ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
МОСКОВСКОЙ ОБЛАСТИ

«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА,
ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

СОВРЕМЕННЫЕ ИННОВАЦИИ В ЭКОНОМИКЕ, ТЕХНИКЕ И ОБЩЕСТВЕ

V Ежегодная научная конференция магистрантов
Технологического университета

Сборник материалов

г.о. Королёв

2022

УДК 330.3:621
ББК 65.011:30:60.56
С56

С56 **Современные инновации в экономике, технике и обществе:** Сборник материалов V Ежегодной научной конференции магистрантов Технологического университета: [Электронный ресурс]: Текст. дан. и граф. – М.: Изд. «Научный консультант», 2022. - 1 электрон. опт. диск (CDR). - Объем издания: 10,4 Мб.; Тираж 500 экз. – Систем. требования: IBMPC с процессором Intel(R) Pentium (R) CPU G3220 @; частота 3.00 GHz; 4Гб RAM; CD-ROM дисковод; Windows 7 Ultimate; мышь; клавиатура, Adobe Acrobat XI Pro, Adobe Reader

Настоящий сборник содержит материалы V Ежегодной научной конференции магистрантов Технологического университета «Современные инновации в экономике, технике и обществе».

Цель проведения конференции - привлечение магистрантов к решению актуальных задач современной науки, обмен информацией о результатах исследований, углубление и закрепление знаний, стимулирование творческого отношения к своей профессии, приобретение навыков научных дискуссий и публичных выступлений.

Тематика конференции соответствует направлениям подготовки магистров «Технологического университета».

***** *Все материалы даны в авторской редакции*

ISBN 978-5-907477-75-9

СОДЕРЖАНИЕ

ПОВЫШЕНИЕ КАЧЕСТВА ИНТЕГРАЛЬНЫХ МИКРОСХЕМ СВЧ В РАДИОЭЛЕКТРОННОЙ АППАРАТУРЕ ПУТЕМ ИСПОЛЬЗОВАНИЯ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ

Азарова Полина Алексеевна, магистрант 1 курса кафедры управления качеством и стандартизации
Научный руководитель: **Асташева Надежда Павловна**, д.б.н., профессор, профессор кафедры управления качеством и стандартизации

В последнее время монолитные интегральные схемы (далее МИС СВЧ) получили широкое распространение не только в гражданской технике, но и особенно в бортовой электронной аппаратуре радиоэлектронных систем вооружения, связи и космической техники. Основными причинами являются бурное развитие высокоскоростных широкополосных систем передачи данных с использованием инновационных технологий при серийном производстве.

СВЧ, радиоэлектронная аппаратура, инновационные технологии.

IMPROVING THE QUALITY OF INTEGRATED MICROCIRCUIT MICROWAVE ELECTRONIC EQUIPMENT BY THE USE OF INNOVATIVE TECHNOLOGIES

Azarova Polina, 1st year graduate student of the Department of Quality management and standardization
Scientific adviser: **Astasheva Nadezhda**, Doctor of Biological sciences, Professor, Professor of the Department of Quality management and standardization

Recently, monolithic integrated circuits (hereinafter referred to as MIS microwave) have become widespread not only in civil engineering, but especially in on-board electronic equipment of radio-electronic systems for weapons, communications and space technology. The main reasons are the rapid development of high-speed broadband data transmission systems using innovative technologies in mass production.

Microwave, radio-electronic equipment, innovative technologies.

Из исследований промышленного рынка с 2017-2022 год можно заключить, что одной из областей роста рынка будут тонкопленочные интегральные микросхемы, поскольку они продолжают вытеснять габаритные микросхемы для традиционных и специальных схем. Интегральные микросхемы в первую очередь всегда буду актуальны при

изготовлении в сегментах рынка передовых медицинских устройств, беспроводных базовых станций и инфраструктуры передачи данных [2, 3].

Область беспроводной связи развивается очень быстрыми темпами. Некоторые известные приложения - это беспроводные персональные сети, локальные сети, глобальные сети, спутниковая связь, сотовая связь и многое другое. Все эти приложения требуют внедрения высокопроизводительных активных и пассивных схем, работающих на высокой частоте. Каждый тип беспроводных систем предъявляет различные требования к производительности составляющих схем и систем.

В секции передатчика шум, подавление помех и избирательность полосы пропускания более ослаблены по сравнению с секцией приемника, но линейность и энергоэффективность являются проблемами, вызывающими озабоченность в секции передатчика. Кроме того, на высоких частотах паразитная емкость и индуктивность вывода делают проектирование схем и систем очень сложным и сложным. Такие характеристики, как небольшие размеры, низкая стоимость и высокая производительность, делают монолитную интегральную схему СВЧ / миллиметровых волн (MMIC) очень подходящим вариантом для проектирования схем и систем на высоких частотах. Одной из специфических проблем при проектировании MMIC для конкретной системы является выбор правильного устройства и правильного материала в соответствии с требованиями схемы и системы. В этой статье предпринята попытка рассмотреть некоторые из известных материалов, используемых для реализации MMIC, наряду с их характеристиками, преимуществами, недостатками, связанными с технологиями активных устройств и потенциальными областями применения.

Материалы МИС СВЧ. На данный момент существует большое разнообразие комбинаций материалов эмиттера, базы и коллектора, и наибольшее распространение получили n-p-n транзисторные гетероструктуры типа InAlAs–InGaAs –InP и InP–InGaAs–InP. СВЧ-приборы на основе нитрида галлия позволяют добиться больших значений удельной плотности выходной мощности [1].

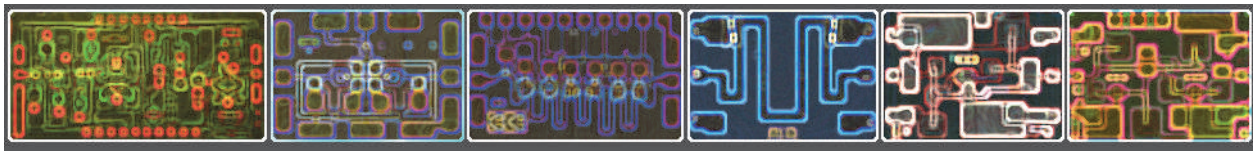


Рисунок 1 – Примеры МИС СВЧ

Активные элементы МИС и их надежность. Монолитные интегральные микросхемы СВЧ (MMIC) с частотой выше 18 ГГц разрабатываются из-за важных потенциальных системных преимуществ в области стоимости, надежности, воспроизводимости и контроля параметров схемы.

Требования к упаковке для MMIC обсуждаются 1n с точки зрения тепловых, механических и электрических параметров для оптимальной желаемой производительности.

Достижения 1n GaAs в области высокочастотных устройств и технологии материалов делают возможной монолитную интеграцию СВЧ-схем.

Монолитные микроволновые интегральные схемы GaAs (MMIC), работающие на высоких частотах (Ku-диапазон и выше), являются перспективными для будущих применений космической связи. Легкий вес, небольшие размеры и высокая надежность из MMIC делают их кандидатами для создания превосходных систем космической связи. Применение систем космической связи MMIC 1n требует разработки модулей передачи и приема для систем фазированных антенных решеток. Чтобы в полной мере использовать характеристики MMIC, упаковка и соединение MMIC для интеграции на этих частотах требуют многочисленных соображений. Низкие потери радиочастотного сигнала, широкая полоса пропускания, удобство изготовления и надежность - вот лишь некоторые из них.

Характеристики MMIC, влияющие на соединения и упаковку требования к дизайну, материалам и изготовлению описаны на примерах, разрабатываемых MMIC. Для радиочастотных соединений ввода/вывода MMIC для детального анализа был выбран переход типа mlcrostrlp от Van-Heuven к волноводу, который обеспечивает простоту интеграции MMIC для тестирования и упаковки. Обсуждаются улучшения, которые были получены 1n при выполнении этого перехода путем модификации 1n конструкции и материалов.

Полевые транзисторы с барьером Шоттки. Понимание природы высоты барьера на двумерной границе раздела полупроводник/металл является важным шагом для встраивания слоистых материалов в будущие электронные устройства. Измерение высоты барьера Шоттки и его понижения на границе раздела дихалькогенид переходного металла (TMD) /металл полевого транзистора показало, что высота барьера на границах раздела золото / однослойный дисульфид молибдена (MoS_2) уменьшается с увеличением напряжения стока, и это снижение достигает 0,5-1 В. Базовая структура выращивания приведена на рис. 2.

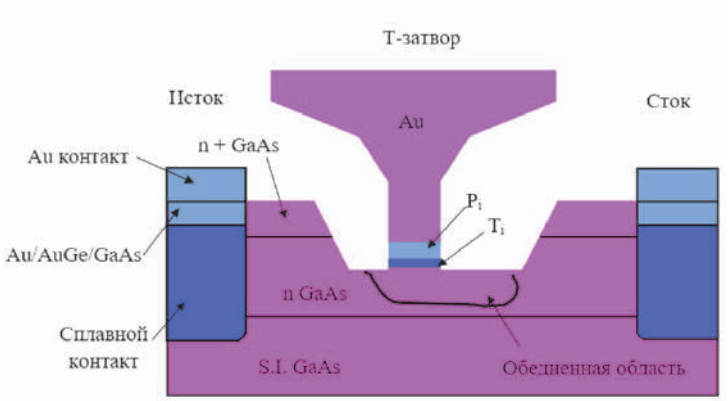


Рисунок 2 – Базовая структура выращивания

Конструкция выращивания высокочистых тонких пленок. Бета-фазный оксид галлия продемонстрировал потенциал в качестве сверхширокополосного полупроводника для применения в силовых электронных устройствах и коротковолновой оптоэлектронике. Для монокристаллической тонкопленочной эпитаксии бета-фазы оксида галлия было исследовано несколько методов изготовления, но каждый из них сталкивается с проблемами, препятствующими росту высококачественных и высокочистых тонких пленок.

Одним из этих методов является металлоорганическое химическое осаждение из паровой фазы (MOCVD), в попытке создать более совершенные тонкие пленки бета-фазы оксида галлия. Исследования, проведённые в 2017 году достигли рекордно высокой подвижности носителей для тонких пленок как при комнатной, так и при низких температурах. Интегральные микросхемы продемонстрировали рекордно низкую концентрацию экстрагируемой компенсации, что имеет решающее значение для контролируемой настройки концентрации легирования.

Исследователи вырастили тонкие пленки бета-фазы оксида галлия, легированные кремнием, на (010)-ориентированных полуизолирующих нативных подложках, легированных железом, с использованием MOCVD. Они варьировали температуру роста, соотношение VI:III и давление в камере, чтобы проверить влияние различных параметров роста на свойства конечного материала. Характеристика материала с помощью сканирующей электронной микроскопии, атомно-силовой микроскопии, масс-спектроскопии вторичных ионов и рентгеновской дифракции подтвердила образование высококачественных и высокочистых тонких пленок. Тонкие пленки демонстрировали отличные электротранспортные свойства, с гладкой морфологией поверхности на атомном уровне и разумной скоростью роста около одного микрона в час.

Эти результаты демонстрируют возможность выращивания тонких пленок бета-фазы оксида галлия с помощью MOCVD, предпочтительной в промышленности полупроводниковой эпитаксиальной технологии, и потенциал этого материала для применения в мощных устройствах.

Технология изготовления выращивания тонкопленочных резисторов. Первым шагом традиционно является изготовление тонкопленочных резисторов. Металл резистора (AuGeNi) испаряется, затем наносится TaN. Базовые этапы технологии приведены на рис. 3. Микросхемы и основе тонкопленочных технологий на основе никель-хромовых слоев обеспечивают повышение производительности и более прочную конструкцию при все более низкой цене по сравнению с решениями на основе толстых пленок. Эпитаксиальная структура базового транзистора с высокой подвижностью электронов (HEMT) приведена на рис. 4а, псевдо-морфного транзистора — на рис. 4б. Ключевым элементом в HEMT является специализированный PN-переход, который он использует. Он известен как

гетеропереход и состоит из соединения, в котором используются различные материалы по обе стороны от соединения. Наиболее распространенными материалами являются арсенид галлия алюминия (AlGaAs) и арсенид галлия (GaAs). Обычно используется арсенид галлия, поскольку он обеспечивает высокий уровень основной подвижности электронов, и это имеет решающее значение для работы устройства. Кремний имеет гораздо более низкий уровень подвижности электронов, и в результате он никогда не используется в HEMT.

Существует множество различных структур, которые могут быть использованы в HEMT, но все они используют в основном одни и те же производственные процессы. При изготовлении HEMT сначала внутренний слой арсенида галлия наносится на полуизолирующий слой арсенида галлия. Его толщина составляет всего около одного микрона. Наносится слой толщиной около одного микрона.

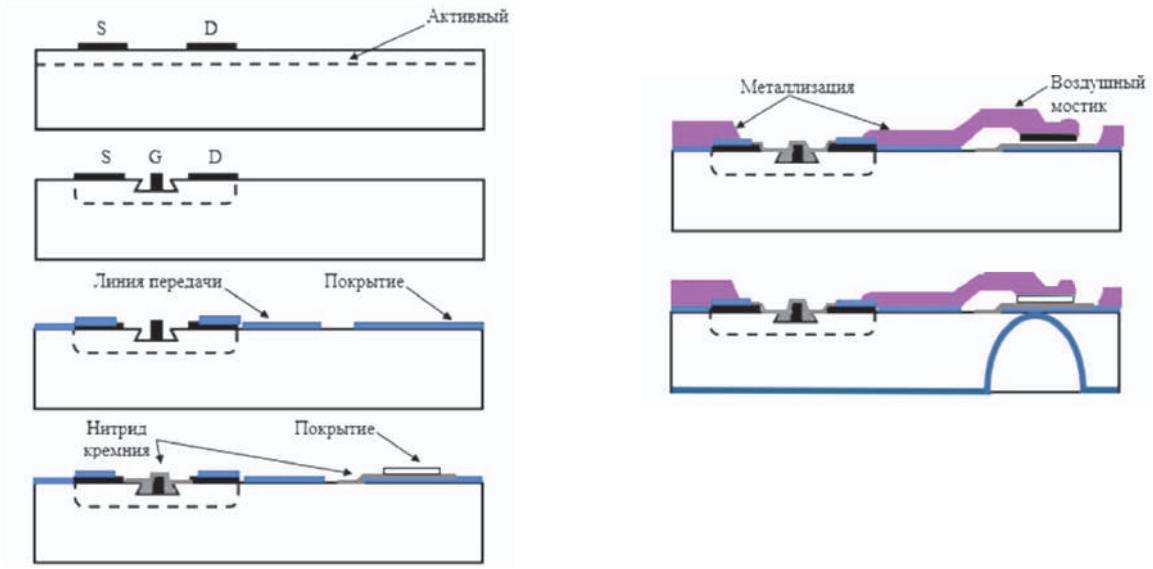
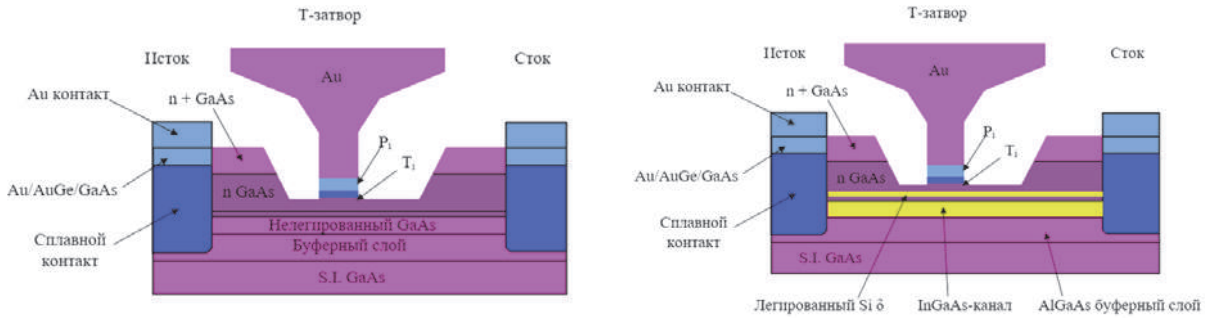


Рисунок 3 – Базовые этапы технологии изготовления выращивания тонкопленочных резисторов



Структура с высокой подвижностью электронов (а)

Структура псевдоморфного транзистора (б)

Рисунок 4 – Эпитаксиальная структура базовых транзисторов

Наносится слой толщиной около одного микрона. Затем поверх этого наносится очень тонкий слой арсенида алюминия-галлия. Его цель состоит в том, чтобы обеспечить отделение границы раздела гетероперехода от области легированного арсенида алюминия-галлия. Это имеет решающее значение для достижения высокой подвижности электронов. Над этим расположен легированный слой арсенида алюминия-галлия. Требуется точный контроль толщины этого слоя, и для этого требуются специальные методы.

Есть две основные структуры, которые используются. Это самонастраивающаяся ионная имплантируемая структура и структура затвора с углублением. В случае самонастраивающейся ионной имплантированной структуры затвор, сток и источник установлены вниз и, как правило, представляют собой металлические контакты, хотя контакты источника и стока иногда могут быть изготовлены из германия. Затвор обычно изготавливается из титана, и он образует крошечный переход с обратным смещением.

Для конструкции затвора с углублением нанесен еще один слой арсенида галлия n-типа, позволяющий устанавливать контакты стока и источника. Толщина под затвором также очень важна, поскольку этим определяется пороговое напряжение полевого транзистора. Размер ворот, а значит, и канала очень мал.

Дальнейшее развитие HEMT известно, как PHEMT. Псевдоморфные транзисторы с высокой подвижностью электронов, широко используются в беспроводной связи. Транзисторы PHEMT находят широкое признание в системах спутниковой связи всех форм, включая спутниковое телевидение прямого вещания, DBS-TV, где они используются в коробках с низким уровнем шума, используемых со спутниковыми антеннами. Технология PHEMT также используется в высокоскоростных аналоговых и цифровых ИС, где требуется чрезвычайно высокая скорость.

Технология изготовления HEMT/PHEMT. Первым этапом является формирование активного канала и имплантация изолятора, после чего формируются омические переходы, затем осуществляется формирование углублений затвора, после — области «затвор–металл». После этого производят травление истока и контактов, формируют воздушные мостики. Подложкой в данном случае служит полупроводниковая пластина арсенида галлия [1]. Типичная последовательность изготовления приведена на рис. 5.

Биполярные гетеротранзисторы. Гетеропереходы позволяют получить качественное улучшение быстродействия биполярных транзисторов. Рабочая скорость биполярного транзистора может быть значительно увеличена, если количество легирования в базе может быть увеличено без изменения эффективности эмиттера. Это можно сделать, если для эмиттерного перехода используется гетеропереход Конструкция биполярных гетеротранзисторов. Подложкой в данном случае служит полупроводниковая пластина арсенида галлия. Эпитаксиальные слои могут

быть выращены раз личными способами, например, молекулярно-лучевой эпитаксией.

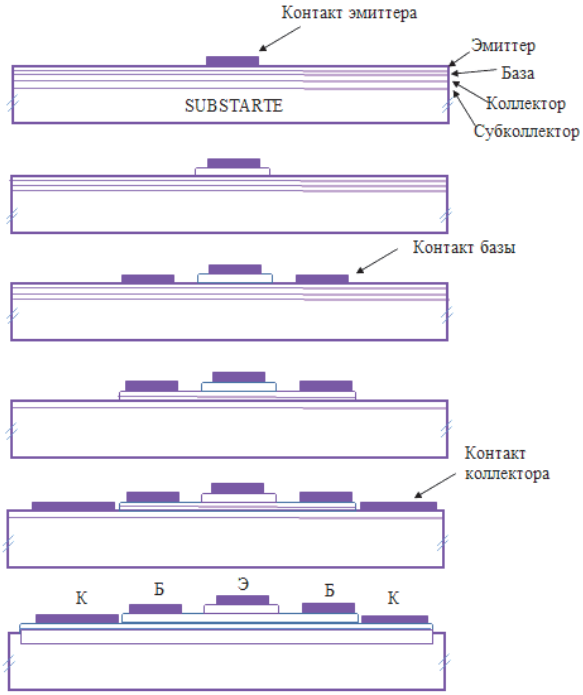


Рисунок 5 – Последовательность изготовления HEMT/PHEMT

Технология изготовления HBT. Гетеропереходные биполярные транзисторы (HBT) представляют собой вертикальные транспортные структуры, многие параметры которых чувствительно зависят от слоев epi. Эти устройства имеют постоянные преимущества в коротком времени прохождения и высоких частотах среза по сравнению с другими транзисторными архитектурами. HBT на основе InP используются в приложениях, включая цифровое и высокочастотное испытательное оборудование OC1920-100 Гбит/с и OC768-40 Гбит/с с высокими требованиями к производительности. MBE используется для производства HBT на основе InP из-за гораздо более высокого максимального уровня легирования n-типа в слоях InP и InGaAs. Превосходная производительность устройства в архитектуре n-p-n обусловлена несколькими факторами в материалах на основе InP, производимых MBE. Что касается излучателя n-типа, In (Al)GaAs имеет перестраиваемую запрещенную зону и транспорт n-типа с высокой подвижностью. Что касается основы, то InGaAs и GaAsSb обладают высокой проводимостью p-типа и могут быть легированы, как правило, углеродом, в количестве, превышающем 1E20/см^3. Что касается коллектора, InP и InGaAs обладают высокой подвижностью n-типа. Легирующие добавки n-типа (кремний) и p-типа (углерод) имеют минимальную тенденцию к диффузии при низких температурах роста MBE, что позволяет создавать высокоэффективные ультратонкие слои. Объем

производства НВТ варьируется в зависимости от того, какие новые области применения требуют самых высоких частот. Литейное производство MBE может масштабироваться для удовлетворения спроса, благодаря многолетнему опыту роста НВТ.

Таким образом, повышение требований к объему передаваемой информации обеспечивает непрерывное динамичное развитие как СВЧ МИС, так и проектирования технологии их производства. Для проектирования это были, прежде всего, усовершенствование конструктивно-технических особенностей СВЧ МИС, разработка технологии производства микросхем на подложках из карбида кремния (SiC) и нитрида галлия (GaN) и конструкции. Постоянное совершенствование конструкции и технологии МИС СВЧ, вызывает необходимость модификации моделей надежности, в том числе новых механизмов отказов, связанных с применением новых материалов и технологий.

Литература

1. КиберЛенинка [Электронный ресурс]. Режим доступа: https://znanium.com/catalog/product/1850071 (дата обращения: 20.04.2022).

2. Электронно-библиотечная система Znanium [Электронный ресурс]. Режим доступа: https://znanium.com/catalog/product/1850071 (дата обращения: 20.04.2022).

3. Электронно-библиотечная система Znanium [Электронный ресурс]. Режим доступа: https://znanium.com/catalog/product/947708 (дата обращения: 20.04.2022).

3D-МОДЕЛИРОВАНИЕ В СПЕЦИАЛЬНЫХ СЛУЧАЯХ

Барилко Ирина Александровна, магистрант 2 курса кафедры математики и естественнонаучных дисциплин
Научный руководитель: **Самаров Ким Леонидович,** д.ф.-м.н., профессор кафедры математики и естественнонаучных дисциплин

Новые технологии развиваются стремительно. Применение 3D-моделирования в медицине улучшает качество вмешательств, проводимых человеку для улучшения состояния здоровья. 3D-моделирование помогает повысить качество усвояемости материала в процессе обучения студентов медиков и как следствие повышает эффективность образовательной деятельности учебного заведения. В статье проведен обзор применения технологии 3D-моделирования в медицине (лечение и диагностика) и при обучении студентов медиков.

3D-моделирование, медицина, медицинские исследования, студенты медицинских вузов.

3D-MODELING IN SPECIAL CASES

Barilko Irina, 2nd year graduate student of the Department of Mathematics and natural sciences
Scientific adviser: **Samarov Kim,** Doctor of Physical and mathematical sciences, Professor of the Department of Mathematics and natural sciences

New technologies are developing rapidly. The use of 3D modeling in medicine improves the quality of interventions carried out for a person to improve their health. 3D modeling helps to improve the quality of material digestibility in the process of teaching medical students and, as a result, increases the efficiency of the educational activities of an educational institution. The article provides an overview of the use of 3D-modeling technology in medicine (treatment and diagnostics) and in teaching medical students.

3D-modeling, the medicine, medical research, medical students.

3D-модели есть везде. Они стоят за каждым физическим объектом, с которым мы сталкиваемся, и широко используются в различных отраслях. В частности, они приносят пользу в медицине: протезирование – одним из самых легендарных и хорошо задокументированных медицинских применений 3D-принтера является производство протезов за меньшую стоимость их заводских оригиналов; медицинские модели – врачи, хирурги и стоматологи могут сделать 3D-сканирование своего пациента и использовать

3D-модель, чтобы заранее отработать процедуру; медицинские приборы и инструменты – печать медицинских устройств особенно полезна в развивающихся странах, где обычные медицинские инструменты не всегда могут себе позволить; стоматология – 3D-печать имеет огромное применение в стоматологии, потому что рот каждого человека уникален.

Крупные корпорации, такие как Facebook, Google, Amazon и Netflix, ежегодно выделяют миллиарды долларов на разработку технологий виртуальной реальности и создание контента, поддерживающего 3D-графику [1].

Поэтому любая профессия, связанная с этими направлениями, сейчас востребована. Задача специалистов по 3D моделированию — придать объем и форму любым объектам в реальном или виртуальном мире.

Сегодня будет рассмотрено 3D-моделирование в особых случаях в медицине.

3D-моделирование может помочь в спасении жизней людей. В мае 2015 года компания Dassault Systems выпустила научно точную и коммерчески доступную 3D-модель здорового человеческого сердца [2]. Подобные 3D-симуляции могут помочь в диагностике сердечно-сосудистых заболеваний, позволяя протестировать бесконечное количество решений перед лечением, что потенциально может привести к гораздо более ранней диагностике и предотвращению большого процента ненужных смертей, вызванных сердечно-сосудистыми заболеваниями.

В последние десятилетия 3D-печать находит все более широкое применение в области медицины. От ортопедии до сердечно-сосудистых заболеваний и визуализации опухолей [3].

В 2016 году Радиологическое общество Северной Америки создало Специальную группу по интересам по 3D-печати для создания руководств, рекомендаций и учебных занятий по надлежащему использованию 3D-печати в медицинских целях с целью улучшения здравоохранения, обслуживание пациентов [4].

