимоотношения агентов рынка с целью достижения нужных результатов.
А. Фенин	Маркетинговая политика – это всеобъемлющий план, ориентирующийся на основную идею или на определенные величины (цели) и устанавливающий основные рамки поведения (стратегии), а также описывающий необходимые оперативные действия (использование маркетинговых инструментов).	Маркетинговая политика – масштабный план по достижению целей.
	Маркетинговая политика – рыночный механизм, определяющий правила деятельности компаний и организаций, бизнесменов, менеджмента, основываясь на существующих общественных и экономических условиях, устоях и законах рынка.	Маркетинговая политика – рыночный механизм, правила деятельности предприятия на рынке.
Е.А. Касаткина	Маркетинговая политика – форма конструирования концепции, стратегии и тактики маркетинговой деятельности компаний .	Маркетинговая политика объединяет концепцию, стратегию и тактику компании.

Е.П. Голубков	Маркетинговая политика – документ, в содержании которого отражаются: главная политика компании, методы разработки бюджета маркетинг, организация маркетинговых исследований, а также вырабатываются применяемые маркетинговые стратегии.	Маркетинговая политика - документ, содержащий маркетинговый бюджет, исследования и стратегии организации.
А.А. Баняева	Маркетинговая политика – курс, линия поведения организации на рынке, определяемые руководством в соответствии с целями, ресурсами и охватывающей все ее формы.	Маркетинговая политика - курс поведения на рынке, соответствующий целям и ресурсам предприятия.
А.Н. Медведев	Маркетинговая политика – заключается в проведении комплекса мероприятий (как стратегических, так и тактических), направленных на удержание позиций предприятия на рынке и обеспечения получения прибыли, расширения сегмента продаж и круга потребителей и получение конкурентных преимуществ.	Маркетинговая политика – комплекс мероприятий по закреплению на рынке и получению прибыли.

По необходимости, целесообразности и компетентности предприятия разрабатывают и в своей деятельности руководствуются кадровой, финансовой, технологической, учетной, политиками и др. (рисунок 1).

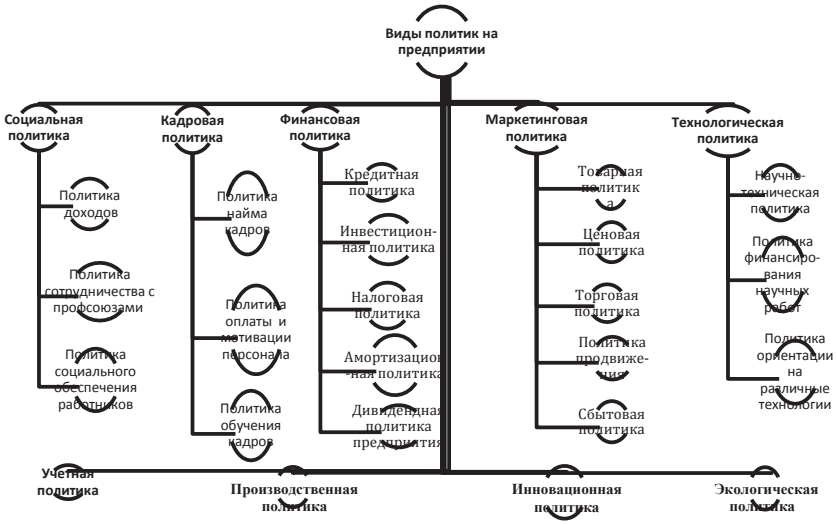


Рисунок 1 – Система политик на предприятии

Роль маркетинговой политики в деятельности предприятия существенна, поскольку решает большой круг задач, и определяется

содержанием и значением маркетинга в рыночной экономике, экономической политике и системе управления предприятием [1, 2, 7]

Роль маркетинговой политики предприятия обусловлена существованием самой рыночной системы хозяйствования и содержанием концепции маркетинга как инструмента управления рынком. МПП различается методами и периодом разработки, содержанием, характером (рисунок 2).