3D-модели при сердечно-сосудистых заболеваниях. 3D и КТ, МРТ, УЗИ.

На сегодняшний день доступные в литературе, традиционные инструменты двумерной (2D) и трехмерной (3D) визуализации ограничены 2D-экраном, что влияет на реалистичность визуализации анатомических структур и патологий для набора 3D-данных. Это проявляется при лечении сложных патологий. Это создало потенциальные возможности для использования технологии 3D-печати в медицинских целях.

Такие методы обследования, как компьютерная томография (КТ), магнитно-резонансная томография (МРТ) и ультразвуковая диагностика УЗИ, – высоко эффективны. Эти методы обследования позволяют выявить и диагностировать различные заболевания с высокой степенью достоверности [5].

Из-за особенностей анатомии сердца, 3D-печать является находкой для раскрытия патологий, связанных с ишемической болезнью сердца.

Исследования подтверждают пользу использования 3D-моделей при ишемической болезни сердца. В частности, в сложных случаях и при предоперационном планировании [9].

10 здоровых добровольцев и 3 пациента с расслоением аорты в анамнезе прошли магнитно-резонансную томографию сердечно-сосудистой системы с использованием 3D-визуализации. На рисунке 1 можно увидеть МРТ сердца. На первой трети картинки показана ориентация плоскостей для кровотока и количественной оценки напряжения сдвига стенки, на второй трети представлено сердце здорового 20-летнего добровольца, и на последней трети изображено сердце 50-летнего мужчины, который имеет проблемы с сердцем [6].

Исследование 1. Была набрана группа из 35 студентов, обучающихся на врачей-кардиологов. Были использованы методы визуализации: обычные 2D-рисунки тетрады Фалло и физические 3D-модели, напечатанные из наборов данных 3D-визуализации сердца (МРТ сердца, КТ и 3D-эхокардиограмма).

17 студентов были включены в группу, использующую 2D-изображения и 18 студентов в группе, использующую 3D-модели.

Студенты, которых обучали с помощью 3D-моделей, дали более высокие суммарные баллы удовлетворенности учащихся. Группа, обучающаяся на 3D-модели, имела более высокие совокупные баллы само эффективности, но разница не была статистически значимой.

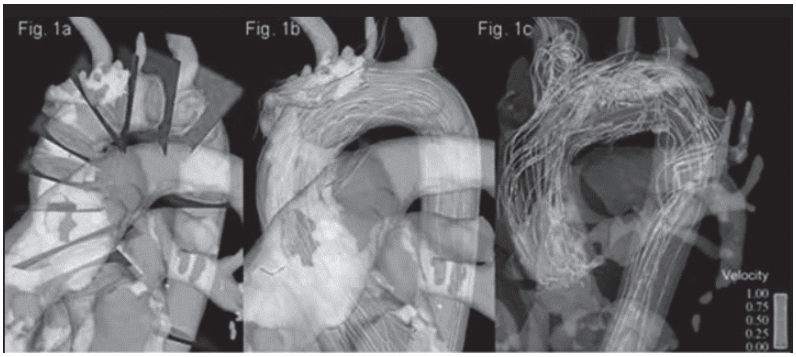


Рисунок 1 – 3D-модель МРТ сердца

Студенты, которых обучали с помощью 3D-моделей, дали более высокие суммарные баллы удовлетворенности учащихся. Группа, обучающаяся на 3D-модели, имела более высокие совокупные баллы само эффективности, но разница не была статистически значимой.

Приобретение знаний измерялось путем сравнения результатов теста знаний до и после занятия. Удовлетворенность учащихся и рейтинги само эффективности измерялись с помощью анкет, которые студенты заполняли после учебных занятий [7].

Значит, физические 3D-модели улучшают обучение студентов теме тетралогии Фалло, повышая удовлетворенность учащихся.

Исследование 2. 60 студентов разделили на две группы, 29 и 31 участников в каждой соответственно. Обе группы получили одну и ту же 20-минутную лекцию, включающую 2D-изображения дефекта межжелудочковой перегородки. Второй группе дополнительно предоставили напечатанные 3D-модели здоровых сердец и несовершенных сердец. По итогу, студенты, которые изучали лекцию с применением дополнительных материалов – распечатанных 3D-моделей быстрее принимали верные решения и чувствовали себя уверенней [7].

Исследование 3. Опыт исследования с использованием 3D-печатных моделей ишемической болезни сердца подтвердил эффективность их использования, доказал влияние на хирургическое планирование и лечение. В исследование были включены 40 пациентов с ишемической болезнь сердца из десяти международных центров. 3D-модели были созданы с использованием изображений КТ и МРТ с высокой точностью изображения анатомических структур. Использование 3D-моделей не привело к изменению хирургического решения в 52,5% случаев, скорее всего, из-за простоты лечения ишемической болезни сердца. Однако почти в половине случаев (48%) хирургический подход был пересмотрен с использованием моделей, напечатанных на 3D-принтере, что подчеркивает клиническую ценность моделей, напечатанных на 3D-принтере, при лечении сложных случаев [9].

Специальная группа по интересам инициировала исследование качества и безопасности для выявления клинических ситуаций, где 3D-печать сердца взрослого человека считается подходящей.

Результаты были разделены по шкале от 1 до 9, где 1–3 считается неуместным, 4–6 возможно, но не желательно, 7–9 3D-печать как метод представления и/или расширения ценности данных, содержащихся в медицинских изображениях.

Ишемическая болезнь сердца получила 7 баллов по этой шкале, Болезнь аортального клапана транскатетерная – 9 баллов. Значит, при этих болезнях использовать 3D-технологии уместно.

Технология трехмерной (3D) печати используется в стоматологии.

При создании имплантов, в челюстно-лицевой хирургии и при протезировании. Использование шаблона, напечатанного на 3D-принтере, делает процедуру восстановления быстрее и удобнее.

Молодые врачи благодаря 3D-моделям могут не только научиться правильно создавать импланты, но и проверять верно ли подобран имплант с помощью 3D-модели челюсти пациента. Реставрация центральных резцов челюсти с использованием шаблона, напечатанного на 3D-принтере показана на рисунке 2 [10]. Она представляет собой быстрый и функциональный вариант реставрации центральных резцов челюсти. Таким образом, шаблон,

напечатанный на 3D-принтере, является приемлемой и надежной альтернативой традиционной прямой композитной реставрации центральных резцов верхней челюсти, включая сломанные зубы и кариес.

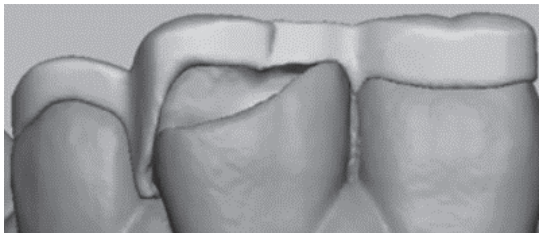


Рисунок 2 – 3D-модель для реставрации центральных резцов

3D-печатные модели опухолей. 3D-моделирование играет важную роль в диагностической оценке опухоли: размер, расположение, распространенность. Эта информация необходима для хирургического планирования и принятия решения об удалении опухоли. Из-за труднодоступности опухоли, технология 3D-моделирования показала большую значимость в оказании помощи при предоперационном планировании. Например, на рисунке 3 представлена 3D-модель печени, пораженной опухолью [5]. Модель была получена с помощь компьютерной томографии. Прототипом выступила печень 52-летней больной женщины, у которой после операции по удалению опухоли были обнаружены метастазы спусти 2 года.

3D-модели точно обнаруживают структуры и опухоли печени с высокой точностью по сравнению с исходными изображениями.

Было проанализировано 15 исследований, где в лечении была применена 3D-модель. В 53% выявлено соответствие развития процесса опухоли у человека 3D-модели и как следствие сокращении времени предоперационного исследования. Таким образом, необходимы испытания с на большем количестве данных, с последующим анализом и применением на практике.

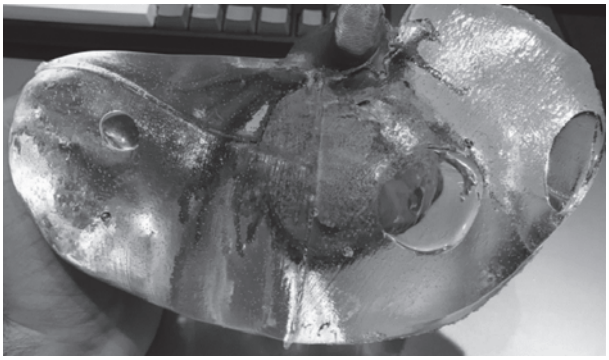


Рисунок 3 – 3D-модель печени, пораженной опухолью

Измерение жесткости опухоли для прогнозирования агрессивности протекания заболевания.

Эндометриальная карцинома является одной из наиболее распространенных первичных злокачественных опухолей у женщин, и ее заболеваемость неуклонно растет во всем мире. 82 пациентки с подозрением на опухоль матки прошли магнитно-резонансную томографии малого таза, и были зарегистрированы 15 пациенток с подтвержденной болезнью. По патоморфологическим результатам (степень опухоли, гистологический подтип, стадия, инвазивность миометрия) пациенты были разделены на две подгруппы. В процессе исследования был сделан вывод, что жесткость опухоли, измеренная с помощью 3D-модели, построенной на основе магнитно-резонансной томографии, может быть потенциально полезна для прогнозирования степени опухоли, стадии заболевания, а также может помочь в предоперационном планировании [11].

Модели, которые печатаются на 3D-принтере, востребованы в медицине: они анатомически точно передают особенности, помогают в пред- и послеоперационном планировании, помогают обучаться студентам-медикам. Медицинская 3D-печать как компонент лечения взрослых с сердечно-сосудистыми заболеваниями становится все более востребованной.

Литература

1. Сайт: piblitz.com [Электронный ресурс]. Режим доступа: https://piblitz.com/pi/3D-Modelling-Art-Design-and-Marketing-34874/i/ar-How%20to%20earn%20your%20rep%20in%203D%20design%3F/ (дата обращения: 24.04.2022)

2. Сайт: qims.amegroups.com [Электронный ресурс]. Режим доступа: https://mashable.com/archive/first-3-dimensional-heart-simulation#44_2ACxp6sqK (дата обращения: 24.04.2022)

3. Сайт: mashable.com [Электронный ресурс]. Режим доступа: https://qims.amegroups.com/article/view/19116/19379 (дата доступа: 24.04.2022)

4. Сайт: pubmed.ncbi.nlm.nih.gov [Электронный ресурс]. Режим доступа: https://pubmed.ncbi.nlm.nih.gov/29782619/ (дата обращения: 24.04.2022)

5. Сайт: innotech.ua [Электронный ресурс]. Режим доступа: https://innotech.ua/ru/news/sozdanie-modeli-chelovecheskoy-pecheni-na-3d-printere-oboshlos-v-150-65657 (дата обращения: 22.04.2022)

6. Сайт: jcmr-online.biomedcentral.com [Электронный ресурс]. Режим доступа: https://jcmr-online.biomedcentral.com/articles/10.1186/1532-429X-13-S1-P392 (дата обращения: 25.04.2022)

7. Сайт: academic.oup.com [Электронный ресурс]. Режим доступа: https://pubmed.ncbi.nlm.nih.gov/28134482/ (дата обращения: 25.04.2022)

8. Сайт: pubmed.ncbi.nlm.nih.gov [Электронный ресурс]. Режим доступа: https://academic.oup.com/ejcts/article/52/6/1139/3925909 (дата обращения: 25.04.2022)

9. Сайт: academic.oup.com [Электронный ресурс]. Режим доступа: https://academic.oup.com/ejcts/article/52/6/1139/3925909 (дата обращения: 25.04.2022)

10. Сайт: bmcoralhealth.biomedcentral.com [Электронный ресурс]. Режим доступа: https://bmcoralhealth.biomedcentral.com/articles/10.1186/s12903-018-0621-4 (дата обращения: 23.04.2022)

11. Сайт: cancerimagingjournal.biomedcentral.com/ [Электронный ресурс]. Режим доступа:https://cancerimagingjournal.biomedcentral.com/articles/10.1186/s40644-021-00420-8 (дата обращения: 23.04.2022)

ОПРЕДЕЛЕНИЕ УСТРОЙСТВ НЕГЛАСНОГО СЪЕМА ИНФОРМАЦИИ НА ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ

Будченков Даниил Сергеевич, магистрант 1 курса кафедры информационной безопасности
Научный руководитель: **Сухотерин Александр Иванович**, к.воен.н., доцент кафедры информационной безопасности

В наше время большее значение набирает защита информации и ее развитие, все больше людей понимают важность безопасности информации и какие последствия ждут при ее потере. Если дело касается бизнеса и больших денег, начальство предпочитает скрывать и тщательно охраняют информацию, разработки и другие конфиденциальные материалы, обрабатываемые на рабочем месте. Одним из наиболее часто применяемых средств нелегального съема информации в настоящее время является использование закладных устройств, функционирование которых может исчисляться днями или годами. Работают они на безобидной технологии беспроводного модуля передачи данных, который в свою очередь использует для передачи перехваченной информации легальные каналы связи, такие как, WiFi, BlueTooth, ZigBee, и другие средства беспроводной связи.

Закладное устройство, информационная безопасность, защита информации, беспроводные технологии, несанкционированный доступ.

DETERMINATION OF DEVICES OF PRIVATE RECEPTION OF INFORMATION AT THE OBJECT OF INFORMATIZATION

Buchenkov Daniil, 1st year graduate student of the Department of Information security
Scientific adviser: **Sukhoterin Alexander**, Candidate of Military sciences, Associate professor of the Department of Information security

Nowadays, the protection of information and its development are gaining more importance, more and more people understand the importance of information security and what consequences await when it is lost. When it comes to business and big money, the bosses prefer to hide and carefully protect information, developments and other confidential materials processed in the workplace. One of the most frequently used means of illegal information retrieval at the present time is the use of embedded devices, the functioning of which can be counted for days or years. They work on the harmless technology of a wireless data transmission module, which in turn uses legal communication channels, such as WiFi, BlueTooth, ZigBee, and other means of wireless communication to transmit intercepted information.

Embedded device, information security, information protection, wireless technologies, unauthorized access.

Возможности закладных устройств и способов промышленного шпионажа являются одними из основных факторов, определяющих угрозу безопасности информации. Поэтому люди, ответственные за обеспечение ее безопасности, должны внимательно отслеживать все изменения и новинки в развитии способов схем информации и технических характеристик средств добывания информации, а также приемников этой информации.

Специалисты, использующие аппаратуру поиска закладок, не могут различить зарегистрированное законное устройство беспроводной передачи информации, не снимающее информацию, от закладного устройства, работающего в это же диапазоне частот маскируемое под легальное средство связи и предотвратить своевременную утечку информации. Нахождение маскируемых закладных устройств без применения специальных документов и методик по выявлению закладных устройств и средств анализа трафика сети в реальном времени, невозможно и не реально.

Всем уже известные стандартные радио закладки моментально привлекают внимание своим видом в спектрограмме, не говоря о маскируемых закладных устройствах, которые могут специально маскироваться, как и внешне так и специально под одно из устройств работающее на объекте информатизации. Сигналы устройств, работающих в каналах беспроводной связи передачи данных, выглядят одинаково, будет это легальное устройство, выполняющее свои функции или же это будет закладное устройство, работающее около рабочего места сотрудника и передающее информацию злоумышленнику.

Стремительное развитие технологий передачи информации “по воздуху” дает развитие в направлении создания разнообразных закладных устройств для различного шпионажа, и с появлением все более современных стандартов передачи информации под угрозой оказывается сам специалист, которому пропустить замаскированный сигнал под легальное устройство достаточно просто без опыта и специального оборудования. Таким образом стоит задуматься над технологиями автоматизации для распознавания сигналов и написанием программ способных выполнять различные функции, что для узкого сканирования для уточнения сигналов в определенном сегменте, что для общего назначения, для определения типа сигнала и дальнейшего его отслеживания.

В наше время проще смастерить цифровой передатчик, используя современные технологии беспроводных средств связи, чем использовать старые технологии. Поэтому новые требования к ПО под управлением комплекса поиска ЗУ стоит разрабатывать из возможностей современных цифровых средств передачи данных, которые используют для этого передачи перехваченной информации. Разберем некоторые из них:

1) Wi-Fi (Wireless Fidelity) – Стандарт IEEE 802.11 используется в наше время постоянно для создания беспроводных локальных сетей в различных компаниях, где невозможно провести оптоволоконный интернет. Так называемые точки доступа или мобильные точки доступа высокоскоростного доступа в интернет, строятся по принципу миниатюрных передатчиков или модемов, работающих на горячих точках (хот-стопах) или точках доступа (переадресация основного хот-стопа), присоединенных к смартфону, или же модему сети фиксированной связи. Радиус покрытия одной точки доступа составляет примерно около 90–110 м. учитывая конструкции здания и плотности стен.

Наибольшее распространение на территории РФ получили следующие разновидности стандарта 802.11, а именно 802.11a, 802.11b, 802.1g.

Таблица 1 – Характеристики стандартов беспроводных сетей стандартов 802.11

Наименование характеристики	Стандарт			
	802.11	802.11b	802.11a	802.11g
Полоса частот, МГц	83,5	83,5	300	83,5
Диапазон частот, ГГц	2,40-2,4835	2,40-2,4835	5,15–5,35 5,725-5,825	2,40-2,4835
Количество непересекающихся каналов	3	3	12	3
Скорость передачи, Мбит/с	1,2	1,2,5.5, 11,22	6,9,12,18,24, 36,48,84	1,2,5.5,11, 22,6,9,12, 18,24,36, 48,54
Метод	DSSS	DSSS	OFDM	DSSS, OFDM
Тип модуляции	DBPSK, DQPSK	DBPSK, DQPSK	BPSK, QPSK, QAM	BPSK, QPSK, QAM

Диаграмма покрытия частотных каналов Wi-fi в 2,4 ГГЦ представлена на рисунке 1.

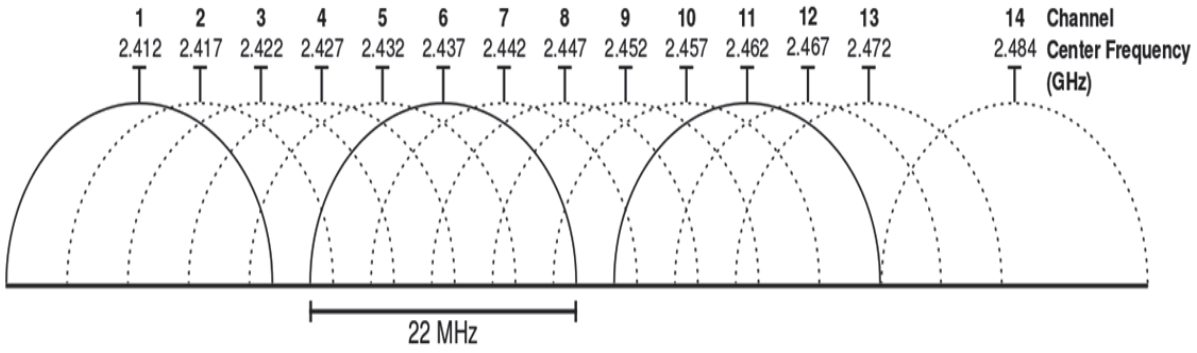


Рисунок 1 – Диаграмма перекрытия частотных каналов Wi-Fi в 2,4 ГГц

2) Стандарт Bluetooth (IEEE 802.15.1) – Соединяет между собой различие устройства как бытового плана, так и мобильные телефоны, ППК и другие виды устройств. От Wi-Fi отличается тем, что в нем для соединения используются радиосредства. Основные характеристики стандарта 802.15.1 представлены в таблице 2.

Таблица 2 – Характеристики стандарта IEEE 802.15.1 (Bluetooth)

Наименование характеристики	Значение характеристики
Диапазон частот, МГц	2400…2483,5
Максимальная эквивалентная изотропно излучаемая мощность для	Менее 2,5
наружных устройств с малым радиусом действия, мВт	
Максимальная эквивалентная изотропно излучаемая мощность для внутриофисных устройств, мВт	Менее 100
Способ расширения спектра сигнала	Псевдослучайная перестройка частоты
Номиналы несущих частот, МГц	2402+N, где N=0,…,76

Стандартный пакет Bluetooth состоит за кода доступа содержащий в себе 72 бита, заголовок, состоящий из 54 бит, и информационное поле, где максимальное количество информации может достигать 2744 бит.

Так же есть пакеты различных типов, которые могут состоять из кодов доступа, где теперь его длина равна примерно 68 битам, или заголовка и кода доступа вместе.

Bluetooth-устройство как правило содержит в себе чип небольших размеров, который выполняет роль приемопередатчика, работающего в диапазоне равный 2,4 ГГц. Соединенные два Bluetooth-устройства позволяют передавать множество данных на скорости примерно колеблющийся от мощности чипа и приемного устройства в районе от 420 до 720 кбит/с на расстоянии до 10–50 м. Всего Bluetooth-устройство может быть связано в реальном времени с другими устройствами, где их число от 4–8 устройств.

3) Стандарт ZigBee (IEEE 802.15.4) – дает возможность для обмена данными в 27 каналах в трехчастотных диапазонах 868,915,2400 МГц. Скорость передачи в единственном разрешённом в России частотном диапазоне составляет 2,4 ГГц, скорость может достигать 250 кбит в секунду. На частоте 2,4 ГГц есть 16 каналов Зигби, каждый канал требует ширины диапазона в 5 МГц.

Соотношение «сигнал/шум» позволяют сигналам стандарта IEEE 802.15.4 успешно сосуществовать с источниками излучения на той же частоте.

Передаваемые пакеты в стандарте IEEE 802.15:

Пакет Зигби содержащий данные;

Пакет Зигби содержащий подтверждения;

Пакет Зигби содержащий MAC команд;

Сигнальный пакет Зигби;

Основные параметры стандарта IEEE 802.15.4 представлены в таблице 3.

Таблица 3 – Основные параметры стандарта IEEE 802.15.4

Наименование характеристики	Стандарт		
	802.15.4 ZigBeeTM	802.15.4 ZigBeeTM	802.15.4 ZigBeeTM
Частота, МГц	868	915	2400
Число каналов/шаг, МГц	1/–	10/2	16/5
География распространения	Европа	Америка	Весь мир
Максимальная скорость кбит/с, модуляция	20, BPSK	40, BPSK	250, O-QPSK
Выходная мощность, ном.	0 dBm (1 мВт)	0 dBm (1 мВт)	0 dBm (1 мВт)
Дальность, м	10–100	10–100	10–100
Чувствительность, дБм	–92	–92	–85
Размер стека, кбайт	4–32	4–32	4–32
Срок службы батареи	От 100 до 1000 и более дней	От 100 до 1000 и более дней	От 100 до 1000 и более дней
Размер сети	65536 (16-битн.адр.), 264 (64-битн. адр.)	65536 (16-битн.адр.), 264 (64-битн. адр.)	65536 (16-битн.адр.), 264 (64-битн. адр.)

Пакет Зигби содержащий данные до 104 байт, используется для передачи информации на другое устройство. Data sequence number - отвечает за контроль нумерации пакетов. FCS (Frame Check Sequence) – отвечает за контрольную сумму последовательности кадров, обеспечивающий безошибочную передачу данных.

Таблица 4 – Общая классификация основных стандартов беспроводной передачи данных

Наименование характеристики	Стандарт		
	ZigBee	Bluetooth	Wi-Fi
Частотный диапазон, МГц	2400–2483	2400–2483	2412–2484
Скорость передачи данных, кбит/с	250	721	11000/54000
Дальность связи, м	200	До 100	100
Потребление тока, active мА/sleep мкА	30/1	70/20	450
Модуляция, доступ к среде	DSSS	FHSS	DSSS
Топология системы	«точка–точка», «звезда», сеть	«точка–точка», «звезда», сеть	«точка–точка», звезда
Частотный диапазон, МГц	2400–2483	2400–2483	2412–2484

Рассмотрим методику поиска закладных устройств.

- Развертывание комплекса
- Создается рабочее место для оператора комплекса, подключается необходимое оборудование в соответствии с требованиями технической безопасности;
- Определение зоны поиска.
- В соответствии с основными организационными мероприятиями, зона поиска характеризуется площадью, внутри которой комплекс радиоконтроля сможет получить сигнал от предполагаемой внедренной закладки на объекте.
- Удаление посторонних из зоны поиска.
- Удаление посторонних лиц из зоны поиска также проводится в соответствии с основными организационными мероприятиями
- Удаление или выключение всех средств беспроводного доступа
- Этот шаг необходим для того, чтобы разгрузить участок радиочастотного спектра, для осуществления его контроля и анализа.
- Отключение электропитания всех электронных устройств
- Перед тем как проводить исследования, необходимо отключить из цепей электропитания все электрические устройства. Это делается с целью получения на первоначальной спектрограмме всех сигналов, за исключением сигналов от возможных ЗУ, подключенных к цепям электропитания различных устройств.
- Включение поискового комплекса на сканирование диапазона частот, используемого для работы средств беспроводного доступа

- На этом этапе производится сканирование диапазона выбранных частот, с целью получения первоначальной спектрограммы, для последующего анализа.
- Включение в цепи электропитания всех электронных устройств
- Этот шаг необходим для выявления ряда демаскирующих признаков функционирования закладочных устройств, имеющих общую цепь питания от устройств.
- Включение всевозможных СВТ в помещении
- Этот шаг необходим для выявления ряда демаскирующих признаков функционирования закладочных устройств, встроенных в средства вычислительной техники.
- Включение тестового акустического сигнала
- Включение тестового акустического сигнала позволяет проверить наличие в помещение возможно внедренных закладочных устройств, работающих по акустопуску. При озвучке помещение, закладки, использующие данный тип включения, незамедлительно выйдут в эфир, отобразившись на спектрограмме.
- Активация комплекса на продолжительный радиоконтроль
- Продолжительный радиоконтроль используется для записи длительной и избыточной спектрограммы выбранного диапазона частот.
- Анализ полученной спектрограммы на наличие демаскирующих признаков функционирования закладочных устройств
- В соответствии с демаскирующими признаками функционирования закладных устройств, построенных на базе средств беспроводного, производится доскональный анализ, полученной спектрограммы на наличие таких признаков.
- Локализация местоположения возможно внедренного закладочного устройства, а также признаков его функционирования
- Осуществляется с помощью вспомогательного оборудования, такого как нелинейные локаторы, имитаторы базовых станций, беспроводные пробники и различные измерители мощности сигнала. Выявление нахождение источника вредоносного сигнала.
- Изъятие закладочного устройства
- После определения типа устройства, определения его местоположения и прочих ТТХ характеристик, уведомляется уполномоченное руководство.

Литература

1. Доктрина информационной безопасности Российской Федерации (№ 646 от 05.12.2016 г.);
2. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации;

3. Федеральный закон "О персональных данных» от 27 июля 2006 года № 152-ФЗ;

4. Белый В.М. Эффективность информационных систем и информационных технологий: учебник / В.М. Белый, Р.В. Белый – Королев МО: ФТА.2013 г – 396 с.;

5. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ТИД Диа Софт, 2002 г.; - 671 с.

6. Хорев А.А. Теоретические основы оценки возможностей технических средств разведки Монография. – М.: МО РФ, 2000 г. – 255 с.;

7. Хорев А.А. Методы и средства поиска электронных устройств перехвата информации. - М.: МО РФ, 1998 г. – 224 с.;

8. Чухнов К. Особенности проектирования радиоканальных объектовых систем сигнализации. Технологии защиты, 2010, № 1;

9. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие. М.: Гостехкомиссия России, 1998. - 320 с.;

10. Статья Обзор современных технологий беспроводной передачи данных в частотных диапазонах ism (bluetooth, zigbee, wi-fi) и 434/868 мгц [Электронный ресурс]. – Режим доступа: https://wireless-e.ru/standarty/short-range-rf/ (дата обращения: 01.02.2022)

РАЗВИТИЕ ЧЕЛОВЕЧЕСКОГО РАЗУМА КАК КРИТЕРИЙ ПРОГРЕССА ЧЕЛОВЕЧЕСКОГО КАПИТАЛА

Гарник Елена Сергеевна, магистрант 2 курса кафедры управления
Научный руководитель: **Хорошавина Наталья Сергеевна**, к.э.н., доцент кафедры управления

Данная статья посвящена раскрытию взаимосвязи развития человеческого разума, как критерия прогресса человеческого капитала. Важную роль в жизни общества и государства играет образование. От уровня образования зависит уровень развития разума человека и его культуры, и, как следствие, уровень развития человеческого капитала страны. Это связано с быстрым и постоянным развитием технологий, которые требуют создания высококвалифицированных трудовых ресурсов, т.к. данные трудовые ресурсы должны справляться с усложняющимися задачами в экономике и на производстве, в том числе и при межнациональном общении. В первую очередь перед государством, обществом и образовательными учреждениями стоит задача в организации образовательного процесса именно таким способом, чтобы все его участники были заинтересованы в эффективном достижении поставленных целей и высоких результатов. Концепция человеческого капитала является одной из форм богатства общества, которое зависит от знаний, способностей, навыков и культуры человека, а также способностей его к созидательному труду и разработке новых технологий, при помощи человеческого разума. Сегодня становление человеческого капитала посредством развития человеческого разума является ключевым фактором цифровой трансформации экономики страны.

Человеческий капитал, человеческий разум, навыки, образование, экстремизм.

THE DEVELOPMENT OF THE HUMAN MIND AS A CRITERION FOR THE PROGRESS OF HUMAN CAPITAL

Garnik Elena, 2st year graduate student of the Department of Management
Scientific adviser: **Khoroshavina Natalia,** Candidate of Economic sciences, Associate professor of the Department of Management

This article is devoted to the disclosure of the relationship between the developments of the human mind as a criterion for the progress of human capital. Education plays an important role in the life of society and the state. The level of development of a person's mind and culture depends on the level of education, and, as a result, the level of development of the country's human capital. This is due to

the rapid and constant development of technologies that require the creation of highly qualified labor resources, because these labor resources must cope with increasingly complex tasks in the economy and in production, including interethnic communication. First, the state, society and educational institutions face the task of organizing the educational process in such a way that all its participants are interested in effectively achieving their goals and high results. The concept of human capital is one of the forms of the wealth of society, which depends on the knowledge, abilities, skills and culture of a person, as well as his abilities for creative work and the development of new technologies, with the help of the human mind. Today, the formation of human capital through the development of human intelligence is a key factor in the digital transformation of the country's economy.

Human capital, human intelligence, skills, education, extremism.

Прежде чем приступить к раскрытию основной темы данной статьи необходимо дать определение человеческому капиталу и разуму. Человеческий капитал – это совокупность навыков и знаний, которые будут использоваться человеком для удовлетворения его потребностей, а также потребностей общества [4]. Разум представляет собой одну из форм сознания или самосознающий рассудок, который направлен на самого себя, выраженный в идеях, принципах или идеалах [6].

Человеческий капитал оказывает непосредственное влияние на инновационную экономику, экономику знаний, что приводит к формированию этапа социально-экономического развития. Раскрываться человеческий капитал может различными способами, как при помощи воспитания, так и при помощи трудовых навыков или получения образования. В свою очередь затраты, связанные с получением знаний, выступают в качестве инвестиций с целью формирования капитала, при помощи которого в дальнейшем человек сможет регулярно получать прибыль в виде престижной и интересной работы, высокого заработка, либо повышения социального статуса в обществе и т.д. Через социальные институты проявляется роль человеческого капитала, что дает возможность проанализировать социальные параметры, а также изучить влияние социальных факторов на рыночную экономику [3, с.45]. Современная рыночная экономика невозможна без межнационального общения внутри нашей страны, что в свою очередь требует от человека наличия культурных навыков. Практика межнационального общения должна строиться на приверженности к общечеловеческим и национальным ценностям, что приводит к отсутствию националистических настроений и национальной замкнутости, составляющих основу такого проявления как экстремизм.

Термин «человеческий капитал» был использован впервые американским экономистом Тэодором Шульцем в 1961 году. В дальнейшем его последователи развили данную тему, описав методы, формы и другие

особенности развития человеческого капитала. В среднем процесс развития человеческого капитала составляет 15- 25 лет. Начинается он, как правило в 3-4 года. Возраст от 13 до 23 лет является наиболее активным периодом развития человеческого капитала. В данный период времени отмечается наибольшее развитие и усвоение профессиональных, творческих и общих навыков у человека. Следовательно, можно заметить, что чем выше уровень накопленных знаний и навыков, тем больше возможностей у человека повысить собственное благосостояние и в целом улучшить жизнь общества [9].

Т. Шульцом была разработана концепция человеческого капитала, включающая в себя последовательную цепочку:

1. Человеческий капитал является дополнительным источником дохода, получение которого возможно при помощи навыков, знаний или способностей человека.

2. Образование позволяет достичь экономического роста, поэтому его с полной уверенностью можно отнести к одной из форм капитала.

3. Капитал образования нельзя рассматривать отдельно от личности, поэтому он тесто связан с человеческим капиталом.

4. В последующий период времени образование выражается в виде капитала, который в дальнейшем выступает в качестве источников будущих заработков и иных благ.

5. Дополнительные вложения в образование в виде инвестиций приведут к увеличению качественных характеристик рабочей силы.

6. Инвестиции, вложенные в образование, в дальнейшем приводят к созданию прибавочного продукта.

Г.С. Беккер выделял три ключевые формы проявления человеческого капитала:

1. Общие знания. Данные знания человек приобретает внутри своей семьи, благодаря воспитанию и образованию в начальных учебных заведениях. В ходе этого доход, который в дальнейшем получит, человек от данных знаний будет принадлежать ему самому или его семье.

2. Специальные знания накапливаются человеком на протяжении его трудовой деятельности при выполнении им каких-либо функций на занимаемом рабочем месте. Поэтому инвесторами социальных знаний выступает как сам работник, так и предприятие, на котором он работает.

3. Прочие виды знаний. Данный вид знаний создается в результате умений и стремлений человека применять на практике информационные продукты и услуги для поиска новых и перспективных условий труда в качестве специалиста [1, с.125].

На сегодняшний день с точки зрения российской ментальности концепция человеческого капитала учитывает мировой эволюционный процесс развития данной области. В свою очередь человеческий капитал включает в себя определенный объем способностей, навыков и знаний

человека, представляющих собой не только экономическую, но и культурную ценность. Экономическая ценность выражается в качестве капитала, который в дальнейшем принесет определенные выгоды и доход. Культурная же ценность позволяет находить компромиссы, достигать соглашений, в том числе и путем проведения переговоров при выстраивании межнациональных связей, не допуская изменения социально-экономического строя в стране и снижения жизненного уровня населения, приводящего к проявлению экстремизма [10]. Отличительная особенность человеческого капитала от экономического заключается в том, что он напрямую зависит от личности своего носителя. В результате данной особенности человеческий капитал может увеличиться или уменьшиться, а причиной этому служит физический или моральный износ, либо сумма вложенных инвестиций.

Основополагающими параметрами инвестиций в человека выступает, профессиональная подготовка, образование, здравоохранение, а также рождение и воспитание детей. Полученная профессиональная подготовка и образование дает возможность развить в человеке дополнительные умения, навыки и знания, помимо тех, что он уже имеет, увеличивая объем человеческого капитала. Высокий показатель здравоохранения увеличивает продолжительность жизни среди населения. Следовательно, увеличивается объем человеческого капитала, а высокий уровень рождаемости и полноценное воспитание детей дает возможность продлить человеческий капитал в будущих поколениях [7].

В свою очередь, рассмотрим сущность человеческого разума и условия его развития. В первую очередь, разум необходимо рассматривать, как процесс или ступени развития: развитие отдельного человека, социальное развитие, глобальное развитие. Разум представляет собой результат объединения мозговой деятельности индивидов, с последующим совмещением опыта и знаний.

Разум – это этап развития жизни и развивающаяся система. Поэтому разум, как развивающаяся система очень многогранен. В силу того, что на сегодняшний день человечество находится на стадии «машинной» цивилизации, социальное развитие человеческого вида привело к замещению в развитии индивидуального разума на глобальные научно-технические знания. В ходе этого возможно формирование ноосферы на основе «машинного разума» с минимальным использованием человеческого разума [2, с. 78].

В ходе органической эволюции человек выступает главным итогом развития материи. Это подтверждается тем, что появление человека на планете Земля повлияло на образование абсолютно новой социальной формы движения материи, которой до этого периода времени не существовало. В качестве доказательства того, что данной материи не существовало ранее, является то, что только человек способен к познанию, самопознанию и

преобразованию окружающего его мира. На определенном этапе человек, без саморазвития, смог выполнить свою другую видовую задачу - создал социум.

Социум представляет собой единую систему наиболее высокого уровня, которая состоит из всего человечества и объединена информационными, экономическими и иными связями, развиваясь по своим собственным законам. Люди разумные настолько, насколько дает возможность их мозг, развитый собственными усилиями. Особенности человеческого мозга остаются неизменными уже на протяжении тысяч лет, и он ничем не отличается от мозга людей в эпоху рыцарей, императоров или в период правления фараонов, что говорит нам об уходящих корнями в вышеуказанные эпохи отношениях, формирующих, при прочих равных, идеологические и иные, религиозные и социальные, аспекты существования различных национальных групп внутри которых порой развиваются течения, направленные на идеологизацию превосходства по национальному, социальному и иным признакам, иными словами, приводящими к экстремизму.

На сегодняшний день люди, безусловно, имеют больше знаний, но это не значит, что у них стало больше разума. Нет сомнений, что человечество продолжит развитие по избранному технократическому пути, несмотря ни на что [5]. Безусловно, разум имеет наиболее широкое понятие, чем ум. Ум концентрируется на определенных умениях и контролировании своих чувств. Разум направлен на тренировку подсознания, формирование привычек и освоение навыков, т.е. осваивая новые привычки, происходит развитие подсознания и дальнейшее закладывание новых механизмов. Таким образом, ум направлен на совершение определенных усилий, а разум отвечает за прошлые навыки, опыт и копит определенный багаж. Развитие разума позволяет достигать поставленных целей [8]. И именно развитие разума человека и его культуры позволяет достичь целей по искоренению нарушений прав и свобод человека в зависимости от его расовой, национальной, религиозной или социальной принадлежности [10].

Можно увидеть чёткую взаимосвязь между развитием человеческого разума и человеческого капитала. В первую очередь это определяется тем, что развитие человеческого разума на подсознательном уровне нацелено на освоение и получение новых навыков, умений и достижении определенных целей. Получение новых навыков и умений достигается при помощи образования, что способствует развитию человеческого капитала.

Помимо этого, развитие разума происходит в результате полученного опыта человеком на протяжении всей его жизни. Степень развития разума формируется с учетом опыта. В свою очередь человек набирается опыта постепенно, т.е. вначале он получает опыт из своей семьи, выполняя поручения своих родителей. Затем человек получает определенный опыт в школе и других учебных заведениях, выполняя поставленные задачи педагогами. После этого получение опыта происходит на рабочем месте,

выполняя поручения коллег и руководства по работе. Таким образом, чем больше нагрузки берет на себя человек в течение жизни, тем больше развивается разум. В ходе этого увеличивается уровень ответственности, которая в свою очередь является инструментом развития разума человека. Чем больше на протяжении всей своей жизни человек развивает в себе ответственность за какие-либо действия, тем больше опыта он получает, а значит увеличиваются его знания и умения, его культура. Следовательно, прогресс человеческого капитала у человека с меньшей долей ответственности гораздо ниже. В данном случае можно проследить взаимосвязь развития разума человека с тремя ключевыми формами проявления человеческого капитала, сформулированными Г.С. Беккером, которые были рассмотрены ранее в данной статье.

В будущем стремление человечества направлено на создание системы, которая сможет объединится в самоуправляемый и саморазвивающийся глобальный «мозг», который будет в миллиард раз больше и мощнее человеческого, что автоматически должно привести к исчезновению радикальных проявлений неравенства по различным признакам, являющихся в настоящее время угрозой человечеству. В свою очередь данная система энергетически будет наиболее выгоднее и не будет направлена на разрушение своей среды обитания, а наоборот будет способствовать самовоспроизводству и бесконечной жизни. В ходе этого пути развития человечества идет активная фаза развития разума, что приведёт к новому прогрессу человеческого капитала. Для будущего страны развитие человеческого капитала играет огромную роль, т.к. оно определяется уровнем развития науки и образования. На сегодняшний день повышение качественных характеристик человеческого капитала является обязательным условием для достижения устойчивого экономического развития государства и его преимуществ на мировом рынке. Возможно, в будущем на планете появится новый вид человека, который будет создан не природой, а человеческим разумом.

Развитие человека является одним из элементов, демонстрирующих многообразие в развитии разума, как постоянно развивающейся системы. В силу этого разум, как и все что есть в мире, постоянно развивается согласно хода времени [5].

Литература

1. Беккер Г.С.Человеческое поведение: экономический подход. – М.: ГУ ВШЭ, 2003. – 672с.

2. Вернадский В.И. Биосфера и ноосфера. - М.: Рольф, 2002. - 576 с.

3. Петренко Т. Исследование человеческого капитала как фактора экономического роста / Петренко Татьяна, Ирина Егорова und Сергей Коваленок. - М.: LAP Lambert Academic Publishing, 2018. - 392 с.

4. Википедия Человеческий капитал – URL: https://ru.wikipedia.org/wiki / (дата обращения: 10.01.2022). – Режим доступа: свободный. – Текст: электронный.

5. Научная электронная библиотека – URL: https://monographies.ru/ru/book/section?id=1135 (дата обращения: 10.01.2022). – Режим доступа: свободный. – Текст: электронный.

6. Основы психологии: теория познания, теория реинкарнации – URL: https://galeevrk.ru/dusha-razum-soznanie-podsoznanie/ (дата обращения: 10.01.2022). – Режим доступа: свободный. – Текст: электронный.

7. Словарь.ru Человеческого капитала теория. – URL: http://tfile.ru/forum/viewtopic.php?t=161538 (дата обращения: 10.01.2022). – Режим доступа: свободный. – Текст: электронный.

8. Электронный журнал «ВикиЧтение» – URL: https://staff.wikireading.ru/25711 (дата обращения: 10.01.2022). – Режим доступа: свободный. – Текст: электронный.

9. Электронный журнал «Успешник» – URL:https://financial-helper.ru/global_economy/chelovecheskijj-kapital.html (дата обращения: 10.01.2022). – Режим доступа: свободный. – Текст: электронный.

10. Официальный сайт Мэра Москвы – URL: https://vost-degunino.mos.ru/social-services/extremism/ (дата обращения: 16.02.2022). – Режим доступа: свободный. – Текст: электронный.

ПУТИ РАЗВИТИЯ SIEM-СИСТЕМ В ОБЛАСТИ МОНИТОРИНГА ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ

Гришин Вячеслав Вадимович, магистрант 1 курса кафедры информационной безопасности
Научный руководитель: **Сухотерин Александр Иванович**, к.воен.н., доцент кафедры боевого применения автоматизированных систем управления ВВА им. Ю.А. Гагарина

В этой статье, будет представлен вашему вниманию анализ наиболее широко используемых систем безопасности информации и управления событиями, чтобы определить их ключевые особенности, преимущества, ограничения и способы улучшить их для корпоративных целей. Анализ текущих SIEM и фокус на их ограничения, чтобы предложить потенциальные улучшения, которые могут быть включены в текущие платформы SIEM в пользу предприятия, использующего SIEM.

Решения SIEM, улучшение SIEM, ограничения SIEM, инфраструктура предприятия.

WAYS OF DEVELOPMENT OF SIEM-SYSTEMS IN MONITORING THE ACTIVITIES OF THE ORGANIZATION

Grishin Vyacheslav, 1st year graduate student of the Department of Information security
Scientific adviser: **Sukhoterin Alexander**, Candidate of Military sciences, Associate professor of the Department of Combat Application of Automated Control Systems of Gagarin Air Force

In this paper, will be presented to your an examine of the most widely used security information and event management systems to identify their key features, benefits, limitations and the ways to improve those for enterprise purposes. Analysis of current SIEMs and focus on their limitations to suggest potential improvements that can be incorporated into current SIEM platforms to benefit the enterprise company that uses SIEM.

Enterprise infrastructures, SIEM solutions, SIEM improvement, SIEM limitations.

Введение

В последние дни риски кибербезопасности для инфраструктуры предприятий значительно возросли, в основном из-за активизации деятельности национальных государств и киберпреступников. Злоумышленники становятся все более настойчивыми и опасными, а их надлежащее и своевременное обнаружение превратилось в настоящую проблему.

Примеры текущих инцидентов кибербезопасности, затрагивающих корпоративную инфраструктуру, включают [2]:

— ransomware-атаки;

— вредоносные программы, влияющие на способность коммунальных служб вести бизнес и операции;

— фишинговые кампании, направленные на руководителей, помощников руководителей, инженеров SCADA, ИТ-администраторов или других привилегированных пользователей;

— компрометация деловой электронной почты, включая захват учетной записи или выдачу себя за руководителя; утечки и кражи данных;

— социальная инженерия для получения конфиденциальной информации от сотрудников.

Структура статьи: в разделе 2 представлены основные коммерческие SIEM-решения с открытым исходным кодом, доступные на рынке. Раздел 3 описывает текущее состояние SIEM, их основные характеристики. В разделе 4 проанализированы ограничения существующих SIEM и представлены потенциальные возможности для улучшения. В разделе 5 предложены потенциальные улучшения для следующего поколения SIEM.

SIEM решения

Системы управления информацией и событиями безопасности (SIEM) призваны помочь администраторам разрабатывать политики безопасности и управлять событиями из различных источников. В целом, простая SIEM состоит из отдельных блоков (например, устройство-источник, сбор журналов, нормализация парсинга, механизм правил, хранение журналов, мониторинг событий), которые могут работать независимо, но без их взаимодействия SIEM не будет функционировать должным образом. На рисунке 1 показаны наиболее известные SIEM-решения.

Рисунок 1 – Различные решения SIEM

Платформы SIEM обеспечивают анализ событий безопасности, генерируемых сетевыми устройствами и приложениями, в режиме реального времени. Несмотря на то, что новое поколение SIEM предоставляет возможности реагирования для автоматизации процесса выбора и развертывания контрмер, существующие системы реагирования выбирают и развертывают меры безопасности без проведения всестороннего анализа воздействия атак и сценариев реагирования [1].

Возможности и характеристики SIEM

В принципе, все SIEM обладают способностью собирать, хранить и коррелировать события, генерируемые управляемой инфраструктурой. В этом разделе приведен список характеристик, которые необходимо учитывать при анализе решений SIEM.

Какие возможности делают SIEM превосходным:

Обработка в реальном времени: эта характеристика рассматривает способность SIEM обрабатывать данные в реальном времени, которые постоянно меняются. Здесь оцениваются возможности контроля, мониторинга и конвейерной обработки в реальном времени, которые инструмент использует для предотвращения или реагирования на инциденты кибербезопасности, а также вычислительные возможности, которыми обладают SIEM для анализа миллионов событий в реальном времени. Все рассмотренные SIEM обладают расширенными возможностями обработки данных в режиме реального времени.

Правила корреляции: Успех обнаружения события системой SIEM зависит от эффективности ее правил корреляции. Хотя большинство SIEM имеют базовые правила корреляции, лишь немногие из них обладают надежными возможностями поиска и поддерживают языки обработки поиска для написания сложных поисковых запросов, которые можно использовать в данных SIEM.

Источники данных: Одной из наиболее важных характеристик SIEM-системы является ее способность собирать события из многочисленных и разрозненных источников данных в управляемой инфраструктуре. Большинство SIEM изначально поддерживают несколько типов источников данных, включая как поддерживаемые датчики, так и типы данных (например, данные об угрозах).

Аналитика данных: Новые версии ведущих SIEM поддерживают широкую интеграцию с детекторами аномалий на основе приложений и пользователей. Эти возможности включают анализ поведения сотрудников, сторонних поставщиков и других сотрудников организации. Для этого SIEM должна включать управление профилями пользователей/приложений и использование машинного обучения для обнаружения неправомерного поведения.

Объем данных: анализ больших объемов данных из различных источников важен для получения более глубокого понимания собранных

событий и обеспечения лучшего мониторинга. Однако хранение больших объемов, собранных данных в системе SIEM часто является дорогостоящим и непрактичным. Эта функция оценивает способность текущих систем поддерживать большие объемы данных для операций корреляции, индексирования и хранения.

Визуализация: одним из ключевых факторов, препятствующих анализу событий безопасности, является отсутствие поддержки соответствующих методов визуализации данных и слабая поддержка интерактивного изучения собранных данных. Поэтому важно понимать возможности анализируемых систем в плане создания новых методов визуализации данных и пользовательских информационных панелей. Производительность: эта характеристика оценивает производительность SIEM-решения с точки зрения вычислительной мощности, возможностей хранения данных (например, чтение/запись), обработки корреляции правил (например, мощный механизм корреляции), а также поиска, индексации и мониторинга данных.

Масштабируемость: Эта характеристика учитывает способность развертывания SIEM расти не только с точки зрения аппаратного обеспечения, но и с точки зрения количества событий безопасности, собираемых на границе инфраструктуры SIEM. Новая цифровая трансформация приводит к увеличению количества датчиков и устройств (например, серверов, агентов, узлов), подключенных к одной сети.

Сложность: SIEM печально известны тем, что их сложно внедрять и управлять ими. Однако важно понять, можно ли установить анализируемую систему для тестирования с минимальными или умеренными усилиями. Из восьми исследованных SIEM, ArcSight - инструмент с самой высокой сложностью в плане развертывания и управления, в то время как LogRhythm и Splunk считаются простыми и удобными в плане установки, развертывания и использования.

Хранение: учитывая, что SIEM обычно не хранят информацию более 90 дней, эта характеристика оценивает, как долго текущие технологии SIEM хранят данные в своих системах для дальнейшей обработки и проведения судебной экспертизы.

Безопасность: эта характеристика оценивает способность реализовать автоматизацию безопасности, а также встроенные возможности шифрования, присутствующие в SIEM, во время мониторинга, обнаружения, корреляции, анализа и представления результатов.

Возможности реагирования и отчетности: Эта характеристика рассматривает действия, поддерживаемые SIEM для реагирования на инциденты безопасности (включая возможности обмена и отчетности), и то, как такие действия передаются механизму корреляции.

Ограничения текущих SIEM

Хотя новое поколение SIEM предоставляет мощные возможности по корреляции, хранению, визуализации и производительности, а также

возможность автоматизировать процесс реагирования путем выбора и развертывания контрмер, существующие системы реагирования очень ограничены, а контрмеры выбираются и развертываются без проведения всестороннего анализа воздействия атак и сценариев реагирования. Кроме того, большинство SIEM поддерживают интеграцию новых коннекторов или анализаторов для сбора событий или данных, а также предоставляют API или RESTful интерфейсы для сбора событий в более позднее время. Эти механизмы позволяют создавать дополнения и расширения для существующих систем [6].

Основными ограничениями являются:

Базовые правила корреляции. Платформы SIEM обеспечивают анализ событий безопасности, генерируемых сетевыми устройствами и приложениями, в режиме реального времени. Эти системы собирают большие объемы информации из разнородных источников и обрабатывают ее на лету;

Базовые возможности хранения данных. В большинстве существующих решений SIEM, как только данные архивируются и удаляются из живой системы, они больше не используются SIEM. Кроме того, пользователь сам решает, как обращаться с архивными данными, где их хранить или переносить, что обычно делается вручную;

Зависимость от человека. Исследования в области технологий SIEM традиционно сосредоточены на предоставлении комплексной интерпретации угроз, в частности, для оценки их значимости и соответствующей приоритизации ответных мер.

Будущие SIEM должны будут использовать эти ограничения для улучшения качества событий, поступающих в систему (например, с помощью новых систем мониторинга или сбора внешних данных из открытых источников), используя пользовательские коннекторы и предоставляя новые инструменты визуализации путем сбора данных из хранилища данных SIEM.

Пути улучшения функционирования SIEM

Лучшим способом уменьшить влияние указанных ограничений SIEM является не только их смягчение, но и внедрение новых возможностей, таких как:

Факторы окружающей среды. Задачи SIEM будут продолжать развиваться, поскольку менеджерам по безопасности придется иметь дело с облачными сервисами, мобильными устройствами, Интернетом вещей и другими новыми технологиями, которые ИТ-отдел не всегда контролирует.

Усиление многообразия безопасности. SIEMS с технологиями, учитывающими разнообразие, является значительным улучшением по сравнению с текущими решениями. Особое внимание должно быть уделено измерению разнообразия, т.е. тому, насколько похожи или насколько отличаются друг от друга системы защиты безопасности, уязвимости, атаки и

т.д. [5]. Эти типы метрик разнообразия менее изучены в литературе, чем метрики для отдельных компонентов.