Пассивная политика направлена на ликвидацию негативного воздействия рынка, реактивная состоит в контроле над симптомами состояния и разработке мер по решению проблем, превентивная обусловлена наличием прогноза развития ситуации и отсутствием средств для ее изменения, а активная МПП обусловлена наличием и прогноза развития ситуации, и средств воздействия на нее.

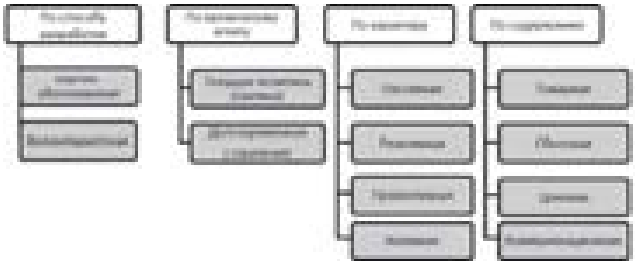


Рисунок 2 - Виды маркетинговой политики предприятия

Формирование маркетинговой политики предприятия начинается с выработки научной концепции развития маркетинга и проходит стадии определения цели предприятия, постановки задач маркетинга, обоснования и выбора маркетинговой стратегии, планирования маркетинговой деятельности предприятия, определения механизма реализации и оценки эффективности маркетинговой политики (рисунок 3).

Рисунок 3 - Процесс разработки МПП

Концепция маркетинговой политики предприятия – это система взглядов на цели, задачи, содержание стратегии и тактики маркетинга и его роли в деятельности предприятия (авторское определение).

При определении цели маркетинговой политики необходимо учитывать такие аспекты как содержание, масштаб цели, время ее достижения и сегмент рынка [6, 10].

Цели маркетинговой политики могут быть, как целями общего характера, так и целями функциональных подразделений, по направлениям бизнеса или по использованию маркетинговых инструментов, таких как товар, цена, сбыт и ФОСТИС [6].

По содержанию и назначению цели маркетинговой политики могут быть связаны с рынком, эффективностью деятельности предприятия, его финансовым состоянием, персоналом или имиджем.

В процессе исследования определены задачи маркетинговой политики (рисунок 4)

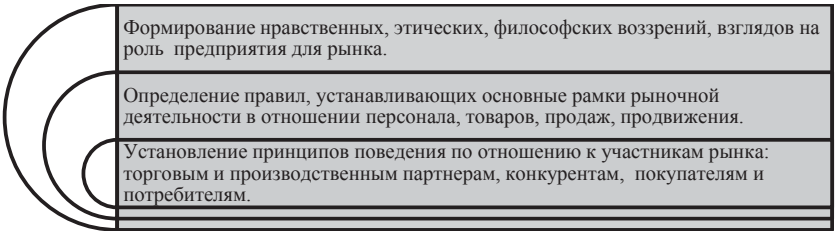


Рисунок 4 − Задачи МПП

Маркетинговая политика предприятия выполняет целый спектр функций (рисунок 5).

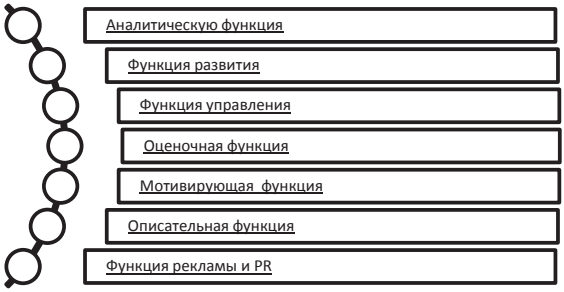


Рисунок 5 − Функции МПП

Содержанием аналитической функции МПП является удовлетворении потребности организации в информации о внешней среде. Сущность функции развития заключается в определении и

развитии целевых сегментов, совершенствовании ассортимента продукции предприятия. Кроме того, МПП выполняет функции управления, оценочную, мотивирующую, описательную, функцию рекламы и PR, т.е. осуществление коммуникаций с потенциальными потребителями [5, 9].