Возможности ИИ/МЛ. Чтобы улучшить возможности обнаружения, корреляции и реагирования, следующее поколение SIEM должно интегрировать технологии AI/ML в свои основные механизмы. Технологии ИИ в SIEM обеспечивают возможности прогнозирования, которые особенно полезны для анализа аномального поведения сетевого трафика, инструментов и пользователей.

Другие потенциальные улучшения Обзор существующих SIEM показал, что эти системы не предоставляют высокоуровневых показателей риска безопасности. Следующее поколение SIEM должно разрабатывать метрики, основанные на оценке риска, которые учитывают несколько уровней зависимостей, таких как хосты, приложения, промежуточное ПО и сервисы. Это позволит оценивать риск в различных операционных и функциональных областях. Метрики распространения и воздействия атак могут быть расширены для учета различных иерархических уровней операций. Хотя стоимостные метрики могут быть сложными для расчета из-за того, что предприятиям трудно оценить затраты на безопасность, возможным усовершенствованием является рассмотрение этой категории метрик с использованием высокоточной оценки затрат для определения приемлемых пороговых значений. Учитывая, что технологии 5G и/или IoT повлияют на текущие архитектуры SIEM из-за увеличения объема данных, которые необходимо обрабатывать, также необходимо создать иерархию SIEM и разработать механизмы совместной работы, чтобы помочь сообщать о соответствующих инцидентах безопасности и управлять ими. Например, в области 5G решение SIEM в настоящее время может охватывать анализ одного участка сети, однако в ближайшем будущем нам понадобятся механизмы взаимодействия между несколькими участками. Такой механизм может быть особенно полезен в архитектурах, где обнаружение должно осуществляться ближе к краю. Например, в сфере IoT большой интерес могут представлять многочисленные системы SIEM, работающие на разных уровнях (например, SIEM, развернутые в шлюзах). Эти SIEM должны быть более легкими и ориентированными на конкретную область, чем существующие решения [4]. Кроме того, ожидается, что интеграция SIEM с платформами расширенного обнаружения и реагирования (XDR) обеспечит ценность двумя различными, но взаимодополняющими способами:

— SIEM, которые сосредоточены на соблюдении нормативных требований и развиваются в более широкую платформу для борьбы с угрозами и операционными рисками;

— XDR, которая фокусируется на угрозах и обеспечивает платформу для более глубокого и узкого обнаружения угроз и реагирования на них.

Будущие SIEM должны будут определять метрики безопасности, учитывающие количественные и вероятностные методы для поддержки решений о том, как лучше сочетать многочисленные средства защиты в условиях угроз. Это включает в себя понимание того, как сильные и слабые стороны различных средств защиты складываются в общую силу системы. Сообщество безопасности признает, что разнообразие потенциально ценно [7]. В литературе упоминается использование ансамблевых методов для оценки результатов систем классификации безопасности; однако SIEM должны ориентироваться на разнообразные входные данные, а не на агрегирование различных методов машинного обучения.

В результате предприятиям необходимы решения, предоставляющие подробную информацию о сетевой и/или пользовательской активности в облаке или на территории предприятия для более точного обнаружения угроз. Учитывая, что для развертывания SIEM обычно требуются операторы SOC и что современные инфраструктуры более разнообразны и динамичны, следующее поколение SIEM должно быть нацелено на обеспечение большей автономности и меньших накладных расходов на развертывание и управление, что, в свою очередь, позволит снизить затраты за счет упрощения использования и эксплуатации.

Выводы

В данной статье представлен коммерческий и технический анализ общего вида ведущих SIEM-решений на рынке, а именно SearchInform, MaxPotrol, LogRhythm, Splunk. С точки зрения поведенческого анализа, анализа рисков и развертывания, существует необходимость в разработке методов и инструментов для анализа, оценки и контроля оптимального использования различных механизмов безопасности в инфраструктуре предприятия. Хотя большинство проанализированных решений предоставляют удобные графические интерфейсы, возможности визуализации и реагирования ограничены для работы с большим количеством собранных событий [3]. Поэтому важно разработать расширения для визуализации и анализа, обеспечивающие пользователям лучшее понимание ситуации и более эффективные возможности принятия решений и реагирования. Что касается хранения данных и цены, то, хотя большинство рассмотренных решений имеют хорошие возможности хранения данных, они ограничены доступностью оборудования и обычно требуют приобретения дополнительных продуктов (и лицензий в зависимости от объема данных), что увеличивает цену.

Наконец, была изучена роль SIEM в ближайшем и долгосрочном будущем для инфраструктуры предприятия с учетом различных аспектов. Из этого анализа можно сделать вывод, что созданы хорошие условия для стимулирования инвестиций в совершенствование и расширение этой технологии как ключевого компонента не только для промышленных систем управления с центрами безопасности, но и для обеспечения управления

кибербезопасностью для малых и средних предприятий с низким уровнем знаний и возможностей в области безопасности.

Литература

1. Elshoush H.T., Osman I.M. Alert correlation in collaborative intelligent intrusion detection systems — A survey // Applied Soft Computing. 2011.

2. Dadkhah S., Shoja M.R.K., Taheri H. Alert Correlation through a Multi Components Architecture // International Journal of Electrical and Computer Engineering (IJECE). 2013.

3. Filkins B. An Evaluator's Guide to NextGen SIEM. [(accessed on 14 February 2022)];2018 SANS White Paper. Available online: https://gallery.logrhythm.com/independent-white-papers/sans-an-evaluators-guide-to-next-gen-siem-independent-white-paper-2018.pdf

4. Scarfone K. Comparing the Best SIEM Systems on the Market. [(accessed on 24 February 2022)]; Online Research. Available online: http://searchsecurity.techtarget.com/feature/Comparing-the-best-SIEM-systems-on-the-market.

5. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 1. // Труды СПИИРАН. 2016. Вып. 47. С. 5-27.

6. Splunk 7 SIEM Trends to Watch in 2019. [(accessed on 5 March 2022)]; Report. Available online: http://www.locuz.com/in/wp-content/uploads/2018/01/7-siem-trends-to-watch-in-2019.pdf.

7. Splunk Top 5 SIEM Trends to Watch in 2021. [(accessed on 19 March 2022)];2018 Technical Report. Available online: https://f.hubspotusercontent30.net/hubfs/8156085/Splunk.%20Top%205%20SIEM%20trends%20to%20Watch%20in%202021.pdf.

СТАНДАРТЫ, РЕГЛАМЕНТИРУЮЩИЕ ОБРАЩЕНИЕ ПРОГРАММНЫХ СРЕДСТВ В РАКЕТНО-КОСМИЧЕСКОЙ ОТРАСЛИ: СОСТОЯНИЕ, ПРОБЛЕМЫ, ПЕРСПЕКТИВЫ

Гусева Мария Александровна, магистрант 1 курса кафедры управления качеством и стандартизации
Научный руководитель: **Привалов Виктор Иванович**, к.т.н., с.н.с., доцент кафедры управления качеством и стандартизации

Динамичное развитие ракетно-космической отрасли по всей России, усиливает конкуренцию за счет увеличения, как количества предпринимателей, так и ассортимента товаров и услуг. Масштабный прогресс современных IT-технологий сказывается и на космических отраслях, что приводит к обновленной, более мощной аппаратуре, что ведет за собой обновление стандартов, регламентирующих обращение программных средств в ракетно-космической отрасли. В настоящее время процесс развития и постоянной модернизации этого нового направления представляет научный и практический интерес.

Ракетно-космическая отрасль, стандарты, программные средства, развитие ракетно-космической отрасли.

STANDARDS REGULATING THE CIRCULATION OF SOFTWARE IN THE ROCKET AND SPACE INDUSTRY: STATE, PROBLEMS, PROSPECTS

Guseva Mariya, 1st year graduate student of the Department of Quality management and standardization
Scientific adviser: **Privalov Viktor**, Candidate of Technical sciences, Senior researcher, Associate professor of the Department of Quality management and standardization

The dynamic development of the rocket and space industry throughout Russia increases competition by increasing both the number of entrepreneurs and the range of goods and services. The large-scale progress of modern IT technologies also affects the space industries, which leads to updated, more powerful equipment, which leads to the updating of standards regulating the circulation of software in the rocket and space industry. Currently, the process of development and continuous modernization of this new direction is of scientific and practical interest.

Rocket and space industry, standards, software, development of the rocket and space industry.

Стандарты, регламентирующие обращение программных средств в ракетно-космической отрасли, объединяются в отраслевом фонде алгоритмов и программ. Отраслевой фонд алгоритмов и программ был создан в 1976 году постановлением Госкомитета по науке и технике Совета Министров СССР и приказом Министерства общего машиностроения.

Фонд позволил существенно ускорить внедрение информационных технологий в РКП. На внедрение программных средств ежегодно до 1991 года представлялось до 600 программных средств.

Главными целями фонда является информационное, нормативно-методическое и организационное обеспечение работ, направленных на повышение эффективности создания и использования прикладного и общесистемного программного обеспечения, используемого в процессе создания, изготовления, внедрения и эксплуатации наукоемких изделий ракетно-космической техники.

Наличие значительного задела и определенного «запаса прочности» ракетно-космической отрасли (РКО) России обуславливали, до последнего времени, отсутствие потрясений катастрофического характера в состоянии отечественной космической деятельности, которые стали бы для руководства страны свидетельством необходимости кардинальных реформ. Факт результативного сравнительно функционирования данной промышленной отрасли в конце XX – начале XXI века отсрочил проведение необходимых институциональных преобразований. Однако глубинные процессы, проходящие в РКО, делают задачу институциональной модернизации неотложной [1].

Важным фактом стало то, что за последнее десятилетие несмотря на сохранение основного потенциала, основное производство ракетно-космической отрасли России, превратилось из серийного в мелкосерийное, при сохранении в целом существовавшей ранее организационно-технологической структуры [3].

На сегодняшний день функционирование фонда алгоритмов и программ ракетно-космической промышленности (ФАП РКТ) регламентируется отраслевыми стандартами, разработанными около 40 лет назад. С учетом изменения законодательства, технологий программирования, смены парка вычислительных средств, машинных носителей информации до настоящего момента отраслевые стандарты не корректировались. Частные инструкции, основанные на базе этих стандартов, также устарели и требуется их переработка [1]. В результате вопросы взаимодействия фонда с разработчиками ПС и пользователями не урегулированы.

С момента распада СССР прямое финансирование фонда не ведется. Все нормативные документы (Положение, отраслевые стандарты и др.) морально устарели и не соответствуют ни современному научно-техническому уровню, ни действующему законодательству. На данный момент однозначно не определен и не отлажен порядок взаимодействия

фонда с предприятиями при передаче прав на использование программных средств [2]. В результате обычные операции по комплектованию фонда и использованию его материалов оказались чрезвычайно затруднены.

Часть стандартов могут быть поглощены переработанным стандартом и аннулированы без замены.

Остальные стандарты призваны регулировать важнейшие направления деятельности фонда. Они должны быть переработаны и поддерживаться в актуальном состоянии. Корректировка имеющихся стандартов должна производиться с учетом наработанного в фонде и зарубежного опыта (стандарты DOD-STD-2167A, MIL-STD-498 и руководство по его применению).

В последние годы появились нормативные документы федерального уровня (например, Постановление Правительства РФ от 22 марта 2012 № 233), позволяющие урегулировать порядок взаимодействия фонда и предприятий по вопросам разработки, хранения и использования РИД и РНТД. С учетом этих документов необходимо доработать стандарты.

Необходимость и полезность доработки отраслевых стандартов объясняется тем, что, в отличие от «Положения», спускаемого «сверху», они проходят согласование с заинтересованными специалистами предприятий отрасли. Это позволит, в частности, выявить неясные, спорные моменты и трудновыполнимые требования современных нормативных документов, выработать коллективные рекомендации по их преодолению.

На предприятиях РКП были разработаны и внедрены отраслевые стандарты по оформлению программной документации. Перечень этих стандартов вместе с ГОСТ ЕСПД.

Оценка качества программного средства проводится в соответствии с требованиями стандартов ГОСТ 34. 603-92 «Информационная технология. Виды испытаний автоматизированных систем», ГОСТ 28195-89 «Оценка качества программного средства. Общие положения», ГОСТ Р ИСО/МЭК 9126-93 «Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению» и ГОСТ Р ИСО/МЭК 12119-2000 «Информационная технология. Пакеты программ. Требования к качеству и тестированию».

Состав отраслевых стандартов по ФАП РКТ в настоящее время явно недостаточен и должен быть дополнен документами, появление которых обусловлено особенностями взаимодействия между Роскосмосом, предприятиями, холдингами, авторами программ, в том числе при использовании электронной почты, электронного документооборота и др. Одним из основных требований к ПС должна быть их информационная безопасность [3] (обеспечение целостности, электронно-цифровой подписи).

Разработка новых и переработка имеющихся нормативных документов должна производиться с учетом опыта, наработанного в ФАП, и зарубежного опыта.

По инициативе отдельных организаций была проведена процедура оценки действующих стандартов, регламентирующие обращение программных средств в ракетно-космической отрасли на соответствие современному техническому уровню.

Была проведена проверка нормативной документации (НД), на соответствие современному техническому уровню с соблюдением требований СТП 851-107-2008 и СТП 851-141-2007 следующих НД, регламентирующих деятельность ФАП РКТ:

По стандартизации были разосланы письма предприятиям отрасли просьбой рассмотреть целесообразность применения действующих НД соответствии со следующими пунктами:

- дальнейшего применения без изменения (с изменением);
- ограничения (снятия ограничения) области распространения,
- срока действия; пересмотра (разработка НД взамен действующего стандарта);
- отмены;
- изменения, пересмотра, ограничения области распространения отмены взаимосвязанных НД (с выдачей конкретных предложений).

В результате были получены рекомендации и предложение по совершенствованию от 32 предприятий. Анализ отзывов предприятий по оценке нормативной документации (НД), показал регламентирующей функционирование ФАП РКТ, разработанные с 1979 по 1991 годы, в результате которого установлено, что применяемые НД не соответствуют современному техническому уровню (ТУ) программных продуктов, экономики, национальной стандартизации и требуют существенной переработки с учетом смены парка вычислительных средств, технологий программирования, машинных носителей информации, что в свою очередь подлежат переработке.

В процессе исследований так же проведен анализ, который показывает, что за последние годы, существенно поменялся подход к решению задач проектирования. Высокий уровень использования коммерческих пакетов, отечественные программные комплексы, удаленный, распределенный доступ к ресурсам супер ЭВМ и т.д., безусловно, требуют другого подхода к НД.

Большинство прикладных программ, разрабатываемых авторами как «побочный продукт» при проведении НИОКР, не документируются (или документируются в произвольной форме) и не регистрируются, хотя программы относятся к научно-технической продукции и подлежат передаче заказчику. Когда речь идет об управляющих программах, ситуация усложняется, которые функционируют в режиме реального времени и, от правильного функционирования которых напрямую зависит реализация важнейших миссий, безопасность, а иногда - человеческие жизни. К надежности подобного ПО, предъявляются очень высокие требования.

Ошибки в программах, к сожалению, приводили и приводят к катастрофическим последствиям [7].

Основными причинами того, что авторы программных средств не оформляют программную документацию для ее регистрации в ФАП РКТ, являются боязнь «отчуждения» интеллектуальной собственности, а также отсутствие какой-либо заинтересованности.

Одним из возможных выходов из такого положения является разработка организационных и нормативно-технических документов, регламентирующих разработку, сертификацию, сдачу программных средств в ФАП и их тиражирование по заявкам предприятий РКП. Данные НД должны учитывать:

- большое разнообразие современных программно-технических средств;
- различные формы отношений между заказчиком, разработчиком и пользователем программного обеспечения;
- накопленный опыт как в стране, так и за рубежом.

Переработка указанных НД будет проводиться с целью обеспечения единого методического подхода и унификации деятельности предприятий отрасли в области проектирования, разработки и постановки на производство изделий космической техники и актуализации НД по методическим подходам и программной документации с учетом замечаний и предложений предприятий, полученных на основании проверки НД на соответствие современному техническому уровню. Внедрение в жизнь перечисленных мер возможно путем разработки и внедрения на предприятиях специализированных методик спецификации, проектирования, разработки и программного обеспечения, поддерживаемых специализированными инструментальными программными средствами. Набор подобных средств индивидуально подбирается на каждом предприятии в зависимости от специфики изготавливаемых изделий [6].

12 марта 2021 года «Роскосмос» объявил об утверждении серии стандартов, регламентирующих работу с электронной технической документацией. Благодаря этой инициативе госкорпорация намерена перевести проектирование перспективных ракетно-космических комплексов полностью в цифровой вид, а также обеспечить создание их цифровых двойников.

«Внедрение данного комплекса стандартов формирует единые требования к проектированию продукции «Роскосмоса», но и для всей нашей кооперации, а это более тысячи организаций. Это создаст надежный фундамент для цифровизации всей отрасли, — отметил директор департамента сертификации, стандартизации и лицензирования «Роскосмоса» Геннадий Абраменков» [5].

Как пояснил директор департамента цифрового развития «Роскосмоса» Константин Шадрин, стандарты определяют унификацию продукции, в том

числе внутри информационных систем, поэтому принятие данных стандартов должно послужить основой для использования единых решений и методик при оформлении электронной технической документации.

По словам Шадрина, утверждение серии стандартов, устанавливающих единые требования к процессу разработки ракетно-космической техники в электронном виде, подвело итог дискуссиям, которые долгое время велись на различных площадках, касаемо корректного представления разрабатываемой электронной документации [8].

При переработке «Основных положений об отраслевом фонде» должно быть четко указано, какие алгоритмы и программы могут быть включены в отраслевой фонд. Принятые в отраслевой фонд алгоритмы и программы должны получать статус государственной регистрации интеллектуальной собственности предприятия-разработчика, а авторы - Свидетельство о регистрации.

Нормативные документы должны разрабатываться в соответствии с требованиями ГОСТ ЕСПД, ОСТ и т.д. За основу можно принять современные действующие стандарты.

Вместе с разработкой проекта новой редакции «Положение о фонде алгоритмов и программ» нормативные документы, регламентирующие функционирование ФАП РКТ, также требуют существенной переработки.

По мнению специалистов, необходимо разработать и принять, по крайней мере, в отрасли комплект стандартов по проектированию, разработке и отработке программного обеспечения по видам (типам) программ: операционные системы, прикладные программы, инструментальные системы поддержки разработки ПО, математическое моделирование и т.д.

За основу можно принять современные действующие стандарты (например, ГОСТ Р ИСО/МЭК 12207-99 «Информационная технология. Процессы жизненного цикла программных средств», ГОСТ Р 51189-98 «Средства программных систем вооружения. Порядок разработки», ГОСТ РВ 51718-2001 «Программное изделие. Общие технические требования».

Таким образом исследование вопроса состояний фонда показывает, что назрела насущная проблема переработки в соответствии с современной базой НД по стандартам, регламентирующие обращение программных средств в ракетно-космической отрасли, подходу к решению задач проектирования.

По мнению специалистов, часть стандартов могут быть поглощены переработанным стандартом и аннулированы без замены.

Разработка организационных и нормативно-технических документов, регламентирующих разработку, сертификацию, сдачу программных средств в ФАП и их тиражирование по заявкам предприятий РКП, должны учитывать выше перечисленные требования, что повлияет на работу авторов программных средств, которые в свою очередь будут оформляют программную документацию для регистрации в ФАП РКТ.

Литература

1. ГОСТ 28195-89 Межгосударственный стандарт. Оценка качества. Программных средств. Общие положения. Ипк издательство стандартов. Москва

2. Сибирский государственный университет путей сообщения. Наука и молодежь XXI века. Материалы XIII научно-технической конференции студентов и аспирантов 13–14 ноября 2014 г. Часть I. Технические науки. Новосибирск 2015.

3. Воронцова, Елена Петровна. Организация государственного финансового контроля в России: диссертация ... кандидата социологических наук : 22.00.08 / Воронцова Елена Петровна; [Место защиты: Юж. федер. ун-т].- Ростов-на-Дону, 2011.- 186 с.: ил. РГБ ОД, 61 12-22/69

4. Роскосмос / под общей ред. А.Н. Перминева. – М.: Реетер, 2007 – 240 с.

5. «Роскосмос» переводит проектирование ракетно-космических комплексов полностью в цифровой вид | Hi-Tech | Селдон Новости https://news.myseldon.com/ru/news/index/247134604 (дата обращения: 10.03.2022)

6. Компания:Российские_космические_системы_(РКС) ОАО «Российские космические системы» https://www.tadviser.ru/index.php/ (дата обращения: 10.03.2022)

7. Об актуальных проблемах ракетно-космической отрасли России https://scienceproblems.ru/ob-aktualnyh-problemah-raketno-kosmicheskoj-otrasli-rossii.html (дата обращения: 10.03.2022)

ВЗАИМОДЕЙСТВИЕ ТРЁХ УРОВНЕЙ ОБРАЗОВАНИЯ НА ПРИМЕРЕ ОБЩЕГО ПРОЕКТА

Гусятинер Леонид Борисович, магистрант 2 курса кафедры математики и естественнонаучных дисциплин
Научный руководитель: **Вилисов Валерий Яковлевич,** д.э.н., к.т.н., профессор кафедры математики и естественнонаучных дисциплин

В данной статье предлагается метод организации совместной работы студентов магистратуры, бакалавриата и колледжа. Приводится описание совместного проекта.

Python, PyQt5, lxml, matplotlib, openpyxl, pandas, requests, sqlite3, проект, сайт.

INTERACTION OF THREE LEVELS OF EDUCATION ON THE EXAMPLE OF A SHARED PROJECT

Leonid Gusyatiner, 2nd year graduate student of the Department of Mathematics and natural sciences
Scientific adviser: **Vilisov Valery**, Doctor of Economic sciences, Candidate of Technical sciences, Professor of the Department of Mathematics and natural sciences

This article describes a possible approach to the creation of programs - "teaching assistants", on the example of four projects.

Lazarus, Python, PyQT5, matplotlib, Selenium, SQLite, portal.

Важной задачей кафедры является привлечение талантливых абитуриентов для продолжения обучения.

Участие в совместной научной и проектной деятельности является проверенным подходом для решения этой задачи. Уверенность в успехе основывается на том, что колледж, бакалавриат и магистратура являются подразделениями единого Технологического университета. В литературе, например, [1] предлагается адаптация учебных планов СПО и бакалавриата, принимая априори, что профессиональный уровень студентов СПО ниже. В данной статье предполагается, что студенты колледжа изучают несколько другую профессию, то есть они могут быть равными участниками проекта. Новое заключается в том, что проект организуется именно в в рамках учебных занятий.

Автору было поручено преподавание дисциплины «Технологии и системы коллективной разработки программ» в группе ПМИ-18 бакалавриата. Для выполнения практических занятий группа была разбита на

бригады от двух до четырех студентов. Каждая подгруппа выбрала проект для коллективной разработки.

Бригада в составе Баранникова Д.В., Лямина М.Е., Мамедовой Е.Е. разработала проект «Сбор и анализ данных новостного источника RIA» [2].

Роли в бригаде распределились так: Мамедова Е.Е. - менеджер, Лямин М.Е. - главный программист, Баранников Д.В. - программист.

В результате была создан однофайловый консольный проект на языке Python с использованием библиотек lxml, openpyxl, pandas, requests. Данные выводятся в xls-файл и строятся сравнительные диаграммы числа просмотров по разным категориям (рисунок 1.1–1.2).

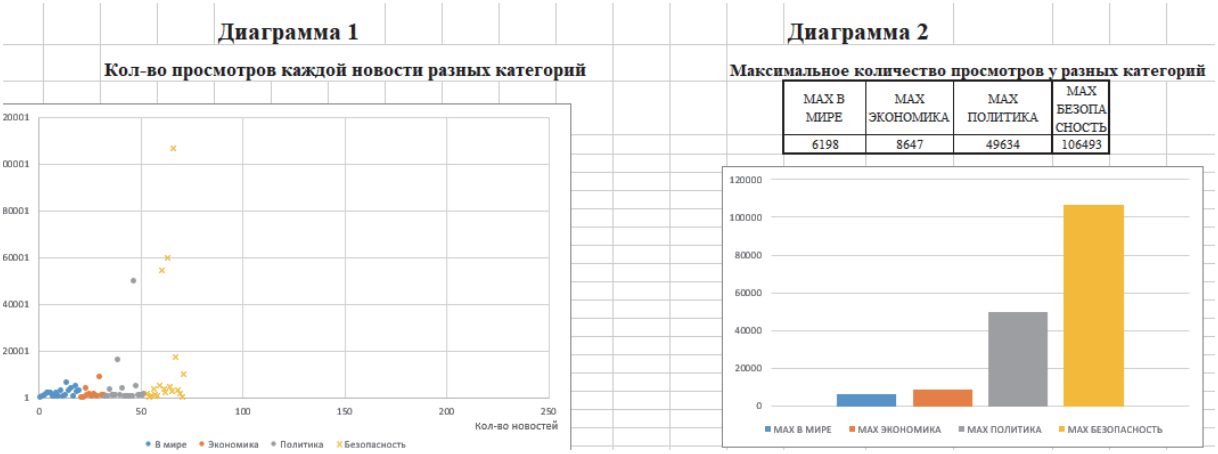


Рисунок 1.1 – Просмотры новостей по категориям

Рисунок 1.2 – Сценарий работы программы (начальная постановка задачи)

При защите проекта на кафедре математики и естественнонаучных дисциплин были указаны пути доработки, в том числе, подключение базы данных, улучшение интерфейса.

Для этого на втором этапе [2] был подключён в рамках производственной практики ПП.01 студент группы П2-19 ККМТ Шакиров Е.К., специализирующийся на разработке визуальных приложений.

Проект становится многофайловым (рисунок 2.1), с графическим интерфейсом. Интерфейс отображает полученные данные в виде таблицы

(рисунок 2.2) и двух графиков (рисунок 2.3–2.4). Добавляется использование библиотек matplotlib, PyQt5.