При разработке маркетинговой политики высокого качества, соответствующей своим целям и задачам, предприятию необходимо следовать принципам гибкости, системности, комплексности, перспективности, количественной и качественной сбалансированности, а также соответствия запросам потребителей и целям предприятия (рисунок 6).

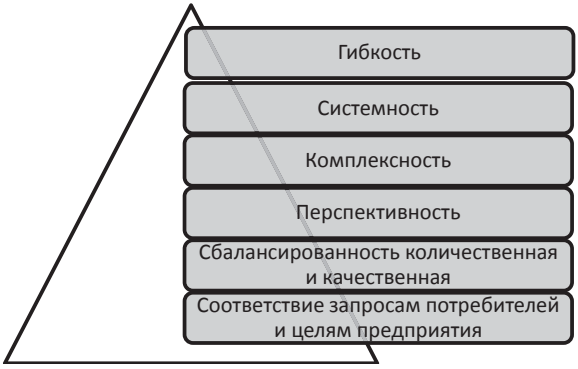


Рисунок 6 − Принципы МПП

На содержание маркетинговой политики влияют факторы внешней и внутренней среды (рисунок 7). Внешними факторами, определяющими содержание МПП, являются конкуренция, правовое регулирование деятельности со стороны государства, сфера деятельности, в которой функционирует предприятие, состояние экономики, технологии и природные условия расположения предприятия.

Наличие маркетингового мышления, цели предприятия, его ресурсы, модель ведения бизнеса, участие собственника в управлении, уровень мотивации персонала и состояние внутренней логистики составляют внутренние условия, которые влияют на маркетинг предприятия.

Особая роль в маркетинговой политике предприятия принадлежит маркетинговой стратегии. Стратегия – это модель поведения, которой следует организация для достижения

долгосрочных целей. Маркетинговая стратегия, являясь элементом общей стратегии компании, определяющим направление использования ресурсов для достижения максимального результата в увеличении продаж в кратко- и долгосрочной перспективе.

Рисунок 7 – Факторы, определяющие содержание маркетинговой политики предприятия

В процессе построения стратегии маркетинга выявляется продолжительность маркетингового периода (краткосрочное, среднесрочное, долгосрочное планирование), определяются цели маркетинга – конечные (стратегические) и промежуточные (тактические), разрабатываются мероприятия, направленные на достижение промежуточных и окончательных целей, проводится мониторинг хода выполнения стратегических планов.

В зависимости от содержания и существующих целей, которые ставят и реализуют предприятия, различают 4 вида маркетинговых стратегий - стратегии роста компании, стратегии охвата рынка, маркетинговые стратегии, зависящие от динамики потребительского спроса и конкурентные стратегии.

Цели предприятия и цели маркетинга, маркетинговая стратегия, как условный, глобальный план поведения для достижения целей предприятия и маркетинговых целей и содержания комплекса маркетинга (товар, цена, сбыт и коммуникации) образуют структуру МПП.

Построенная нами модель МПП, отражающая связи и взаимодействия между службами и структурными подразделениями предприятия в процессе разработки и реализации маркетинговой поли-

тики, представлена на рисунке 8. Субъектами маркетинговой политики являются руководство, службы и персонал предприятия.