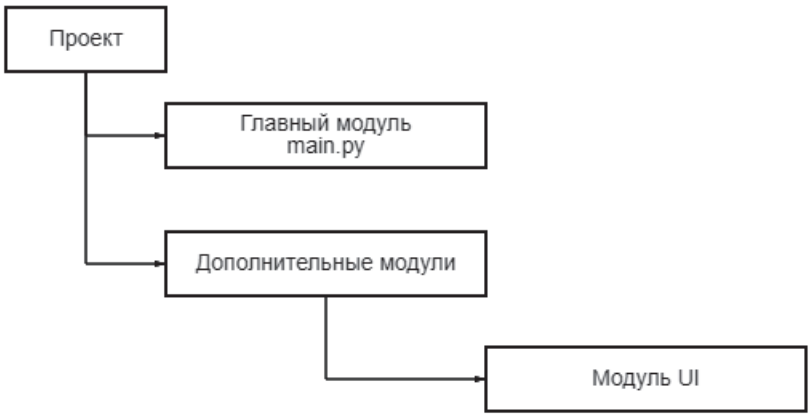
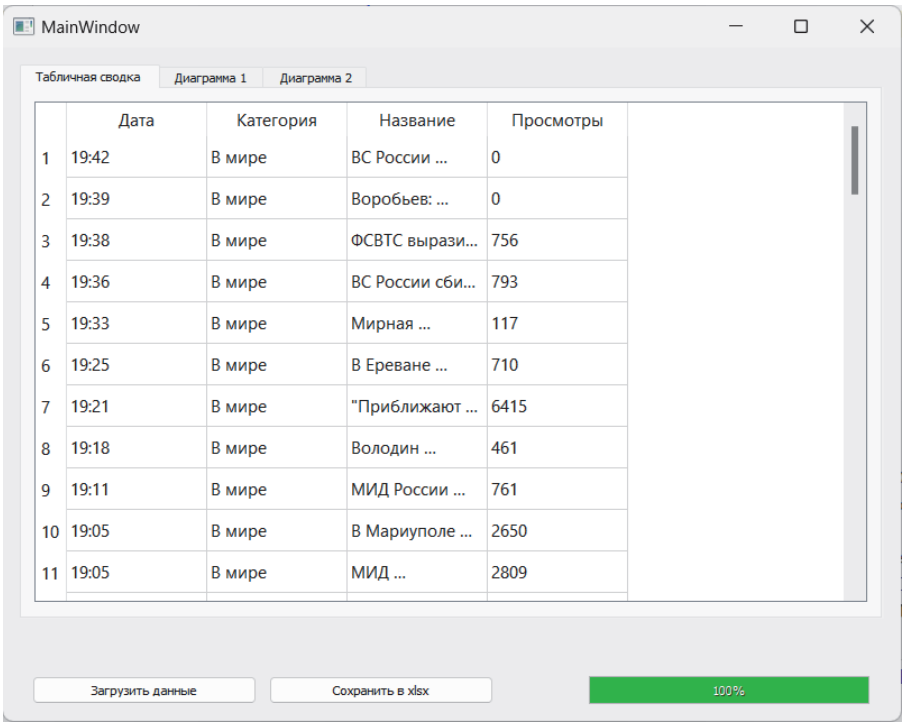


Рисунок 2.1 – Структура проекта на втором этапе



	Дата	Категория	Название	Просмотры
1	19:42	В мире	ВС России ...	0
2	19:39	В мире	Воробьев: ...	0
3	19:38	В мире	ФСВТС вырази...	756
4	19:36	В мире	ВС России сби...	793
5	19:33	В мире	Мирная ...	117
6	19:25	В мире	В Ереване ...	710
7	19:21	В мире	"Приближают ...	6415
8	19:18	В мире	Володин ...	461
9	19:11	В мире	МИД России ...	761
10	19:05	В мире	В Мариуполе ...	2650
11	19:05	В мире	МИД ...	2809

Рисунок 2.2 – Табличная сводка данных

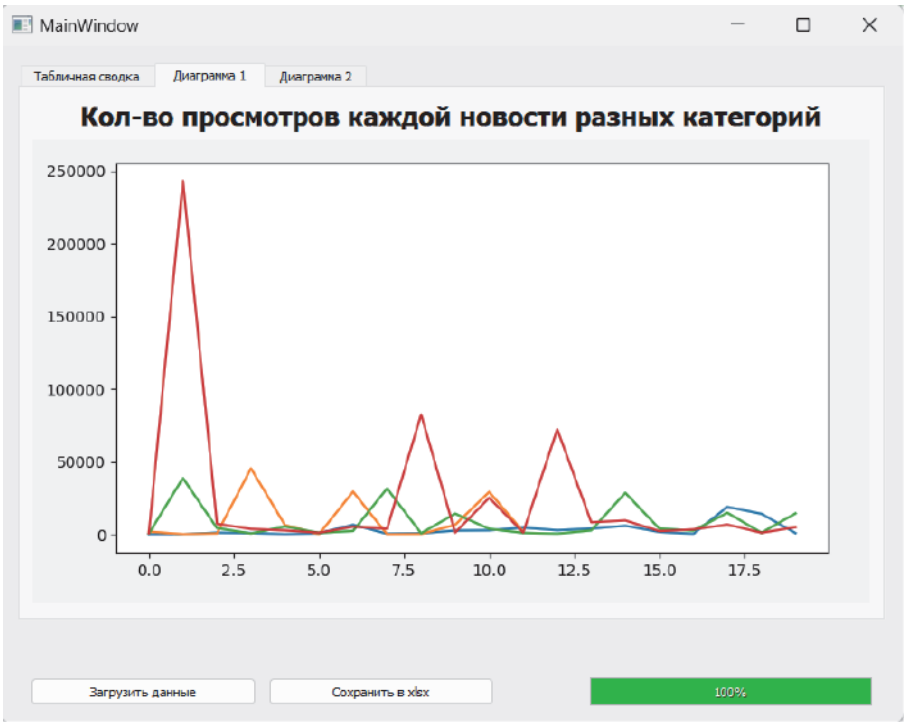


Рисунок 2.3 – Просмотры новостей разных категорий

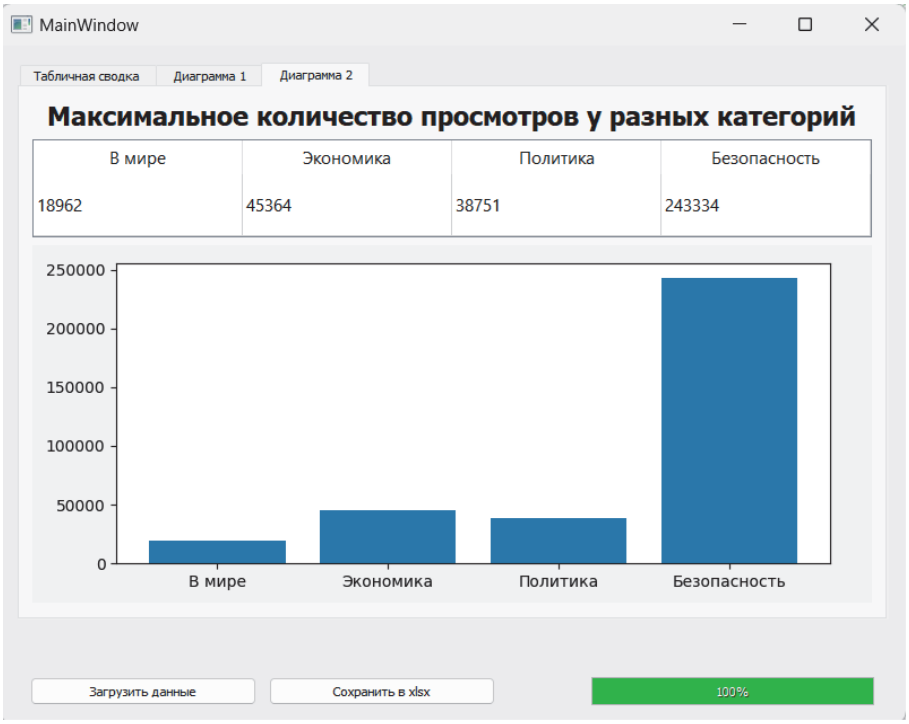


Рисунок 2.4 – Максимальное количество просмотров по категориям

Наконец, на третьем этапе [3] к разработчикам присоединяется студент группы П2-19 ККМТ Ковалев А.Г. для выгрузки данных в базу (рис.3). В проект добавляется новый модуль. Структура и алгоритм проекта принимает окончательный вид (рисунок 4–5).

Таким образом, от первой версии до третьей значительно усилен функционал (таблица 1).

```
SELECT * FROM rbk
```

id	date	class	name	views
30	04:20	Экономика	Эксперт рассказал о перспективах евро ...	28576
31	02:15	Экономика	Специалист рассказал о факторах, опре...	8286
32	02:15	Экономика	"Углю повезло": эксперт рассказал, что п...	23346
33	11:50	Политика	Песков рассказал об уникальных отноше...	7272
34	08:43	Политика	Матвиенко назвала День единения наро...	2029
35	08:00	Политика	Ставка Макрона на Украину провалилась	29669
36	20:34	Политика	Макеева: западные страны Украине "пом...	2759
37	18:32	Политика	Мария Бутина: у Байдена что-то идет не ...	3392

Рисунок 3 – Результат выполнения запроса к базе данных (этап 3)

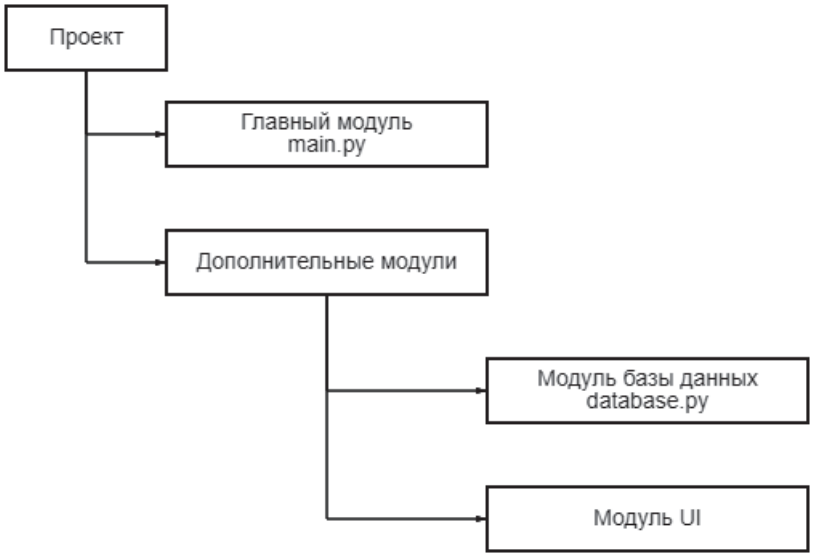


Рисунок 4 – Структура итогового проекта

Рисунок 5 – Сценарий работы итоговой программы

Таблица 1 – Сравнение функционала версий программы

Функционал	Первая версия проекта, консольное приложение	Итоговая версия проекта, программа с интерфейсом
Вывод данных в xlsx файл	Присутствует	Присутствует
Отображение данных в программе	Отсутствует	Присутствует (таблица данных, 2 графика)
Наличие графического интерфейса	Отсутствует	Присутствует
Наличие возможности вывода данных в базу данных	Отсутствует	Присутствует
Обработка ошибок в результате выполнения программы	Отсутствует	Присутствует

Данный проект можно было бы изначально организовать так:

1. Преподаватель кафедры знает постановки задач в сфере своих научных интересов.

2. Магистрант-постановщик может сформулировать эти задачи для реализации.

3. Студент-математик бакалавриата умеет применить статистические методы и разработать прототип.

4. Студент-программист колледжа может по прототипу построить качественное приложение.

Данный метод можно использовать, например, в рамках учебной (ознакомительной) практики магистрантов первого года обучения.

При этом повышается качество проекта, так как включаются разработчики разных специальностей менеджер проекта, математик-постановщик, программист.

Появляется заинтересованность студентов младших уровней обучения в продолжение образования на нашей специальности.

Литература

1. Самохина, В. М. Технологии реализации преемственности в системе СПО-ВУЗ / В. М. Самохина. — Текст : непосредственный // Молодой ученый. — 2016. — № 24 (128). — С. 511-512. — Режим доступа: https://moluch.ru/archive/128/35539/ (дата обращения: 17.04.2022).

2. Контрольная Мамедовой [Электронный ресурс] Режим доступа: https://github.com/Dmitry2602/parser_kkmt.git/ (дата обращения 17.04.2022).

3. Проект Шакирова-1 [Электронный ресурс] Режим доступа: https://github.com/Dmitry2602/parser_kkmt.git/ (дата обращения 17.04.2022).

4. Проект Шакирова-2 [Электронный ресурс] Режим доступа: https://github.com/Dmitry2602/parser_kkmt.git/ (дата обращения 17.04.2022).

ПОЧЕМУ НУЖНО ОБРАТИТЬ ВНИМАНИЕ НА «ЛОЯЛЬНОСТЬ» ПЕРСОНАЛА

Дубицкий Денис Русланович, магистрант 1 курса кафедры информационной безопасности
Научный руководитель: **Сухотерин Александр Иванович**, к.воен.н., доцент кафедры боевого применения автоматизированных систем управления ВВА им. Ю.А. Гагарина.

Данная статья направлена на привлечение внимания к такому важному каналу утечки информации, как социальная инженерия. А также, содержит мнение, которое может пролить свет на эту проблему и помочь усовершенствовать систему защиты вашей организации, путем внедрения методов ранжирования персонала и использования специальных систем видеонаблюдения с внедренным искусственным интеллектом для анализа действий персонала.

Информационная безопасность, социальная инженерия, «лояльность» персонала.

WHY WE NEED TO PAY ATTENTION TO THE "LOYALTY" OF STAFF

Dubitskiy Denis, 1st year graduate student of the Department of Information security
Scientific adviser: **Sukhoterin Alexander**, Candidate of Technical sciences, Associate professor of the Department of Combat Application of Automated Control Systems of Gagarin Air Force

This article aims to draw attention to such an important channel of information leakage as social engineering. And also, contains an opinion that can shed light on this problem and help improve the protection system of your organization, by implementing methods of personnel ranking and using special video surveillance systems with implemented artificial intelligence to analyze the actions of personnel.

Information security, social engineering, "loyalty" of personnel.

За период своей шестилетней работы в области информационной безопасности, занимаясь обследованием информационных систем, проектированием, созданием, внедрением систем защиты информации, аттестацией объектов информатизации, а также аудитом информационной безопасности, нередко встречались ситуации, в которых руководство компании, выделяло значительные средства на создание систем защиты

информации от утечек по техническим каналам и организацию физической защиты предприятия, но в тоже время игнорировало важность работы с персоналом. Зачастую, именно это и приводило к утечке защищаемой информации, и как следствие к финансовым убыткам. Ежегодно объем обрабатываемых данных растёт, следовательно, растёт и количество вероятных угроз. Таким образом, любая компрометация данных, может повлечь существенные финансовые потери.

В современном мире существует большое множество угроз информационной безопасности и целостности данных. Злоумышленники постоянно меняют методы и средства с помощью которых они бы могли заполучить необходимые данные. Поэтому, механизмы их воздействия — это уже не только удалённые атаки на определенные ресурсы, а вдобавок к этому, активное использование методов социальной инженерии. На данном этапе становления и развития общества информация становится одним из ключевых условий и ресурсов для развития предприятия, региона и государства в целом, а главной задачей – обеспечение информационной безопасности. В 2021 году, не малоизвестная компания АО «Позитив Технолоджиз», опубликовала данные о методах атак на организации и частных лиц за 2020 год, которые представлены на рисунке 1 и рисунке 2.

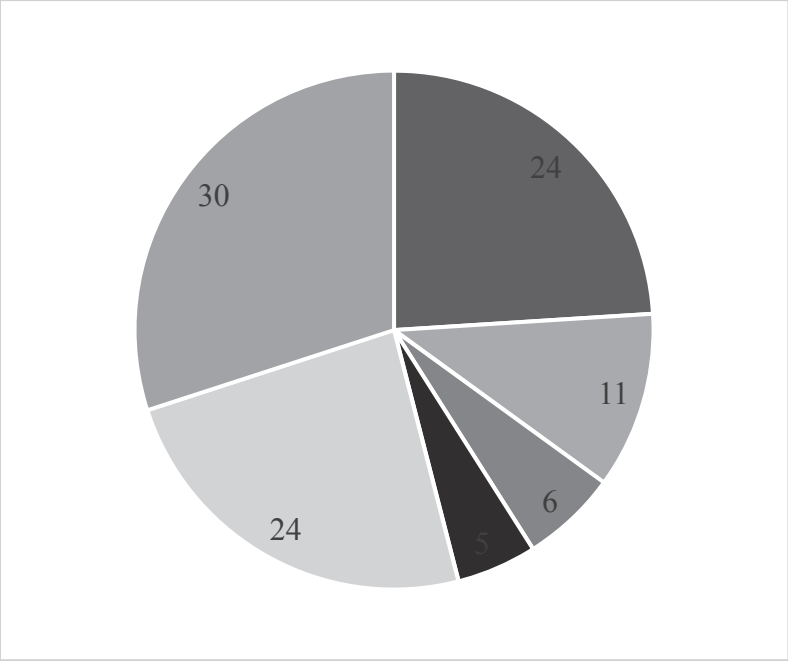


Рисунок 1 – Методы атак на организации в 2020 году

На рисунке 1, в % долях отображены методы атак на организации, а именно:

- 30% - Социальная инженерия;
- 24% - Использование вредоносного программного обеспечения;
- 24% - Хакинг;

- 11% - Эксплуатация веб-уязвимостей;
- 6% - Другие;
- 5% -Подбор учетных данных.

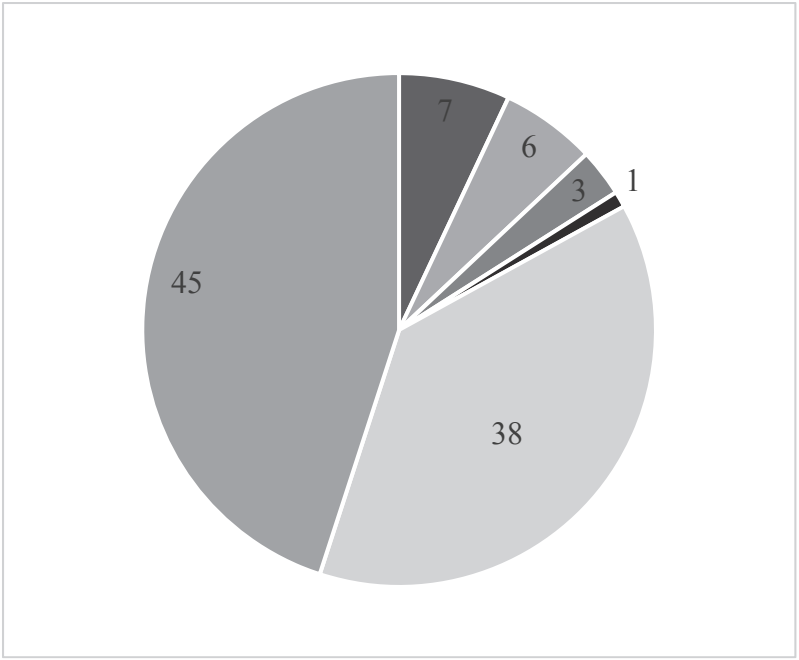


Рисунок 2 – Методы атак на частных лиц в 2020 году

На рисунке 2, в % долях отображены методы атак на частных лиц, а именно:

- 45% - Социальная инженерия;
- 38% - Использование вредоносного программного обеспечения;
- 7% - Хакинг;
- 6% - Подбор учетных данных;
- 3% - Другие;
- 1% - Эксплуатация веб-уязвимостей.

Проанализировав Рисунок 1 и Рисунок 2 можно сделать вывод о том, что социальная инженерия лидирует в числе всех возможных методов атак, а значит необходимо разобраться в том, что она из себя представляет.

Использование социальной инженерии направлено на получение необходимого доступа к информации. Данные методы основаны на изучении психологии человека, а также психологическом воздействии на субъект, который потенциально может иметь доступ к защищаемым активам. Вид угрозы, который образуется не извне, а внутри организации, при котором используются такие методы, принято называть «инсайд атаки». Этот вид атак опасен тем, что сотрудник, действия которого привели к нарушению информационной безопасности и потери ценных активов, может и не подозревать, что совершил противоправные действия.

Социальная инженерия используется ежедневно обычными людьми в повседневных ситуациях. Например, во взаимодействии педагогов со своими учениками. Врачи, психологи и психотерапевты часто используют элементы социальной инженерии, чтобы “манипулировать” своими пациентами, для принятия мер, которые помогут пациенту, а мошенник использует элементы социальной инженерии, чтобы убедить его выполнить действия, необходимые злоумышленнику или способные привести к раскрытию информации [1]. Опытный психолог в своей работе использует фразы и вопросы, которые помогают пациенту прийти к выводу, который необходим для улучшения качества его жизни. Таким же образом, злоумышленник может пользоваться определенными вопросами и фразами, чтобы определить уязвимые места субъекта. Методы манипулирования, аналогично другим психологическим механизмам, можно применять как для достижения положительных целей, так и для отрицательных. В рамках информационной безопасности, социальная инженерия, подразумевает психологическое воздействие на человека, которое приводит к выполнению желаемого действия, и как следствие получение доступа к ценному активу. Таким образом происходит злоупотребление доверием, которое приводит к негативным последствиям. Зачастую во время анализа совершившегося инцидента информационной безопасности, с высокой вероятностью можно найти проявление социальной инженерии. В широком смысле социальная инженерия — это процесс психологического влияния на человека, который провоцирует субъект совершить действие, которое необходимо манипулятору, не подозревая о негативных последствиях. Основные этапы атак с применением социальной инженерии:

1. Предварительное обследование и сбор базовой информации о потенциально атакуемом объекте;
2. Разработка точного плана действий и подготовка выбранных механизмов атаки (вредоносные вложения, фишинговые ресурсы и т.д.);
3. Установление связи по сети или реальное знакомство с субъектом атаки, и процесс успешного возникновения с ним доверительных отношений;
4. Финальный этап - непосредственно получение доступа к защищаемому активу.

Чтобы избежать этого, необходимо разработать и внедрить технологию менеджмента уровня «лояльности» персонала. Данная технология должна помочь устранить проблемы этого характера в системе ИБ.

Как я вижу возможное решение этой проблемы? Для начала нужно определить защищаемые ресурсы и степень их значимости. Если мы берем в пример коммерческую организацию, не обрабатывающую сведения, составляющие государственную тайну, то обычно степень значимости защищаемой информации определяется присвоенными метками конфиденциальности, такими как, «конфиденциально» и «строго конфиденциально». После этого, необходимо провести ранжирование

персонала в соответствии с его потенциальной возможностью влияния на систему защиты информации и доступа к ценным активам. Это позволит разбить весь персонал на группы и определить какие из них требуют особенного наблюдения. Для удобства я обозначаю эти группы пользователей следующим образом: «Специальные» - которые имеют доступ к строго конфиденциальным активам компании и/или имеют доступ к настройкам средствам защиты информации, которые образуют основной каскад системы защиты информации, «Значительные» - которые имеют доступ к конфиденциальным активам компании, «Незначительные» - у которых нет доступа к защищаемой информации. Далее необходимо создать начальную «точку отсчета» для каждого человека, который входит в «Специальную» группу персонала. «Точка отсчета» формируется исходя из анализа личного дела и проведения аудирования в свободной форме. В процессе аудирования субъекта с ним обсуждаются вопросы, составленные компетентным психологом, ответы на которые позволят составить психологический портрет человека. Это нужно для определения фундамента «лояльности» рассматриваемой единицы персонала. Сформировав фундамент «лояльности» для каждой из групп персонала, можно переходить ко второму этапу.

Второй этап включает в себя процесс внесения полученных данных в специальное программное обеспечение, которое поставляется вместе с системой видеонаблюдения, к которой мы вернемся чуть позже. Программное обеспечение позволяет вести карточки пользователей с отображением текущего и прогнозируемого уровней «лояльности» персонала, которые основываются на анализе введенных данных о фундаменте «лояльности» субъекта и информации, полученной из следующих этапов.

Следующий этап подразумевает под собой внедрение специальной системы видеонаблюдения со встроенной функцией распознавания лиц людей и обучаемым искусственным интеллектом, который имеет возможность оценивать и анализировать действия и жесты субъектов персонала, которые входят в различные группы персонала. Система должна уметь анализировать состояние человека посредством оценки его обычных каждодневных действий, жестов и мимики которые накапливаются с течением времени в базе данных и сообщать администратору системы, когда происходит действие, жест или мимика, которые не характерны для этого субъекта персонала. Также программный блок-системы, отвечающий за аналитику, должен использовать совокупность данных полученных из базы данных поведения персонала, карточек пользователей в базе данных специального программного обеспечения, рассмотренного на втором этапе и действий, жестов и мимики персонала в режиме реального времени. На основе этих данных и должно происходить формирование уровня «лояльности» каждой ячейки групп персонала. Это позволит предугадать

запланированное нарушение полномочий или акт, направленный на умышленное негативное воздействие на систему защиты информации или ценные активы организации. При этом система должна быть гибко настроена, для того чтобы не создавать негативный эффект от ощущения сильного контроля над персоналом.

Четвертый этап состоит из организации и проведения специальных мероприятий, направленных на реализацию двух различных типов ситуаций. Первый тип подразумевает под собой ситуацию с психологическим и моральным подтекстом, в которую попадает субъект из выбранной группы персонала, а дальше происходит анализ его действий и принимаемых решений. Второй тип ситуации должен имитировать процессы, применяемые в методе социальной инженерии. Это позволит определить модель поведения субъекта персонала в потенциально опасных ситуациях, которые могут привести к потере ценных активов, и как следствие возникновение ущерба организации.

Пятый этап включает в себя проведение мероприятий, направленных на поднятие уровня доверия и комфорта работы персонала, а также в целом его нахождения в компании. Я считаю это один из самых важных этапов предлагаемой мной системы. От остальных этапов его отличает то, что он направлен не на увеличение контроля за персоналом, а на создание более благоприятных условия для работы, что, по моему мнению, является одним из самых важных аспектов для поддержания необходимого уровня «лояльности». Исходя из опыта могу с уверенностью сказать, что сотрудники, которым нравятся условия и организация их работы, а также чувствуют отдачу от руководства, менее подвержены влиянию методов социальной инженерии и много реже за ними замечено умышленных негативных воздействий на защищаемые активы и систему защиту информации.