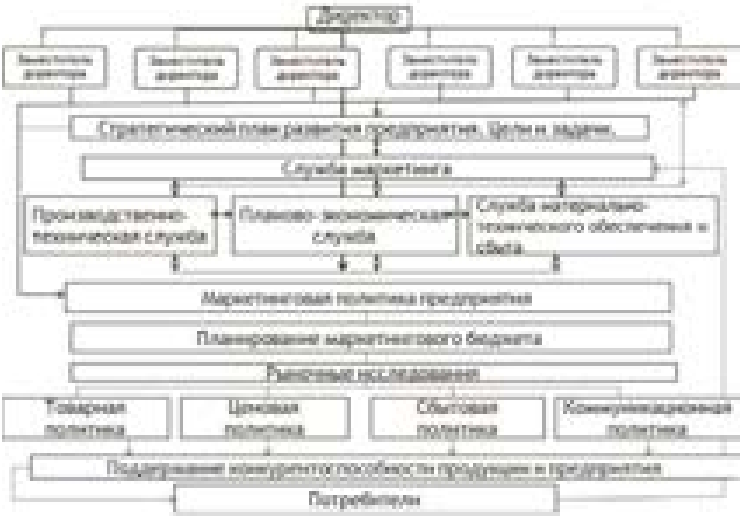


Рисунок 8 - Модель маркетинговой политики предприятия

Формирование маркетинговой политики предприятия заключается в подготовке аналитической информации для разработки маркетинговой политики; разработке содержания МПП, отвечающего целям и задачам предприятия на каждом конкретном этапе его развития; оформлении и утверждении организационно-распорядительного документа «Положение о маркетинговой политике предприятия».

Для оценки маркетинговой политики предприятия предлагаем использовать показатели, представленные в таблице 3.

Таблица 3 – Оценка маркетинговой политики предприятия

№	Показатели	Единицы измерения	Расчет
1	Выручка от реализации	руб.	$В = Q \cdot Ц$
2	Прибыль от реализации	руб.	$П = В - С$
3	Доля рынка	%	$Др = \frac{Qo}{Емкость\ рынка}$
4	Расходы на продажу	руб.	Расходы на хранение, тару и упаковку, погрузку продукции, рекламу, участие в выставках, др. акции по формированию спроса и стимулированию сбыта

5	Выручка от реализации на 1 руб. расходов на продажу	руб.	$Врп = \frac{В}{Рас.прод}$
6	Прибыль на 1 руб. расходов на продажу	руб.	$Прп = \frac{П}{Рас.прож}$
7	Коэффициент конкурентоспособности предприятия	-	$Кк = Крас + Кдох + Кч$
8	Коэффициент конкурентоспособности по цене	-	$Кк = \frac{Ц\max + Ц\min}{2 \cdot Цпредпр}$

Итогом работы является выявление степени определенности понятия маркетинговой политики предприятия, обоснование его значение в деятельности предприятия, описание процесса разработки, определение концепции и установление факторов, определяющих содержание маркетинговой политики, построена ее модель, а также предложены показатели для её оценки.

Литература

1. Банчева, А.А. К вопросу о маркетинговой политике предприятия (маркетинговая политика в теории и практике) / А.А. Банчева // Маркетинг в России и за рубежом. – 2011. – № 6. С. 14–22.

2. Крипак, Е.М. Формирование эффективной маркетинговой политики предприятия: методы, модели, технологии [Электронный ресурс] / Е.М. Крипак // Вестник Оренбургского государственного университета. 2011. № 13 (132). С. 263-268. Режим доступа: http://vestnik.osu.ru/2011_13/45.pdf (дата обращения: 11.11.2015)

3. Медведев, А.Н. Маркетинговая политика организации для целей налогообложения. Электронный ресурс. Режим доступа: http://www.nalvest.ru/nv-articles/detail.php?ID=32683 (дата обращения 10.11.2015).

4. Пантелеева, Т.А. Теоретические и методологические подходы к исследованию сбытовой и коммерческой политики предприятия / Т.А. Пантелеева // Экономика и управление: новые вызовы и перспективы. – 2011. Т. 1., № 2. С. 275-278

5. Рубцова, Н.В. Маркетинговая политика как форма операционного маркетинга: содержание и проявления в условиях российской практики [Электронный ресурс] / Н.В. Рубцова // Электронный научный журнал Известия. – 2013. - №1. Режим доступа: http://eizvestia.isea.ru/reader/article.aspx?id=18685 (дата обращения: 10.12.2015)