Механизмами, которыми можно выполнить пятый этап могут являться, например, организация индивидуального графика работы, создание удобного и комфортного рабочего места, проведение разнообразных корпоративов и так далее.

Применение описанных в статье этапов (использование технических и организационных мер), обеспечивает реализацию комплексного подхода, что позволяет максимально эффективно воздействовать на систему защиты информации. При этом, очень важно чтобы все пять этапов повторялись циклически, чтобы система постоянно адаптировалась и совершенствовалась. Схема циклической реализации этапов представлена на рисунке 3. Применение описанной технологии поможет поднять уровень «лояльности» персонала в компании.

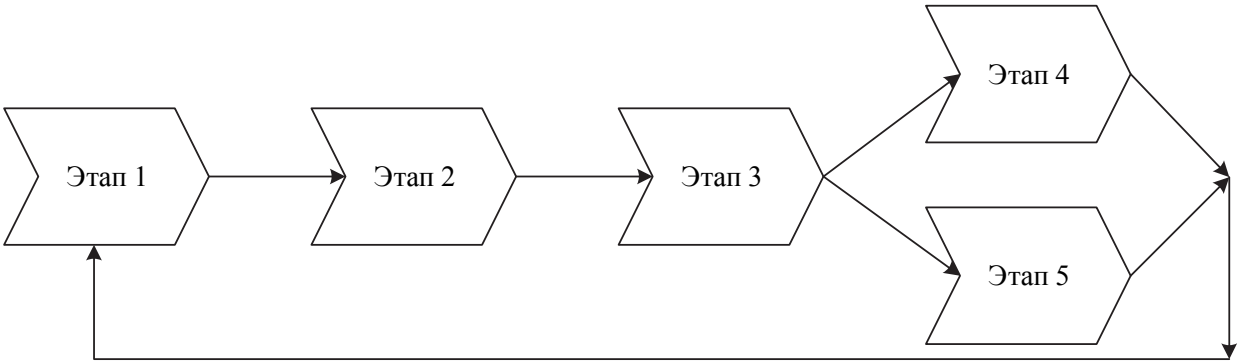


Рисунок 3 – Последовательность этапов технологии управления «лояльностью персонала»

Таким образом, используя основы данной системы управления уровнем «лояльностью» персонала, при этом внедряя ее у себя в организации с учетом особенности ее функционирования, можно добиться желаемого уровня «лояльности» персонала, значительно уменьшив риск реализации потери ценных активов организации посредством реализации «социальной инженерии».

Литература

1. Мартынова Л.Е., Назарова К.Е. Социальная инженерия и информационная безопасность. 2017. № 1. С. 61–63.

2. Актуальные киберугрозы [Электронный ресурс]. 2021. Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/cybersecurity-threatscape-2019-q4-rus.pdf (дата обращения: 19.05.2022).

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СТРОИТЕЛЬСТВЕ

Дымова Анастасия Вячеславовна, магистрант 2 курса кафедры математики и естественнонаучных дисциплин
Научный руководитель: **Бугай Ирина Владимировна**, к.т.н., доцент, заведующий кафедрой математики и естественнонаучных дисциплин

Постоянно растущий уровень конкуренции в строительстве требует оптимизацию по строительно-монтажным работам с использованием автоматизированных систем проектирования, которые позволяют снизить трудозатраты строителей и сократить время выполнения работ. Информационные технологии отличный инструмент для этого.

Информационные технологии, САПР, моделирование.

INFORMATION TECHNOLOGIES IN CONSTRUCTION

Dymova Anastasia, 2nd year graduate student of the Department of Mathematics and natural sciences
Scientific adviser: **Bugay Irina**, Candidate of Technical sciences, Associate professor, Head of the Department of Mathematics and natural sciences

The ever-increasing level of competition in construction requires optimization of construction and installation work using computer-aided design systems, which can reduce the labor costs of builders and reduce the time of work. Information technology is a great tool for this.

Information technology, CAD, modeling.

Понятие «информация» применима во всех областях применения. В строительстве под информацией можно понимаются любые данные, сведенья, знания, которые кого-то интересуют. По степень доступности для человека информацию можно разделить на три вида (рис.1) [3, С.6].

Рисунок 1 – Разновидность информации

Развитие научно-технического прогресса ведет к интенсивному увеличению используемого объема информации. Каждые десять лет объем удваивается. Совершенствование компьютерной техники и изобретений, позволяющей хранить и извлекать огромное количество информации, способствует повышению эффективности и развитию информационных технологий, их распространению во всех отраслях жизни.

Для эффективного управления работой строительной компании необходимо иметь обширную информацию о ситуации в компании и способность быстро реагировать на меняющуюся ситуацию. Для этого у руководителя компании всегда должна быть свежая и достоверная информация. Организовать управление работой строительной организации необходимо так, чтобы была обеспечена быстрая и надежная связь между различными работниками для их наиболее согласованного взаимодействия.

Информационные технологии и специализированное программное обеспечение все чаще используется в современном строительстве. К ним относится система автоматизированного проектирования (САПР), системы управления проектной документацией и программное обеспечение для оценки.

САПР – представляет собой комбинацию аппаратного и программного обеспечения, предназначенных для участия в процессе проектирования, помогает добиться максимальной эффективности проекта.

Автоматизировать одну задачу проекта – совсем не значит автоматизации процесса проектирования в целом, так как нет возможности совместить в одной программе все требования всех стадий проектирования. Объем информационных потоков в строительном проекте огромен ускоренная обработка информации должна помочь сократить время и стоимость, а также повысить качество работ.

Внедрение информационных технологий в офисную работу в основном предполагает автоматизацию рутинных задач, в том числе обмен строительными документами в цифровом приложении – это наиболее распространенное его использование, то есть компьютерная обработка для офисного и контактного администрирования. Применение офисной автоматизации может повысить эффективность внутреннего управления компании.

Программы САПР также должны обеспечивать простое редактирование проекта и возможность сравнения его нескольких вариаций, уметь выявлять и оповещать о различных ошибках в проектировании. Единство системы САПР обеспечивается наличием набором взаимосвязанных моделей, определяющих объект проектирования в целом, а также набора системных интерфейсов, реализующих взаимосвязь.

Создание и использование моделей объектов строительства в прикладных задачах осуществляется с помощью комплекса средств

компьютерного проектирования (КСАП). Структурными частями КСАП являются различные комплексы ресурсов, а также компоненты организационной безопасности (рис. 2).

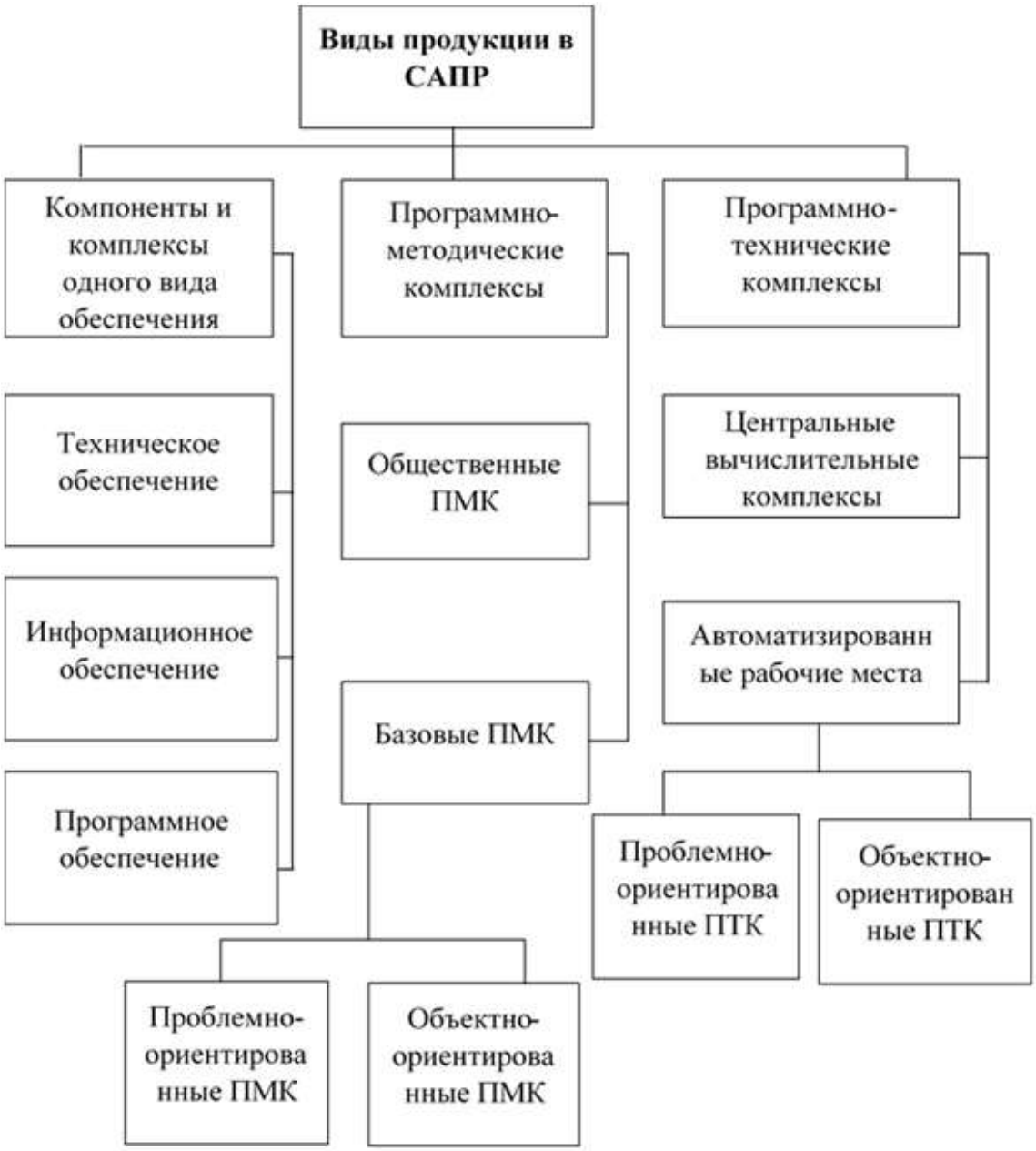


Рисунок 2 – Виды компонентов и комплексов САПР

Самой популярной в мире системой автоматизированного проектирования является программа AutoCAD. Он был разработан Autodesk более 20 лет назад, давно отвечает самым взыскательным требованиям дизайнеров. Программа может рисовать 2D и 3D модели. Богат набором инструментов и возможностью подстроиться под требования пользователей, но он уже не удовлетворяет запросы большинства проектировщиков. Его можно использовать для разработки очень небольших и относительно

простых проектов, при этом автоматизируя только рутинную работу чертежной доски. Современным проектировщикам требуется больше, чем быстрые и красивые чертежи. С его помощью можно спроектировать любой строительный объект, вносить в него изменения при необходимости, виртуально создавать нужные формы и поверхности, которые можно рассматривать под разными углами. Так же с его помощью можно обмениваться информацией через интернет и связывать данные с сайтами. Пример работы можно увидеть на рис. 3.

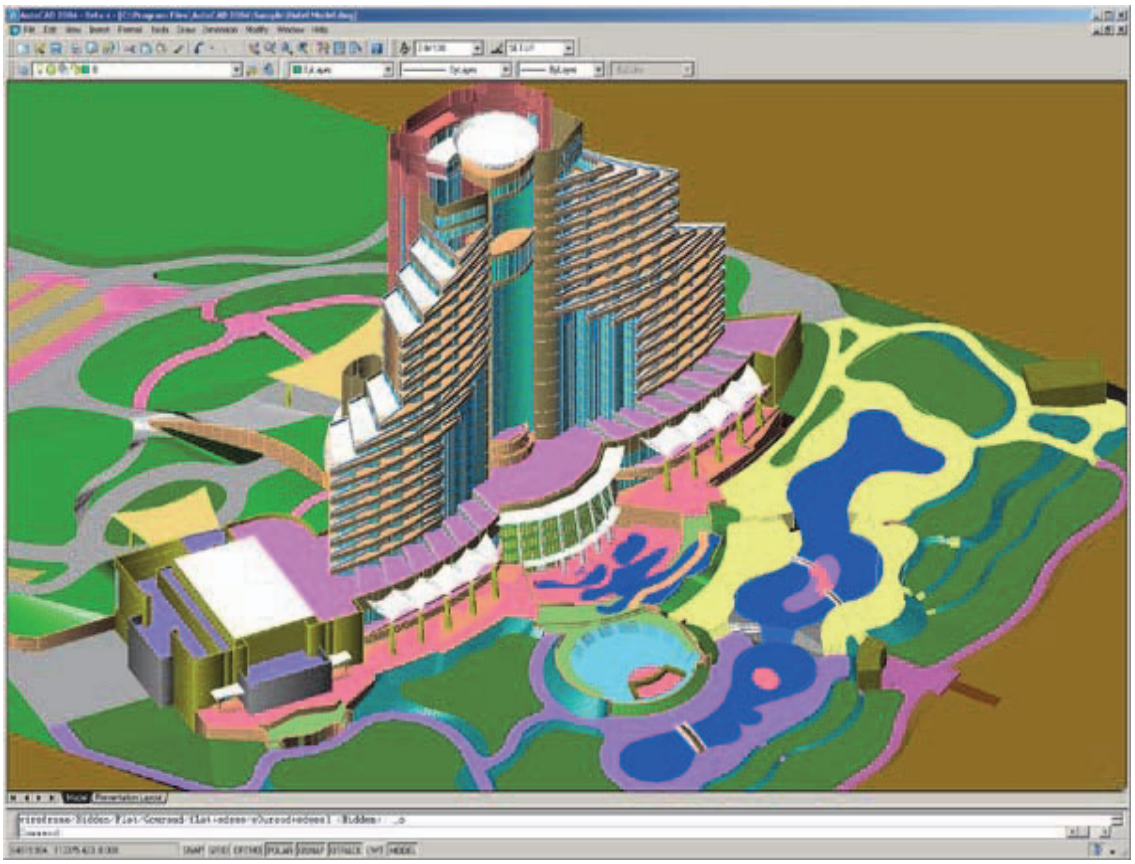


Рисунок 3 – Трехмерный чертеж, выполненный в AutoCAD

Информационные технологии сама по себе не может решить фундаментальные проблемы строительства, только лучшие теории и концепции могут, а информационные технологии могут оказать поддержку (рис. 4)

Здесь прямо признается факторы такие как, общие принципы управления операциями, понимание особенностей их построения, и информационные технологии, которые могут привести к изменениям в информационных процессах. Эти подходы взаимодействуют друг с другом и могут усиливать или ограничивать влияние на информационные процессы.

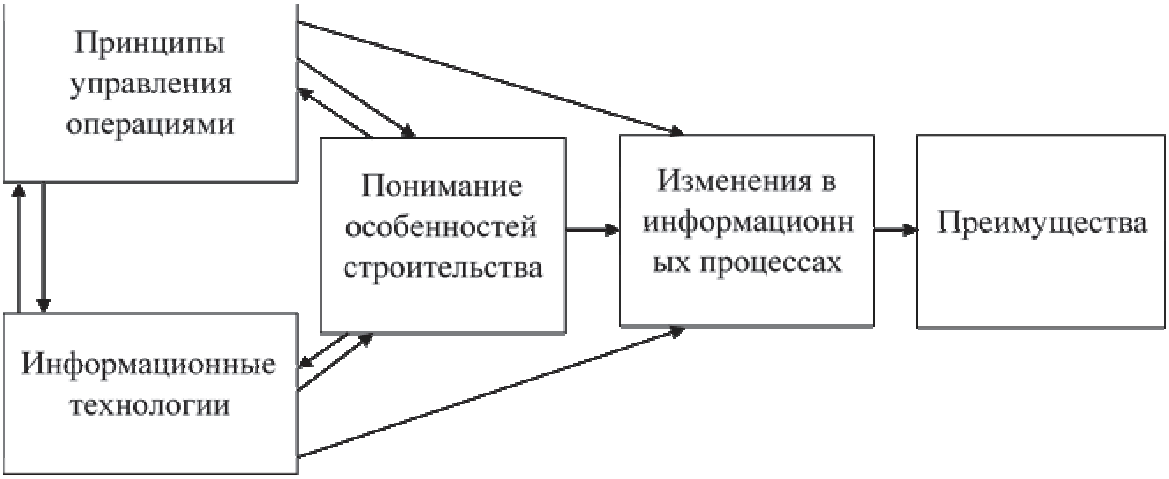


Рисунок 4 – Взаимосвязь между управлением операциями, пониманием строительства и информационных технологий

В строительстве моделирование играет важную роль. Моделирование каркаса не имеет связанных с ним поверхностей, просто линии и дуги, которые представляют края или пределы объекта. Это форма моделирования представляет хороший переход от режима 2D-чертежа к представлению о 3D-визуализации. Каркасные модели, к сожалению, не объемные и не дают пользователю увидеть объект как в реальной жизни.

Твердотельное моделирование – это компьютерное моделирование трехмерных твердых объектов. Цель такого моделирования обеспечить геометрическую правильную поверхность. Это считается наиболее сложным аспектом в области автоматизированного моделирования (САПР), поскольку оно требует, чтобы программного обеспечение САПР имитировало объект изнутри и снаружи. Это очень важно, так как позволяет дизайнерам представлять срезы дизайна. Оно позволяет проектировать, создавать, визуализировать и анимировать 3D-модели. Программное обеспечение, для твердотельного моделирования основано на необходимости предельной точности информации в механической геометрии.

Моделирование поверхности - это математический метод, обычно представляемый в приложениях автоматизированного проектирования для отображения объектов с твердым покрытием. Моделирование поверхности позволяет пользователям смотреть на конкретный объект под определенными углами с твердыми поверхностями. Этот вид моделирования является популярным для архитектурных проектов и визуализации. Такой метод считается более сложным методом отображения объектов, чем каркасное моделирование. Так же имеет гораздо менее неоднозначные функциональные возможности отображения по сравнению с каркасным моделированием, но не так много или сложно, как твердотельное моделирование. Техника часто включает в себя преобразования между различными типами трехмерного моделирования (рис.5).

Типичные процессы связанные с моделированием поверхности:

- Генерация модели, объединяющая трехмерные поверхности и твердые тела;
- Преобразование модели в процедурные поверхности с использованием преимуществ ассоциативного моделирования;
- Проверка дефектов с помощью инструментов анализа поверхности;
- Восстановление поверхностей объектов для применения гладкости к объекту.

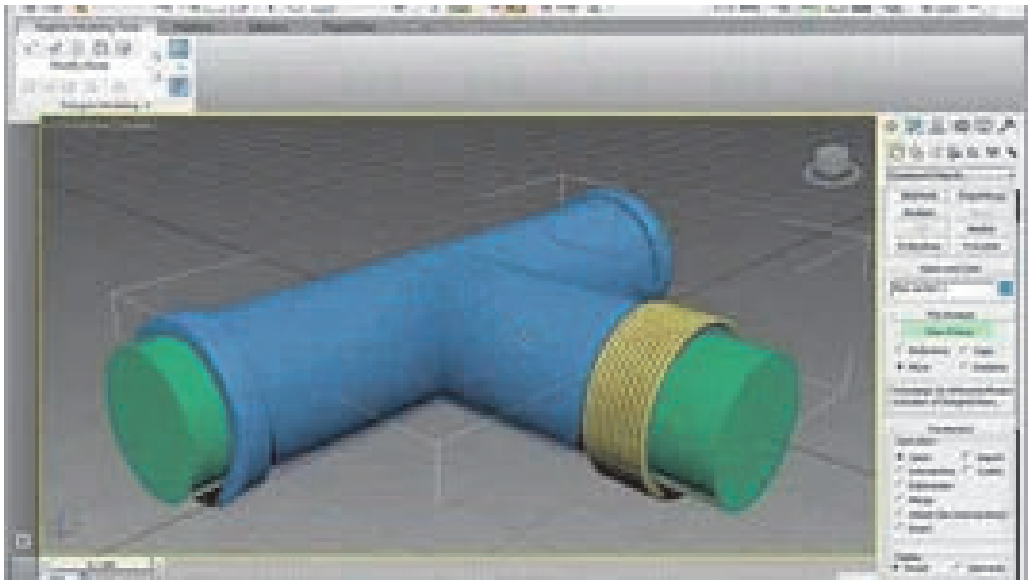


Рисунок 5 – Пример моделирования поверхности

Одним из уникальных свойств поверхностных моделей является то, что они не могут быть разрезаны, как твердые модели. Объекты, используемые в моделировании поверхности, могут быть геометрически неправильными, в отличие от твердотельного моделирования, где оно должно быть правильным.

Литература

1. Лихачева, Г.Н. Информационные системы и технологии: учебно-методический комплекс / Г.Н. Лихачева, М.С. Гаспариан. – Москва: Евразийский открытый институт, 2011.-370 с.

2. Моделирование организационно-технологических решений в строительстве: учебное пособие / С. М. Кузнецов, А. И. Круглов, О. А. Легостаева, К. С. Кузнецова; отв. ред. А. И. Круглов. – Москва; Берлин: Директ-Медиа, 2016. – 95 с.

3. Пеньковский Г.Ф. Основы информационных технологий и автоматизированного проектирования в строительстве: конспект лекций / СПбГАСУ. – СПб., 2008. – 150 с.

САМООЧИЩЕНИЕ АТМОСФЕРЫ ОТ КРУПНЫХ АЭРОЗОЛЬНЫХ ЧАСТИЦ

Евдокимова Виктория Александровна, магистрант 2 курса кафедры математики и естественнонаучных дисциплин
Научный руководитель: **Чаусова Ольга Владимировна,** к.ф.-м.н., доцент кафедры математики и естественнонаучных дисциплин

Настоящая работа посвящена исследованию процессов самоочищения атмосферы от вредных для здоровья людей аэрозольных частиц. В ходе решения задачи определены скорости термофоретического и диффузиофоретического движения крупных летучих частиц, учтено небольшое отклонение формы частиц от сферической. Найдено выражение для вычисления времени полной очистки заданного объема от аэрозоля. Сделан вывод о возможном направлении движения аэрозольных частиц в зависимости от входящих в итоговую формулу характеристик.

Аэрозольные частицы, самоочищение атмосферы, скорость термодиффузиофореза.

SELF-PURIFICATION OF THE ATMOSPHERE FROM LARGE AEROSOL PARTICLES

Evdokimova Victoria, 2nd year graduate student of the Department of Mathematics and natural sciences
Scientific adviser: **Chausova Olga,** Candidate of Physical and mathematical sciences, Associate professor of the Department of Mathematics and natural sciences

This work is devoted to the study of the processes of self-purification of the atmosphere from aerosol particles harmful to human health. In the course of solving the problem, the velocities of the thermophoretic and diffusiophoretic motion of large volatile particles were determined, and a small deviation of the particle shape from spherical was taken into account. An expression for calculating the time of complete cleaning of a given volume from aerosol has been found. A conclusion is made about the possible direction of movement of aerosol particles, depending on the characteristics included in the final formula.

Aerosol particles, self-purification of the atmosphere, rate of thermodiffusiophoresis.

В настоящее время все большую актуальность приобретают вопросы, связанные с механизмами очистки атмосферы от находящихся в ней

аэрозольных примесей. Деятельность промышленных предприятий, связана с выбросами частиц пыли, сажи, металла, которые оказывают пагубное воздействие на здоровье человека и окружающую среду. Так выбросы пыли при работе цементных заводов, строительных предприятий могут влиять на климат, образуя облака, задерживающие прохождение солнечных лучей к поверхности земли. Оксиды металлов (цинка, марганца, кремния) разрушают озоновый слой. Попадая в организм человека при дыхании вредный аэрозоль пагубно сказывается на работе легких, снижает уровень насыщения крови кислородом, вызывают заболевания кожи, аллергические реакции [1].

В настоящей работе исследуется механизм самоочищения атмосферы от крупных аэрозольных капель. За счет процессов, происходящих в атмосфере (столкновения, гравитационное осаждение и прочие), частицы могут сливаться в достаточно крупные капли, размер которых в десятки раз превосходит изначальные размеры аэрозольных частиц. При этом, частицы, на поверхности которых происходит фазовый переход образуют вокруг себя неоднородные по температуре и концентрации поля. Вследствие чего наблюдается направленное движение аэрозоля относительно капли (к поверхности или от нее). Таким образом происходит естественное вымывание вредного аэрозоля из атмосферы.

Выделим в пространстве вокруг капли радиуса R_d некоторый объем $V = \frac{4}{3}\pi R_V^3$. При испарении капли (либо при ее конденсационном росте) вокруг нее создаются сферически симметричные распределения температуры и концентрации, с градиентами $\nabla T_e, \nabla C_1, \nabla C_2$ соответственно (T_e распределение температуры вне капли, $\mathrm{C}_1 = \frac{n_1}{n_0}$ −относительная концентрация летучего вещества капли, $\mathrm{C}_2 = \frac{n_2}{n_0}$ −относительная концентрация несущего компонента газовой смеси, n_1, n_2 −числа молекул компонентов газовой смеси в единице объема, $n_0 = n_1 + n_2$). Рассматривается установившийся процесс испарения, однако время решения задачи ограничено условием конечности размеров летучей капли.

Для вычисления времени очистки заданного объема от аэрозоля необходимо определить скорость переноса аэрозольных частицы, которая будет складываться из скоростей термофреза, диффузиофореза и скорости центра инерции газовой смеси:

$$U_r = U_r^D + U_r^T + U_r^{\text{ц.м.}},$$

где U_r^D – скорость диффузиофоретического движения капли, U_r^T – скорость термофоретического движения капли, $U_r^{\text{ц.м.}}$ – скорость движения среды относительно центра капли.

Так как рассматривается движение крупных частиц - характерный размер капли много больше средней длины свободного пробега газовых молекул, решение проводится в гидродинамическом режиме. По составу капля однокомпонентная, теплопроводность капли χ_i, динамическая вязкость

η_0^i Газовая смесь двухкомпонентная, ее средняя теплопроводность χ_e, вязкость η_0^e, коэффициент взаимной диффузии D_{12}^e. При движении капли сохраняют свою сферическую форму.

Задача обладает сферической симметрией, поэтому решение проводится в сферической системе координат $(r;\theta;\varphi)$, начало которой совпадает с геометрическим центром капли. В данной системе координат частица покоится, а внешняя среда набегает на нее со скоростью $\vec{U}$.

Вычисление скорости термофоретического переноса капли.