6. Скударева, Н.З., Рыжкова, Т.В. Использование системы маркетинга как фактор повышения статуса вуза. Современная экономика: проблемы, пути решения: Сборник статей открытой научно-практической конференции преподавателей кафедры экономики. М.: Изд-во «Научный консультант», 2015. С. 111-123.
7. Соловьев, Б.А. Управление маркетингом: 17-модульная программа для менеджеров «Управление развитием организации». Модуль 13 / Б.А. Соловьев. – М.: ИНФРА-М, 2000. – 288 с.
8. Степина А.Ф. Маркетинговая политика и налоговые обязательства компании / А.Ф. Степина, Д.М. Касаткин // Управление рисками. – 2004. – № 3. – С. 53–60.
9. Фадеев, В.А. Особенности формирования и реализации маркетинговой политики предприятия в условиях рыночной экономики [Электронный ресурс] / В.А. Фадеев // современная наука: актуальные проблемы теории и практики. Серия Экономика и право. – 2012. – № 1. Режим доступа: http://www.nauteh-journal.ru/index.php/---ep12-01/342 (дата обращения: 01.12.2015).
10. Хасбулатова, Б.М. Концептуальные подходы к определению маркетинговой и товарной политики предприятия [Электронный ресурс] / Б.М. Хасбулатова // Теория и практика общественного развития. – 2014. – № 16. Режим доступа: http://teoria-practica.ru/rus/files/arhiv_zhurnala/2014/16/economics/khasbulatova.pdf (дата обращения: 10.12.2015)

КОМПЛЕКСНОЕ ИСПОЛЬЗОВАНИЕ ВОСТОЧНОГО И ЗАПАДНОГО ПОДХОДОВ К УПРАВЛЕНИЮ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ ТРУДОВЫХ РЕСУРСОВ

Цыганкова Марина Сергеевна, студентка 4 курса кафедры Экономики
Научный руководитель: **Лучкина Вероника Вячеславовна,** к.э.н., доцент кафедры Экономики

Российские предприятия нуждаются в качественно новом подходе к управлению для повышения эффективности использования трудовых ресурсов и хозяйственной деятельности в целом. Изучение Восточного и Западного подходов к управлению дало идею их практического применения в комплексе. При правильном понимании целей комплексное использование инструментов вышеупомянутых

подходов даст возможность по-новому подойти к проблеме оптимизации хозяйственной деятельности и повышения эффективности трудовых ресурсов.

Оптимизация бизнеса, повышение эффективности, Восточный подход, Западный подход, бенчмаркинг, управленческая культура.

INTEGRATED USAGE OF EASTERN AND WESTRERN MANAGEMENT METHODS TO IMPROVE EFFICIENCY OF LABOR FORCE

Tsygankova Marina, 4th year student of the Department of economics
Scientific adviser: **Luchkina Veronica,** Candidate of Economic Sciences, Associate Professor of the Department of economics

Russian companies need a whole new management method to improve the improve efficiency of labor force and economic activity in general. The study of Eastern and Western management methods gave an idea of their practical application in the complex. With the right understanding of the objectives of the integrated use of the tools above methods will enable a new method to the problem of optimization of economic deyatelnoti and efficiency of labor resources.

Business optimization, improvement the efficiency, the Eastern management method, the Western management method, benchmarking, management culture.

Российский фирмы и предприятия часто сталкиваются с проблемой поиска внутренних резервов для оптимизации бизнеса и для повышения его эффективности. На сегодняшний день на большинстве предприятий происходит следующее: бизнес-процессы не оптимальны, простои оборудования, все склады заполнены готовой продукцией, численность персонала не соответствует адекватной реальности, соотношение производственного и административного персонала не оптимально.

Для того чтобы понять, как решить проблему оптимизации и повышения эффективности бизнеса, необходимо рассмотреть два подхода: Восточный и Западный подходы.

Суть Восточного подхода заключается в первую очередь в оптимизации методов работы: исследование проблем, создание новых инструкций, работа по новым инструкциям, изменение нормативов

труда, оптимизация численности. Кроме этого все это поддерживается корпоративной культурой, направленной на совместное решение проблем, и использование следующих инструменотов: Кайдзен (непрерывное совершенствование), Канбан (непрерывное пополнение запасов), Пока-йоке (защита от ошибок), 5S (организация рабочего места), составление карт потоков создания ценности. Японская модель основывается на философии « Мы все одна семья», поэтому самая важная задача японских менеджеров – установить нормальные отношения с работниками, сформировать понимание того, что рабочие и менеджеры – одна семья. По данным опросов 70% японцев считают себя обязанными принимать близкое участие в делах друзей (рис.1).

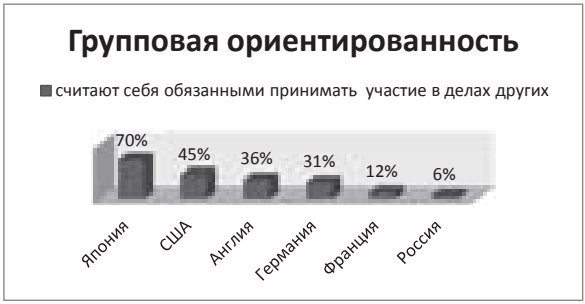


Рисунок 1 - Групповая ориентированность трудоспособного населения в разных странах

Опросы работников всемирно известной фирмы «Сони Корпорейшен» показали, что 83% опрошенных считают себя одной «командой», усиленные совместные действия которой принесут всем ее членам пользу (рис.2).

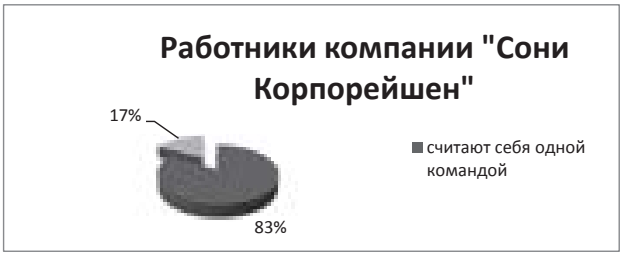


Рисунок 2 - Результаты опроса работников компании «Сони Корпорейшен»

Суть Западного подхода состоит в том, чтобы сначала определить максимально достижимую цель, а затем разработать меры по достижению желаемого результата. В основе этого подхода лежит система измерения и бенчмаркинга. Одним из самых распространенных показателей измерения является OEE (overall equipment effectiveness), показывающий, насколько эффективно используются основные производственные фонды. Этот показатель складывается из трех составляющих: время простоя оборудования, производительность, качество.

После проведения измерений наступает время бенчмаркинга: компании изучают лучшие показатели по OEE у конкурентов с аналогичным оборудованием или моделируют максимально возможный OEE с учетом предельно интенсивной загрузки своего оборудования. Таким образом, компании понимают, каких целей необходимо достичь при оптимизации производства. Множество фирм добилось успеха, основываясь на этом подходе (рис.3).

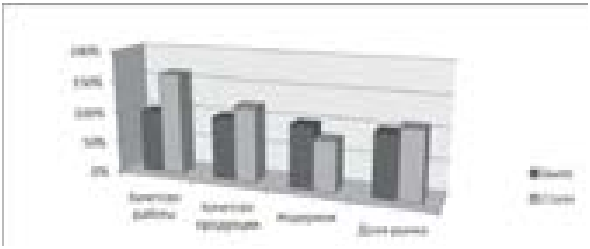


Рисунок 3 - Результаты применения Западного Подхода в компании «Ксерокс»

После постановки целей можно переходить к выявлению причин проблем и планированию изменений.

Этот подход рассчитан на иную, чем у японцев, управленческую культуру: гораздо более персональную (зависящую от решений конкретных людей), а не регламентированную, директивную, а не консенсусную.