Распределение скоростей, давления, концентрации и температуры находятся из решения системы уравнений Стокса, неразрывности и Лапласа

$$\eta^e \Delta \vec{v}^e = \nabla p^e \quad (1)$$

$$div\ \vec{v}^e = 0 \quad (2)$$

$$\Delta C_{1e} = 0 \quad (3)$$

$$\Delta T^e = 0 \quad (4)$$

$$\Delta T^i = 0 \quad (5)$$

при следующих условиях граничных условиях и условиях на бесконечности [4].

$$r \to \infty:$$

$$v_r^e = \left|\vec{U}\right| cos\,\theta\,, v_\theta^i = -\left|\vec{U}\right| \sin\theta\,, p^e = p_0^e, \quad (6)$$

здесь p_0^e – невозмущенное значение давления при температуре T_0^e

$$z = r\cos\theta$$

$$T^e = T_0^e + |(\nabla T_e)_\infty|\, r\cos\theta\,, \quad (7)$$

здесь T_0^e – невозмущенное значение температуры на бесконечности, $A_T = (\nabla T)_\infty$ - постоянный градиент температуры

$$\mathrm{C}_{1e} = C_{01e} \quad (8)$$

$$r = R:$$

$$v_\theta^e - v_\theta^i = \frac{K_{TSl}}{T_0^e R}\frac{\partial T^e}{\partial \theta} + K_{Sl}^e D_{12}^e \frac{1}{R}\frac{\partial C_{1e}}{\partial \theta}, \quad (9)$$

здесь K_{TSl} – коэффициент теплового скольжения, β_T – коэффициент, учитывающий небольшое отклонение формы капли от сферической.

$$-p^e + 2\eta_0^e \frac{\partial v_r^e}{\partial r} - \frac{2}{R}\frac{\partial \sigma}{\partial T^i}\Big|_{T^i - T_0^i}\left(T^i - T_0^i\right) - \frac{2\sigma}{R}\Big|_{T^i - T_0^i} =$$

$$= -p^i + 2\eta_0^i \frac{\partial v_r^i}{\partial r}. \quad (10)$$

Слагаемые $\frac{2}{R}\frac{\partial \sigma}{\partial T^i}\Big|_{T_i - T_0^i} - \frac{2\sigma}{R}\Big|_{T^i - T_0^i}$ обусловлены наличием поверхностного натяжения на границе раздела капля – газовая среда.

$$\eta_0^e\left(\frac{1}{r}\frac{\partial v_r^e}{\partial\theta}+\frac{\partial v_\theta^e}{\partial r}-\frac{v_\theta^e}{r}\right)+\frac{1}{R}\frac{\partial\sigma}{\partial T^i}\Big|_{T_i-T_0^i}\frac{\partial T^i}{\partial\theta}=$$
$$=\eta_0^i\left(\frac{1}{r}\frac{\partial v_r^i}{\partial\theta}+\frac{\partial v_\theta^i}{\partial r}\right.$$
$$\left.-\frac{v_\theta^i}{r}\right) \quad (11)$$

Выражение $\frac{\partial\sigma}{\partial T^i}\Big|_{T_i-T_0^i}\frac{\partial T^i}{\partial\theta}$ есть первая производная $\frac{\partial\sigma}{\partial\theta}$, взятая в первом приближении при разложении по малому параметру.

$$n_{20}^e v_r^e - D_{12}^e n_{0e}^2\frac{m_1}{\rho_0^e}\frac{\partial C_2^e}{\partial r}=0 \quad (12)$$

$$n_{10}^e v_r^e - D_{12}^e n_{0e}^2\frac{m_2}{\rho_0^e}\frac{\partial C_1^e}{\partial r}=n_{0e}\alpha\nu(C_{1e}^{\mathrm{H}}-C_1^e) \quad (13)$$

$$-\kappa_0^e\frac{\partial T^e}{\partial r}+\kappa_0^i\frac{\partial T^i}{\partial r}=-n_{0e}\alpha\nu Lm_1(C_{1e}^{\mathrm{H}}-C_1^e), \quad (14)$$

$$T^e=T^i. \quad (15)$$

Индекс «0» у величин означает, что коэффициенты переноса принимаются как постоянные величины при температуре $T=T_0^e$.

Решения уравнений Стокса представляются в виде разложений [1] по полиномам Лежандра n-го порядка $P_n(\theta)$:

$$v_r^e=\left|\vec{U}\right|\cos\theta+\frac{\gamma}{r}+\sum_{n=1}^{\infty}\left[-\frac{n+1}{r^{n+2}}A_{-n-1}+\frac{n+1}{2(2n-1)}\frac{B_{-n-1}}{r^n}\right]P_n(\theta),$$

$$v_\theta^e=-\left|\vec{U}\right|\sin\theta+\sum_{n=1}^{\infty}\left[-\frac{A_{-n-1}}{r^{n+2}}-\frac{n-2}{2(2n-1)}\frac{B_{-n-1}}{r^n}\right]\frac{dP_n(\theta)}{d\theta},$$

$$p^e=\eta_0^e\sum_{n=1}^{\infty}\frac{B_{-n-1}}{r^{n+1}}P_n(\theta)+p_0^e,$$

$$v_r^i=v_{r0}^i+\sum_{n=0}^{\infty}\left[nA_nr^{n-1}+\frac{n}{2(2n+3)}B_nr^{n+1}\right]P_n(\theta),$$

$$v_\theta^i=\sum_{n=0}^{\infty}\left[A_nr^{n-1}+\frac{(n+3)B_n}{2(n+1)(2n+3)}r^{n+1}\right]\frac{dP_n(\theta)}{d\theta},$$

$$p^i=\eta_0^i\sum_{n=0}^{\infty}B_nr^nP_n(\theta)+p_0^i,$$

$$T^e=T_0^e+\sum_{n=1}^{\infty}\frac{T_n^e}{r^{n+1}}P_n(\theta)+A_T\cos\theta+\frac{\varphi_1}{r},$$

$$T^i = T_0^i + \sum_{n=1}^{\infty} T_n^i r^{(n)} P_n(\theta)$$

Подставляя указанные выше разложения в граничные условия, получаем систему уравнений, из решения которой находится выражения для скорости тремофоретического переноса капли:

$$U_T = K_{TSl}^e \frac{2\chi_e \left(1 + \alpha\nu R \frac{n_{02}^e}{2n_0^e D_{12}^e}\right)}{T_0^e \Phi_0} (\nabla T_e)_\infty + \frac{K_{Sl}^e \chi^e \alpha\nu R}{\Phi_0} \frac{n_{02}^e}{n_o^e} \frac{\partial C_{1e}^H}{\partial T_i} (\nabla T_e)_\infty$$
$$+ \chi_e \frac{n_0^e m_1}{\rho_0^e} \frac{\alpha\nu R}{\Phi_0} \frac{\partial C_{1e}^H}{\partial T_i} (\nabla T_e)_\infty, \qquad (16)$$

Где

$$\Phi_0 = \left(2\chi^e + \chi^i\right)\left(1 + \alpha\nu R \frac{n_{20}^e}{2n_0^e D_{12}^e}\right) + n_0^e \alpha\nu R L m_1 \frac{\partial C_{1e}^H}{\partial T_i}.$$

Нахождение скорости диффузиофоретического переноса капли.

Задача решается при тех же ограничениях, что и задача для термофореза. Движение капли описывается осесимметричными дифференциальными уравнениями Стокса, неразрывности и Лапласа [2]:

$$\eta \Delta \vec{v}^e = \nabla p^e \qquad \eta \Delta \vec{v}^i = \nabla p^i$$
$$div\ \vec{v}^e = 0 \qquad div\ \vec{v}^i = 0$$
$$\Delta T^e = 0 \qquad \Delta T^i = 0$$
$$\Delta C_1^e = 0$$

Граничные условия на бесконечности:

$$v_r^e = \left|\vec{U}\right| cos\,\theta\,, v_\theta^e = -\left|\vec{U}\right| \sin\theta\,, p^e = p_0^e,$$
$$C_1^e = C_{10}^e + |(\nabla C_{1e})_\infty| r\cos\theta,$$
$$T^e = T_0^e$$

Граничные условия на поверхности капли:

$$n_{20}^e v_r^e - D_{12}^e n_{0e}^2 \frac{m_1}{\rho_0^e} \frac{\partial C_2^e}{\partial r} = 0$$

$$n_{10}^e v_r^e - D_{12}^e n_{0e}^2 \frac{m_2}{\rho_0^e} \frac{\partial C_1^e}{\partial r} = n_{0e} \alpha\nu (C_{1e}^{\mathrm{H}} - C_1^e)$$

$$v_\theta^e - v_\theta^i = \frac{K_{TSl}}{T_0^e R} \frac{\partial T^e}{\partial \theta} + K_{Sl}^e D_{12}^e \frac{1}{R} \frac{\partial C_{1e}}{\partial \theta},$$

$$T^e = T^i.$$

$$-\chi_0^e \frac{\partial T^e}{\partial r} + \chi_0^i \frac{\partial T^i}{\partial r} = -n_{0e} \alpha\nu L m_1 \left(C_{1e}^{\mathrm{H}} - C_1^e\right),$$

$$v_\theta^e - v_\theta^i = \frac{K_{TSl}}{T_0^e R} \frac{\partial T^e}{\partial \theta} + K_{Sl}^e D_{12}^e \frac{1}{R} \frac{\partial C_{1e}}{\partial \theta},$$

$$-p^e + 2\eta_0^e \frac{\partial v_r^e}{\partial r} - \frac{2}{R}\frac{\partial \sigma}{\partial T^i}\Big|_{T^i - T_0^i}\left(T^i - T_0^i\right) - \frac{2\sigma}{R}\Big|_{T^i - T_0^i} = -p^i + 2\eta_0^i \frac{\partial v_r^i}{\partial r}.$$

Решения дифференциальных уравнений Стокса неразрывности и Лапласа представляются в виде известных разложений по полиномам Лежандра и описаны выше. Подставляя решения уравнений в граничные условия и решая получившуюся систему уравнений получим выражение для скорости диффузиофореза капли:

$$\begin{aligned}\overrightarrow{U_D} = -\frac{6\eta_0^i}{\left(3\eta_0^i + 2\eta_0^e\right)\Delta}\Bigg\{ & K_{Sl}^e {D_{12}^e}^2\left[2\chi^e + \chi^i + n_{0e}\alpha\nu L m_1 R\delta\right] \\ & + \left[\frac{K_{Tsl}^e}{T_{0e}} + \frac{R}{3\eta_{0i}}\delta_\sigma\right] D_{12}^e n_0^e \alpha\nu L m_1 R\Bigg\}\left(\nabla C_1^e\right)_\infty \\ & + \frac{3\left(\eta_0^i + 2\eta_0^e\right) D_{12}^e m_1}{\left(3\eta_0^i + 2\eta_0^e\right)\Delta\,\rho_0^e}\left[\left(2\chi^e + \chi^i\right) n_0^e \alpha\nu R\right]\left(\nabla C_1^e\right)_\infty, \end{aligned} \tag{17}$$

Где

$$\Delta = \left[2\chi_e + \chi^i\right]\left(2D_{12}^e + \frac{n_{20}^e}{n_0^e}\alpha\nu R\right) + 2D_{12}^e n_0^e \alpha\nu\, L m_1 R\delta,$$

$$\delta = \frac{\partial C_{1e}^H}{\partial T_i}, \qquad \delta_\sigma = \frac{\partial \sigma}{\partial T_i}$$

Далее определим скорость движения центра масс газовой смеси:

$$U^{\text{ц.м.}} = -D_{12}^e \frac{n_{0e}^2 m_1}{n_{20}^2 \rho_0}\left(\nabla C_1^e\right)_\infty \tag{18}$$

Таким образом, выражения (16), (17), (18) дают нам все составляющие для скорости движения аэрозольной капли:

$$U_r = U_r^D + U_r^T + U_r^{\text{ц.м.}}$$

Подставим все найденный значения запишем выражения для скорости движения капли

$$\overrightarrow{U_r} = -(\varphi_1 + \varphi_2)\frac{R_d}{R_V^2}\vec{n},$$

Где

$$\vec{n} = \frac{\vec{r}}{r},$$

$$\begin{aligned}\varphi_1 = \Bigg\{ & \frac{6\eta_0^i}{\left(3\eta_0^i + 2\eta_0^e\right)\Delta}\left[K_{Sl}^e {D_{12}^e}^2\left(2\chi^e + \chi^i + n_0^e\alpha\nu L m_1 R\delta\right) + \frac{K_{TSl}^e}{T_0^e} D_{12}^e n_{0e}\alpha\nu m_1 R\right] \\ & - \frac{3\left(\eta_0^i + 2\eta_0^e\right) D_{12}^e m_1}{\left(3\eta_0^i + 2\eta_0^e\right)\Delta\rho_0^e}\left(2\chi^2 + \chi^i\right) n_0^e \alpha\nu R + D_{12}^e \frac{{n_0^e}^2 m_1}{n_{20}^e \rho_0}\Bigg\}\left(C_{1e}|_{r-R_V}\right. \\ & \left. - C_{10}^H\right)\end{aligned}$$

$$\varphi_2 = \left[K_{TSl}^e \, 2\chi^e \left(1 + \alpha\nu R \frac{n_{20}^e}{2n_0^e D_{12}^e}\right) + K_{Sl}^e \, \frac{\chi^e \alpha\nu R \frac{n_{20}^e}{n_0^e} \frac{\partial C_{1e}^H}{\partial T_i}}{\Phi_0} \right.$$
$$\left. + \frac{\frac{\chi^e n_0^e m_1}{\rho_0^e} \alpha\nu R \frac{\partial C_{1e}^H}{\partial T_i}}{\Phi_0} \right] \left(T^e|_{r-R_V} - T_0^e\right).$$

Очевидно, что направление движения частицы зависит от знака выражения $(\varphi_1 + \varphi_2)$. Если $\varphi_1 + \varphi_2 > 0$, то частицы движутся к капле и происходит захват аэрозоля, если напротив $\varphi_1 + \varphi_2 < 0$, то частицы вымываются из рассматриваемого объема.

Вычисление времени очистки заданного объема от аэрозольных частиц

Существенный вклад в построение теории захвата аэрозольных частиц каплей внесли ряд отечественных и зарубежных исследователей: Н.А. Фукс, В.М. Волощук, Ю.П. Гупало, L. Facy, F. Prodi, H. Pruppacher, Б.В. Дерягин и др.

Расчет времени очистки производится по формуле:

$$t = \int_{R_d}^{R_v} \frac{dr}{U_r} = \frac{R_V^2 (R_V - R_d)}{(\varphi_1 + \varphi_2) R_d},$$

Можно упростить данное выражение, учитывая, что $R_d \ll R_V$:

$$t \approx \frac{R_V^3}{(\varphi_1 + \varphi_2) R_d}.$$

Выражения для скорости термодиффузиофоретического движения капли находятся в согласии с имеющимися исследованиями в области физики аэрозолей и в предельных случаях нелетучих частиц переходят в описанные ранее результаты.

Литература

1. Ефремова Д.А. Аэрозоли: положительное и отрицательное воздействие на организм человека // Abstracts Nationwide scientific forum of students with international participation «Student science – 2020» с.434

2. Яламов Ю.И., Ставцева О.В., Баринова М.Ф., Костицына Л.И. «Теория термо-диффузиофоретического переноса умеренно крупных летучих аэрозольных частиц при прямом учете влияния коэффициента испарения» Учебное пособие.- М.: Издательство МГОУ, 2008г, 65с.

3. Яламов Ю.И. Теория движения аэрозольных частиц в неоднородных газах.— Докторская диссертация.- М., 1968.

4. Brock I . R. Forces on Aerosols in Gas Mixtures // J. Colloid Sci. 1963. Vol. 18,-6. P.P. 489-501.

МЕТОДИКА ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ НА ОСНОВЕ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА

Еремеева Арина Андреевна, магистрант 1 курса кафедры информационной безопасности
Научный руководитель: **Сухотерин Александр Иванович**, к.воен.н., доцент кафедры информационной безопасности

Аудит информационной безопасности организаций является востребованной услугой. Хотя многие заказчики до сих пор не понимают его важность и необходимость. Внедрение эффективной системы безопасности достаточно дорогостоящая процедура, поэтому задача управления безопасностью состоит в том, чтобы найти баланс между стоимостью реализованных мер безопасности и рисками, связанными с защитой информации. Для обеспечения баланса целесообразно применение подхода к обеспечению информационной безопасности, основанного на оценке рисков.

Информационная безопасность, аудит информационной безопасности, риск-ориентированный подход, оценка рисков.

METHODOLOGY FOR AUDIT OF INFORMATION SECURITY OF ORGANIZATIONS ON THE BASIS OF A RISK-ORIENTED APPROACH

Eremeeva Arina, 1st year graduate student of the Department of Information security
Scientific adviser: **Sukhoterin Alexander**, Candidate of Military sciences, Associate professor of the Department of Information security

Information security audit of organizations is a demanded service. Although many customers still do not understand its importance and necessity. Implementing an effective security system is quite expensive, so the task of security management is to find a balance between the cost of implemented security measures and the risks associated with protecting information. To ensure a balance, it is advisable to use a risk-based approach to ensuring information security.

Information Security, information security audit, risk-based approach, risk assessment.

В настоящее время услуга аудита информационной безопасности (ИБ) организаций становится все более востребованной. Внедрение эффективной системы безопасности может быть очень дорогостоящим, особенно для

крупных организаций, из-за необходимости приобретения аппаратного и программного обеспечения для реализации технических мер безопасности, а также персонала для управления административными и техническими аспектами безопасности. Таким образом, задача управления безопасностью состоит в том, чтобы найти надлежащий баланс между стоимостью реализованных мер безопасности и рисками, связанными с защищаемыми данными и системами. Для обеспечения этого надлежащего баланса системы безопасности должны разрабатываться на основе оценки рисков.

Прежде чем переходить к оценке риска, необходимо понять, что подразумевается под риском. Риск - влияние неопределенностей на процесс достижения поставленных целей [1]. Иными словами, риск определяется как неопределенное событие или условие, которое, если оно происходит, оказывает положительное или отрицательное влияние на цели проекта.

Риск можно разделить на три вида. Первый вид риска – неотъемлемый риск. Это подверженность ошибкам, которые могут быть существенными по отдельности или в сочетании с другими ошибками, при условии отсутствия соответствующего внутреннего контроля. Например, информационная система, содержащая номера социального страхования, адреса, номера банковских счетов и медицинские записи нескольких миллионов клиентов, будет рассматриваться как имеющая высокий уровень неотъемлемого риска. То есть, если бы система была взломана, последствия были бы серьезными.

Второй тип риска — это риск средств контроля. Это риск того, что ошибка, которая может произойти и которая может быть существенной, по отдельности или в сочетании с другими ошибками, не будет своевременно предотвращена или обнаружена и исправлена системой внутреннего контроля. Средство контроля — это основанное на действиях заявление, в котором содержатся инструкции о том, как уменьшить или свести к минимуму риски безопасности. По сути, контрольный риск, связанный с информационной безопасностью, зависит от качества процессов обеспечения безопасности. Например, система, которая позволяет пользователям подключаться без уникального идентификатора пользователя или пароля, не записывает подключения и доступна с терминалов в неконтролируемых общественных местах, будет рассматриваться как имеющая чрезвычайно высокий уровень риска контроля [3].

Оценка риска информационной безопасности (организации); оценка риска ИБ (организации): Общий процесс идентификации, анализа и определения приемлемости уровня риска информационной безопасности организации [1].

Риск измеряется с точки зрения воздействия и вероятности. Это может быть выражено в виде формулы:

РИСК = (Вероятность убытка) Х (Последствия убытка)

Хотя вероятности и последствия часто не могут быть легко выражены в количественных показателях, чтобы можно было фактически вычислить

формулу, это обеспечивает основу для рассмотрения концепции риска, связанного с оценкой риска безопасности.

Можно выделить пять отдельных этапов подхода к управлению рисками и указать результаты, полученные в результате каждого из них.

Этап 1. Проведение анализа влияния на бизнес.

Проведение анализа влияния на бизнес помогает идентифицировать и документировать важные бизнес-процессы и лежащие в их основе зависимости, а также оценивать и ранжировать их на основе критичности. Технические и нетехнические факторы включены в качестве зависимостей (например, активы, персонал, данные, оборудование и приложения).

Проведение анализа влияния на бизнес показывает, как эти ключевые операции и функции повлияют на непрерывность бизнеса, если они будут затруднены.

Проведение анализа влияния на бизнес – это первый шаг в создании планов обеспечения непрерывности бизнеса и аварийного восстановления [2].

Этап 2. Проведение оценки рисков.

Оценка риска — это количественный и качественный процесс, который выявляет угрозы, уязвимости и нормативные требования, применимые к соответствующим бизнес-процессам и лежащим в их основе зависимостям. Он рассчитывает возможные последствия, если эти угрозы будут реализованы, и выдаёт выходное значение риска.

Выходное значение риска дает возможность понять и помочь определить приоритеты различных рисков, с которыми сталкивается организация. Этот результат является одним из самых больших преимуществ этого подхода, позволяющего создавать персонализированные показатели.

Знание выходного значения риска дает возможность ранжировать определенные уязвимости в реестре рисков. Реестр рисков обеспечивает действенную отправную точку для сосредоточения стратегических ресурсов на снижении рисков, представляющих наибольшую угрозу для непрерывности бизнеса и соблюдения нормативных требований [4].

Этап 3. Определение и внедрение необходимых средств контроля.

На этом этапе берутся неприемлемые риски и определяются, адаптируются, внедряются и назначается ответственность за элементы управления, которые уменьшат эти риски.

Персонализированные риски позволяют организации лучше настраивать средства контроля для устранения выявленных уязвимостей и угроз. Это также позволяет организации использовать компенсирующие меры, поскольку весь процесс принятия решений документируется. Документация демонстрирует, что организация понимает угрозу, которую средство контроля должно покрывать, и адекватно применяет другие компенсирующие средства контроля на основе анализа затрат и рисков.

Определение и внедрение правильных или необходимых средств контроля обеспечивает структуру и возможность обновлять или создавать политики и процедуры, которые укрепляют и передают видение и приоритеты организации в отношении ее безопасности.

Точно так же этот подход может обеспечить более активное участие и соблюдение требований, поскольку он создает возможность для диалога с отдельными заинтересованными сторонами, которые «владеют» процессом, включая поддержку со стороны руководства среднего звена. По сути, этот подход, основанный на оценке рисков, дает руководству убедительную причину для адаптации и принятия решений.

Этап 4: Тестирование, проверка и отчет.

После того, как средства безопасности будут реализованы, их необходимо протестировать и подтвердить. Примеры различных типов тестирования включают тесты на проникновение, дополнительные оценки рисков, тесты управления уязвимостями, упражнения на обеспечение непрерывности бизнеса, внутренние аудиты и оценки контроля соответствия.

Тестирование и проверка не только дают уверенность в том, что элементы управления работают и обеспечивают необходимый уровень безопасности, но и при периодической переоценке предоставляют возможности для включения недавно реализованных элементов управления безопасностью.

Теперь появляется возможность получить новую оценку стоимости риска, называемую остаточным риском, которая документируется и добавляется в реестр рисков для будущего анализа и определения приоритетов. Основываясь на инвестициях в новый контроль, рейтинг риска может снизиться, что указывает на более здоровый профиль риска [4].

Результаты тестирования и проверки должны быть задокументированы и зарегистрированы. Наличие эффективного механизма отчетности продемонстрирует прогресс на пути к исполнительному руководству и соответствие требованиям регулирующих органов. Кроме того, эффективная отчетность закладывает основу для создания процессов устранения пробелов и эскалации, которые увековечиваются на заключительном этапе.

Этап 5: Непрерывный мониторинг и управление.

Цель этого этапа — увековечить этапы 1–4 в воспроизводимый бизнес-процесс. Оценки рисков должны проводиться не реже одного раза в год, а действия по устранению последствий должны осуществляться, контролироваться и включаться в реестр рисков. Кроме того, должны быть созданы механизмы отчетности для внутренних сотрудников, чтобы выявлять потенциальные риски для организации. Часто у менеджеров и других сотрудников есть важные сведения о слабых сторонах или нарушениях нормативно-правовых требований, которые могут быть скрыты от группы управления рисками.

Соблюдение цикла может гарантировать, что любые новые уязвимости или угрозы будут выявлены и устранены последовательно и своевременно, что снизит вероятность того, что основные проблемы останутся незамеченными.

Непрерывное управление на протяжении всего жизненного цикла подхода, основанного на оценке рисков, будет способствовать подотчетности за внедрение и оценку средств контроля. Это создает пути эскалации для сложных или несоответствующих заинтересованных сторон и обеспечивает последовательность в адаптации контроля. Наконец, цикл предоставляет возможность обновлять или создавать необходимые политики или процедурную документацию и последовательно сообщать об изменениях в организацию.

Таким образом, риск-ориентированный подход — это систематический метод, который выявляет, оценивает и приоритизирует угрозы, стоящие перед организацией. Это настраиваемый метод, который позволяет бизнесу адаптировать свою систему безопасности к конкретным организационным потребностям и операционным уязвимостям.

Первым шагом в проведении оценки рисков является определение всех данных, находящихся в области ответственности организации. В организациях с централизованными информационными системами и минимальным количеством внешних услуг это может быть простой задачей. В других случаях, когда ответственность за управление информационными технологиями или бизнес-функциями передана поставщикам, или отдельные отделы несут полную или частичную ответственность за разработку и управление своими собственными системами, задача может значительно усложниться. Группе оценки рисков может потребоваться запросить управление информационными системами и управление бизнес-функциями. Обзор существующих документов может также предоставить ценную информацию о действующих системах. В случаях, когда услуги были переданы по контракту, способность организации влиять на средства контроля безопасности будет более ограниченной и должна быть достигнута в первую очередь путем включения в договор требований безопасности, а также процесса мониторинга соблюдения договорных требований.

Второй шаг – это оценка убытков в случае нарушения безопасности. Этот шаг соответствует определению уровня неотъемлемого риска, связанного с каждой системой или набором данных. В идеале эффект убытка следует выразить в денежной единице. Однако получить конкретную цифру может быть трудно, кроме того, фактические потери, связанные со сбоем в системе безопасности, могут быть искажены. При оценке риска необходимо учитывать последствия инцидентов и время, затрачиваемое на реагирование на них, а также негативные последствия для пользователей, если потерянные данные будут получены и использованы для преступной деятельности.