В Восточном и Западном подходах есть общие черты, которые заключаются не только в целевом применении – первый и второй предлагают для оптимизации создание кружков качества. Например, для компании «Вестингауз» специальный колледж "качества" организовал подготовку в области качества двадцати тысяч работников объединенных в 2000 «кружков качества». Это помогло компании в последние три года увеличить производительность труда

на 7 % в год. Кроме этого, увеличить на пятьдесят процентов объем производства без привлечения внешних ресурсов.

В России нет таких организаций, которые имели бы успех после аппробации одного из подходов. Управленческая культура отечественных компаний в большинстве своем более персональная, чем регламентированная, т.е. на первое место ставятся не инструкции, а конкретные люди. При этом она более директивная, чем консенсусная — конкретные инициативы идут сверху, от руководства к коллективу. На уровне менеджмента наша культура часто более достиженческая, склонная к самостоятельности, а на «нижних этажах» организации — исполнительская.

Существует ли особенный, российский подход к оптимизации?

Возможно, Россия еще не готова к созданию своего особенного подхода. Таким образов решить проблему оптимизации можно с комплексным использованием двух вышеосписанных подходов с учетом фактора времени.

Компаниям и предприятиям, не имеющем временных резервов, нуждающимся в оперативном решении проблемы, предлагается следовать Западному подходу, поскольку российским компаниям он намного ближе и освоить его национальным предприятиям намного проще. Восточный подход в краткосрочной перспективе освоить не представляется возможным – российский работник не готов действовать по причине непонимания данного подхода (для освоения не обходимо достаточно времени).

Компаниям и предприятиям, располагающим достаточными резервами времени, компаниям, которые рассматривают долгосрочную перспективу развития необходимо следовать Восточному подходу, который способствует «закалке» предприятия на начальном уровне. Возможно, использование Восточного подхода создаст благоприятную бизнес-среду молодым предприятиям в будущем.

Если при использовании одного из двух подходов с учетом фактора времени, предприятие добилось успеха, то следующим шагом будет – поддержание достигнутой оптимизации для достижения еще большей эффективности бизнеса. С этой целью, можно применять два подхода комплексно, однако «вводить второй в дело» необходимо постепенно, чтобы российский работник успел усвоить для чего это нужно: для улучшения эффективности работы предприятия в целом, подразделения, личного карьерного роста.

Таким образом, для достижения своих целей по оптимизации, российским компаниям необходимо с осторожностью применять подходы для решения своих проблем. Только так возможно закрепить полученный результат и понять схему действия подходов, которые умеют успех в странах Востока и Запада.

Литература

1. Мескон М., Перевод с английского. Общая редакция д.э.н. Евенко Л.И. Основы менеджмента – управление трудовыми ресурсами [Текст] //М.: Дело. – 2009 – 672 с.
2. Пирогов С.В. Социальное прогнозирование и проектирование. [Текст] // М.:Проспект – 2015. – 363 с.
3. Половец Н.Д. Типы руководителей – стили управления. [Текст] //М.: 2004. – 221 с.
4. Шевчук Д. Стратегический менеджмент: конспект лекций. // Издат.: ЭКСМО. - 2009. - 122 с.

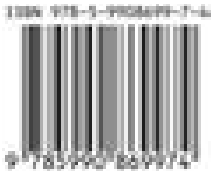
Научное издание

РЕСУРСАМ ОБЛАСТИ - ЭФФЕКТИВНОЕ ИСПОЛЬЗОВАНИЕ

XVI Ежегодная научная конференция студентов
Технологического университета

Сборник материалов
Часть 1

Сдано в набор 15.08.2016.	Подп. в печ. 22.08.2016.
Формат 60×88/16.	Бумага офсетная.
Усл.печ.л. 8,5	Тираж 50 экз.



Издательство Научный консультант
123007, г. Москва, Хорошевское ш., 35к2, офис 508.
Тел.: +7 (926) 609-32-93, +7 (499) 195-60-77 www.n-ko.ru keyneslab@gmail.com