Следующий шаг – это оценка угроз и уязвимостей.

Угроза информационной безопасности организации; угроза ИБ организации: Совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации [1]. Проще говоря, угроза — это то, что может нанести ущерб системе или бизнес-функции, которую она поддерживает. Уязвимость (информационной системы): Свойство информационной системы, обусловливающее возможность реализации угроз безопасности, обрабатываемой в ней информации [1]. Другими словами, уязвимость — это недостаток в элементах управления безопасностью, который позволяет угрозе нанести ущерб.

Разработка списка угроз и уязвимостей для каждой системы и связанного с ней уровня риска управления должна осуществляться в сотрудничестве с подсистемами управления безопасностью, управления информационными системами и управления бизнес-функциями. Также могут быть привлечены внешние консультанты или аудиторы.

Следующим шагом идёт определение остаточного риска и приоритезация рисков. Остаточный риск — это риск того, что реализация угрозы приведет к значительному неблагоприятному воздействию на информационные системы или бизнес-процессы. Остаточный риск определяется как риск, остающийся после внедрения средств контроля безопасности.

Процесс определения остаточных рисков и приоритизации рисков должен быть практически синонимом определения того, на какие системы организация будет делать упор при разработке политик и внедрении средств контроля безопасности. Определение остаточных рисков с использованием простой системы высокого, среднего и низкого уровня риска демонстрируется в таблице 1.

Таблица 1 – Определение остаточного риска

	Неотъемлемый риск			
Контрольный риск		**Высокий**	**Средний**	**Низкий**
	Высокий	Высокий остаточный риск: сосредоточить ресурсы здесь	Средний остаточный риск: выделить ресурсы здесь	Низкий остаточный риск: выделить незначительные ресурсы
	Средний	Средний остаточный риск: выделить ресурсы здесь	Средний остаточный риск: выделить ресурсы здесь	Низкий остаточный риск: выделить незначительные ресурсы
	Низкий	Низкий остаточный риск: выделить незначительные ресурсы	Низкий остаточный риск: выделить незначительные ресурсы	Низкий остаточный риск: выделить незначительные ресурсы

Если система была оценена как имеющая высокий уровень неотъемлемого риска и высокий уровень риска средств управления, организация стоит инвестировать значительные ресурсы в средства управления безопасностью этой системы, чтобы снизить уровень риска. Принимая решения о распределении ресурсов, организация должна стремиться к тому, чтобы их распределение обеспечивало соответствие всем применимым законам, нормативным актам и контрактным требованиям [5].

Ещё один шаг – это разработка структуры политики безопасности. Хотя создание документов для аудиторов часто рассматривается как обременительное занятие, разработка и распространение политик и процедур является важной частью создания эффективной системы безопасности.

Ценность написания полных политик и процедур заключается в том, что, если пользователи не знают, что от них ожидается, они, не будут делать это. Политики и процедуры обеспечивают базовый стандарт, в соответствии с которым будут настраиваться функции безопасности, и предоставляют пользователям рекомендации по использованию систем.

Процедуры должны быть легко доступны для всех сотрудников, ответственных за их соблюдение или обеспечение. Следует также рассмотреть и внедрить обучение политикам и процедурам безопасности, а также потребовать от сотрудников письменного подтверждения того, что они прочитали и поняли процедуры.

Немаловажный этап – это разработка и внедрение технических решений для защиты данных. Этот этап включает в себя выбор аппаратных и программных решений, которые одновременно выполняют бизнес-цели, для которых были разработаны системы, и обеспечивают адекватные и экономичные средства достижения целей безопасности. Главный вывод, который следует сделать, заключается в том, что конкретные технические решения следует выбирать только после проведения оценки рисков, чтобы гарантировать, что реализованные решения соответствуют целям безопасности организации.

Таким образом, подход к обеспечению информационной безопасности, основанный на оценке рисков, принесет много преимуществ, включая персонализированную оценку рисков, расставленные по приоритетам уязвимости, адаптированные средства контроля и более надежный цикл для устранения новых рисков и уязвимостей.

Литература

1. Национальный стандарт Российской Федерации ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» от 01.10.2009: текст с изменениями и дополнениями на 2018 г. [Электронный ресурс] // Кодекс: электронный фонд правовых и нормативно-технических документов. Режим доступа: https://docs.cntd.ru/document/1200075565 (дата обращения: 20.04.2022)

2. Методы оценки риска: анализ воздействия на бизнес BIA (Business Impact Analysis) [Электронный ресурс] // Управление рисками: отраслевой портал. Режим доступа: https://upravlenie-riskami.ru/. (дата обращения 20.04.2022)

3. Определение терминов: Аудиторский риск, Неотъемлемый риск, Риск необнаружения и др. [Электронный ресурс] // Audit-ot: Бухгалтерский учёт. Налоги. Аудит. Режим доступа: https://www.audit-it.ru/inform/slovar/msfo-audit-6.html (дата обращения: 20.04.2022)

4. Применение риск-ориентированного подхода к кибербезопасности [Электронный ресурс] // CyLumena. Режим доступа: https://www.cylumena.com/insights/risk-based-cybersecurity/ (дата обращения: 20.04.2022)

5. Чалдаева Л.А., Килячков А.А., Дыдыкин А.В. Остаточные риски: определение, описание и методы снижения [Электронный ресурс] // Журнал «Финансы и кредит», 2009. Режим доступа: https://cyberleninka.ru/article/n/ostatochnye-riski-opredelenie-opisanie-i-metody-snizheniya (дата обращения: 20.04.2022)

ИСПОЛЬЗОВАНИЕ СУБД MYSQL И ЯЗЫКА PHP ПРИ РАЗРАБОТКЕ АДАПТИВНЫХ WEB-ПРИЛОЖЕНИЙ

Заруба Дмитрий Сергеевич, Гусев Леонид Сергеевич, Васильева Полина Юрьевна, магистранты 2 курса кафедры информационных технологий и управляющих систем
Научный руководитель: **Стреналюк Юрий Вениаминович,** д.т.н., профессор кафедры информационных технологий и управляющих систем

Статья отражает современные методы разработки веб-приложений на базе СУБД MySQL, PhpMyAdmin, HTML и PHP. Отдельное внимание в статье уделено анализу рациональных подходов в области разработки, а также описанию методик применения совместной работы языков программирования и ПО.

Информационные технологии, СУБД, PHP, разработка, веб-приложение, HTML.

USING MYSQL AND PHP IN DEVELOPING ADAPTIVE WEB APPLICATIONS

Zaruba Dmitry, Gusev Leonid, Vasilyeva Polina, 2nd year graduate students of the Department of Information technology and control systems
Scientific adviser: **Strenalyuk Yuriy**, Doctor of Technical sciences, Professor of the Department of Information technologies and control systems

The article presents modern methods of developing web applications based on DBMS MySQL, PhpMyAdmin, HTML and PHP. Particular attention is paid to the analysis of rational approaches to development, as well as a description of methods for the use of collaborative programming languages and software.

Information technology, DBMS, PHP, development, web application, HTML.

Как правило, в процессе разработки веб-сайта перед разработчиком встает вопрос о создании базы данных. Для создания собственного веб-сайта создается html-страница, в которой размещено ее содержимое. Постепенно сайт развивается, на нем появляется новая информация, а количество страниц, на которых она хранится, увеличивается. В связи с этим возникает необходимость в решении вопроса о хранении данных, отображающихся на веб-страницах и структуре ее организации.

Самый простой вариант – это создание индивидуальных html- файлов под каждую страницу контента, однако такой подход очень неудобен при работе с большим количеством информации. При изменении какого-либо общего элемента в изначальной структуре файлов возникают сложности с рациональным распределением сил разработчика, поскольку необходимо

будет менять каждый из файлов. Объем таких файлов может быть достаточно большим, поэтому обработка одним разработчиком не представляется возможной в короткие сроки.

С другой стороны, если вы хотите найти какой-то конкретный файл, то это будет очень сложно.

Но самым главным недостатком является непосредственная работа сайта заказчиками, которые сегодня являются людьми, далекими от программирования. В современном мире необходимость создания качественного сайта для представителей бизнеса, торговли и людей занимающихся предоставлением услуг, очень высока. Очень важно предоставлять актуальную информацию пользователям сайта для того чтобы повысить его репутацию и увеличить доходность. При необходимости внесения поправок, заказчик вряд ли сможет разобраться с программным кодом, и в нужный момент внести их на сайте.

Для решения этих проблем необходимо будет использовать более рациональный подход к разработке, который заключается в использовании баз данных. База данных (БД) – это программа, которая позволяет хранить и обработать информацию в структурированном виде.

Задача разработчика – создать общий файл с разметкой документа. Для всех страниц сайта он будет главным, а вся информация (текст, логические значения) страницы выводится в базу данных и в дальнейшем хранится в ней. При этом разделяется структура веб-страницы: разметка и содержание.

В своей сути БД представляют собой обычные таблицы, содержащие строки и столбцы с данными (рисунок 1). В частности, название хранится в колонке «Название», а в колонке «ТИП» задается форма отображения данных – «int» представляет собой цифровые величины, «varchar» - буквенные и т.д. Каждый элемент сайта хранится в отдельном поле ББ [2].

Обзор | Структура | SQL | Поиск | Вставить | Экспорт | Импорт | Операции

#	Имя	Тип	Сравнение	Атрибуты	Null	По умолчанию	Дополнительно	Действие
1	id	int(50)			Нет	Нем	AUTO_INCREMENT	Изменить Удалить
2	order	bigint(50)			Нет	Нем		Изменить Удалить
3	date port	datetime			Да	NULL		Изменить Удалить
4	customer	varchar(50)	utf8_unicode_ci		Да	NULL		Изменить Удалить
5	country	varchar(20)	utf8_unicode_ci		Да	NULL		Изменить Удалить
6	products	varchar(50)	utf8_unicode_ci		Да	NULL		Изменить Удалить
7	grade	varchar(50)	utf8_unicode_ci		Да	NULL		Изменить Удалить
8	size	float			Да	NULL		Изменить Удалить
9	length	varchar(100)	utf8_unicode_ci		Да	NULL		Изменить Удалить
10	quantity	int(20)			Да	NULL		Изменить Удалить
11	date	datetime			Да	NULL		Изменить Удалить
12	gruzo	varchar(100)	utf8_unicode_ci		Да	NULL		Изменить Удалить
13	id_rm	int(10)			Да	NULL		Изменить Удалить
14	id_file	int(11)			Да	NULL		Изменить Удалить

Рисунок 1 – Пример структуры программы PHPmyAdmin

Когда все содержимое размещено в базе данных, необходимо настроить веб-сервер - программное обеспечение, которое доставляет содержимое веб-страниц в браузер пользователя. Это делается для того, чтобы при посещении пользователем определенной веб-страницы он видел именно такую страницу в базе данных (Рисунок 2).

Например, пользователь вводит URL в поле поиска поисковой системы, соответствующий php-файл, обрабатывает запрос, обращается к базе данных и загружает ее на веб-сервер, отображая содержимое запрошенного файла, используя вызовы интерпретатора PHP для распознавания текста PHP. Последний, в свою очередь, создает на сервере скрипт и генерирует HTML-страницу. В этот момент страница передается в браузер клиента. Такая структура позволяет избежать проблемы хранения большого количества файлов на сервере.

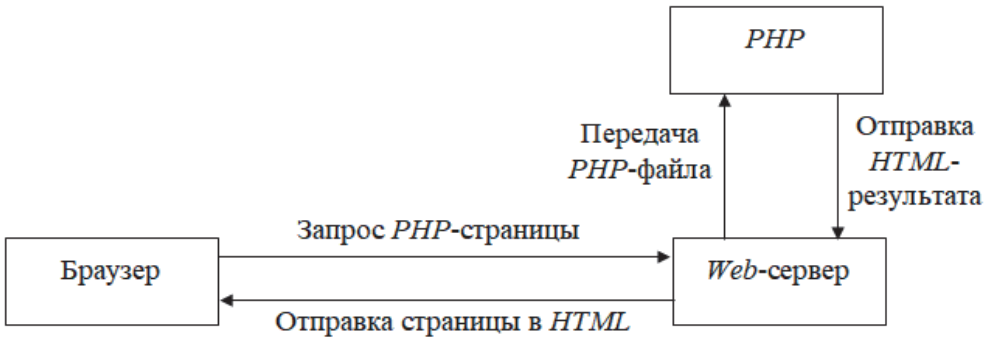


Рисунок 2 – Схема работы веб-сервиса

С точки зрения терминологии, "база данных" и "система управления базами данных" имеют разные значения. База данных - это информация и ее структура, а СУБД - это программа, которая позволяет внешним приложениям получать доступ к базе данных.

База данных MySQL - это бесплатная реляционная (реляционная база данных - это база данных, состоящая из таблиц) система управления базами данных. Его универсальность заключается в том, что он поддерживает большое количество типов таблиц. Например, полнотекстовые таблицы поиска или обработка транзакций на уровне записей. Он также стабилен, поддерживает множество операционных систем, не имеет проблем с локализацией и довольно прост в освоении. Это позволит вам максимально эффективно решать поставленные задачи и повысить производительность труда. Я являюсь разработчиком программы под названием "MySql". Система управления базами данных MySQLSql доступна на многих языках программирования, таких как Java, C, C++, Python, Rerl и PHP. Последний является наиболее часто используемым.

Это скриптовый язык общего назначения, используемый для разработки веб-приложений. Большинство хостинг-провайдеров предлагают

поддержку PHP, и это один из основных инструментов для создания веб-сайтов. Веб-приложение phpmyAdmin с открытым исходным кодом написано на PHP и представляет собой веб-интерфейс для управления системой управления базами данных MySQL. Он позволяет управлять сервером MySQL и выполнять команды SQL, а также просматривать содержимое таблиц и баз данных с помощью веб-браузера. Это приложение популярно среди веб-разработчиков, поскольку позволяет управлять MySQL без непосредственного ввода SQL-команд.

MySql - это система управления базами данных, которая прекрасно работает с PHP, и она оказала такое влияние на веб, что многие ресурсы используют ее для этих целей.

При разработке страниц с помощью HTML очень трудно заставить сайт выглядеть по-другому, и нет возможности выделить для этой деятельности специального разработчика. Однако этот язык не является достаточно гибким и динамичным, чтобы писать на нем веб-сайты. Благодаря сочетанию PHP и HTML можно создавать HTML-страницы с PHPS-скриптами, которые затем можно отправлять пользователям.

Язык PHP позволяет создавать и проектировать широкий спектр веб-сайтов, которые хорошо работают с базами данных, файловыми системами, хранилищами и электронной почтой.

Помимо этого, базы данных требуют специальных программ - СУБД - для организации способа хранения данных и обеспечения наиболее быстрого и эффективного доступа к ним. На сегодняшний день самой популярной, надежной и быстрой СУБД является Mysql (язык программирования PHP), который включает в себя язык PHPS. Лучшим приложением для работы с базами данных является phpMyAdmin, с помощью которого можно создавать, удалять или редактировать таблицы, а также изменять свойства пользователей. Такое сочетание обеспечивает оптимальную и комфортную среду для совместной работы разработчиков и веб-пользователей над данными.

Современные веб-приложения часто требуют обработки больших объемов данных. К ним относятся, например, различные автоматизированные информационные сервисы, веб-сайты и веб-приложения, социальные сети, мессенджеры и другое подобное программное обеспечение. Для того чтобы они работали должным образом, необходимо хранить большое количество различных данных. В большинстве случаев для решения этой проблемы используются системы управления базами данных (СУБД). Одной из самых популярных систем является реляционная система управления базами данных MySQL.На рисунке 3 представлен график популярности различных СУБД по состоянию на 2019 год, из которого видно, что на долю MySQL приходится 38,9% рынка.

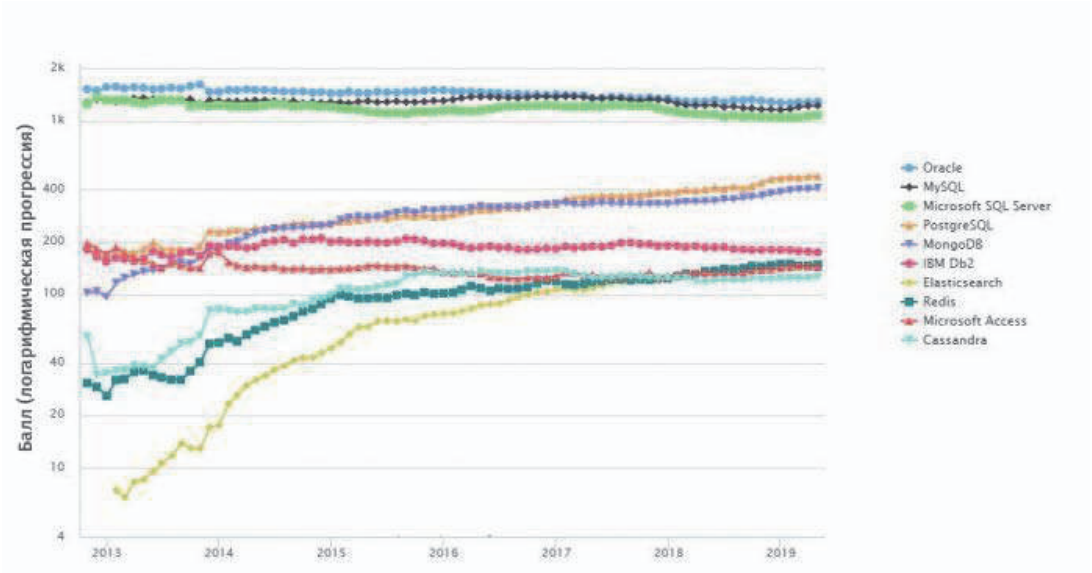


Рисунок 3 – Популярность различных СУБД

Исходя из этого, можно предположить, что большое количество веб-приложений в настоящее время используют MySQL в качестве хранилища данных. Эта база данных использует SQL-запросы для доступа к данным. SQL - это декларативный язык программирования для создания и изменения данных в реляционных базах данных, управляемых соответствующей системой управления базами данных. В первую очередь это язык информационной логики, предназначенный для описания и модификации данных, хранящихся в реляционной базе данных. Как правило, один и тот же набор данных часто запрашивается приложением. Если такой набор данных запрашивается регулярно, он сохраняет свою актуальность, поскольку СУБД не успевает вносить изменения в данные, но процесс извлечения данных приходится начинать заново при каждом новом запросе. Такой процесс можно значительно ускорить, используя инструменты кэширования данных.

Как правило, самыми проблемными запросами являются те, в которых используются операторы join, применяемые для объединения нескольких таблиц и различных вычислений. Пример такого запроса показан на рисунке 4.

```
SELECT DISTINCT `artist`.*, COUNT(distinct pls.playlist_id) AS `playlists`, COUNT(DISTINCT CASE
  WHEN FROM_UNIXTIME(pls.created_at, '%Y.%m.%d') = cend
      THEN pls.playlist_id END) ceplaylists, COUNT(DISTINCT CASE
    WHEN FROM_UNIXTIME(pls.created_at, '%Y.%m.%d') = cstart
    THEN pls.playlist_id END) csplaylists, COUNT(DISTINCT CASE
    WHEN pls.created_at BETWEEN 1604188800 AND 1606780800
    THEN pls.playlist_id END) psplaylists, ROUND(AVG(playlist_average_position)) playlist_average_position, ROUND(AVG(
    ceplaylist_average_position)) ceplaylist_average_position, ROUND(AVG(csplaylist_average_position)) csplaylist_average_position, ROUND(AVG(
    psplaylist_average_position)) psplaylist_average_position, csplaylist_average_position - ceplaylist_average_position
    cplaylist_average_position FROM `artist` INNER JOIN `artist_track` ON artist.id = artist_track.artist_id INNER JOIN (SELECT `artist_id` FROM
    `artist_country` WHERE `country` IN ('Украина', 'Россия', 'Беларусь', 'СССР', 'Азербайджан', 'Казахстан', 'Узбекистан', 'Грузия', 'Российская
    империя', 'Русское государство') GROUP BY `artist_id`) `artist_country` ON artist.id = artist_country.artist_id LEFT JOIN (SELECT
    `track`.`id` AS `trackId`, ROUND(AVG(position)) playlist_average_position, ROUND(AVG(DISTINCT CASE
            WHEN FROM_UNIXTIME(ytp.created_at,"%Y.%m.%d") = cend
                THEN position END)) ceplaylist_average_position, ROUND(AVG(DISTINCT CASE
            WHEN FROM_UNIXTIME(ytp.created_at,"%Y.%m.%d") = cstart
                THEN position END)) csplaylist_average_position, ROUND(AVG(DISTINCT CASE
            WHEN ytp.created_at BETWEEN 1604188800 AND 1606780800
                THEN position END)) psplaylist_average_position, `cend`, `cstart` FROM `yandex_track_playlist` `ytp` INNER JOIN `track` ON
                ytp.track_id = track.yandex_id INNER JOIN (SELECT `track`.`id` AS `trackId`, FROM_UNIXTIME(MAX(CASE WHEN ytp.created_at BETWEEN
                1606780800 AND 1609372800 THEN ytp.created_at END),"%Y.%m.%d") cend, FROM_UNIXTIME(MIN(CASE WHEN ytp.created_at BETWEEN
                1606780800 AND 1609372800 THEN ytp.created_at END),"%Y.%m.%d") cstart FROM `yandex_track_playlist` `ytp` INNER JOIN `track` ON
                ytp.track_id = track.yandex_id GROUP BY `track_id`) `info` ON track.id = info.trackId GROUP BY `track_id`) `plspos` ON
                artist_track.track_id = plspos.trackId WHERE `artist`.`yandex_id` IS NOT NULL GROUP BY `artist`.`id` ORDER BY `listens` DESC
```

Рисунок 4 – Пример проблемного запроса в MYSQL

Это связано с тем, что при текущей настройке СУБД выполнение данного запроса занимает более 30 секунд. Для ускорения этого типа запросов необходимо настроить кеширование на стороне СУБД. Главным достоинством данного метода является то, что он не требует внесения изменений в код приложения. Достаточно отредактировать конфигурационный файл mySQL, что занимает намного меньше времени. Это основной конфигурационный файл Ubuntu, расположенный в /etc/mysquad/mysql.conff.d и называется mysquad.conff. Этот файл необходимо отредактировать в разделе конфигурации кэша запросов, как это показано на рисунке 5.

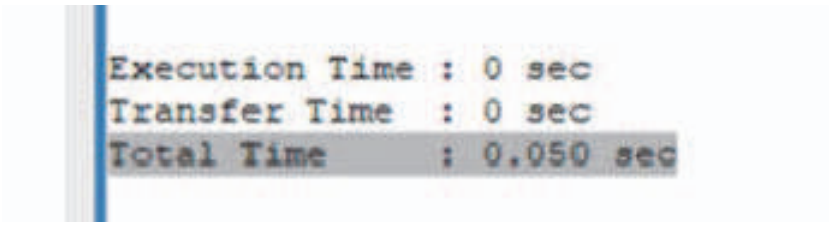


Рисунок 5 – Время выполнения запроса после активации кеширования

Так, например, для таких сложных запросов можно добиться разных улучшений производительности.

Основная часть статьи была посвящена способам повышения производительности сайтов. Особенное внимание уделяется использованию для этой цели кэш-памяти результатов запроса, который был получен на стороне СУБД. Так, с помощью этих инструментов можно добиться многократного повышения производительности при работе с сложными запросами, в которых используются операторы объединения или различные вычисления.

Такая работа может быть использована для разработки современных веб-приложений.

Литература

1. База данных. Реляционная база данных. — Текст: электронный // htmlacademy.ru: [сайт]. — Режим доступа: https://htmlacademy.ru/tutorial/php/databases (дата обращения: 14.02.2022).

2. Ченгаев, Дмитрий. Что такое база данных веб-сайта и зачем это нужно / Ченгаев Дмитрий. — Текст: электронный // webkyrs.info: [сайт]. — Режим доступа: https://webkyrs.info/page/chto-takoe-baza-dannykh-veb-saita-i-zachem-eto-nuzhno (дата обращения: 14.02.2022).

3. Цехановский, В. В. Управление данными: учебник / В. В. Цехановский, В. Д. Чертовской. — Санкт-Петербург: Лань, 2021. — 432 с. — ISBN 978-5-8114-1853-4. — Текст: электронный // Лань: электронно-

библиотечная система. — Режим доступа: https://e.lanbook.com/book/168835 (дата обращения: 14.02.2022). — Режим доступа: для авториз. пользователей.

4. Ульман, Л. MySQL / Л. Ульман. — Москва: ДМК Пресс, 2008. — 352 с. — ISBN 5-94074-229-7. — Текст: электронный // Лань: электронно-библиотечная система. — Режим доступа: https://e.lanbook.com/book/1241 (дата обращения: 14.02.2022). — Режим доступа: для авториз. пользователей.

5. PHP. — Текст: электронный // wikipedia.org: [сайт]. — Режим доступа: https://ru.wikipedia.org/wiki/PHP (дата обращения: 14.02.2022).

6. phpMyAdmin. — Текст: электронный // wikipedia.org: [сайт]. — Режим доступа: https://ru.wikipedia.org/wiki/PhpMyAdmin (дата обращения: 14.02.2022).

УПРАВЛЕНИЕ КАЧЕСТВОМ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ

Ибрагимова Анастасия Игоревна, магистрант 2 курса кафедры управления качеством и стандартизации
Научный руководитель: **Асташева Надежда Павловна**, д.б.н., профессор, профессор кафедры управления качеством и стандартизации

Дополнительное образование позволяет мотивировать детей на устойчивую потребность в познании и творчестве, а также самоопределиться профессионально и личностно. Технические виды спорта являются уникальным направлением творческой деятельности. Они соединяют в себе науку, технику, спорт, а также учат творчески мыслить, изобретать и применять полученные знания на практике. Отметим, что на сегодняшний день очень большое внимание уделяется технологической культуре. Она является своеобразным фундаментом для общей культуры, кроме того, лежит в основе развития современного общества и производства, и является его условием. Формы образовательного процесса, которые сегодня развиваются, дают нам толчок к изучению особенностей управления качеством образования.

Дополнительное образование, технологическая культура.

QUALITY MANAGEMENT OF ADDITIONAL EDUCATION

Ibragimova Anastasia, 2nd year graduate student of the Department of Quality management and standardization
Scientific adviser: **Astasheva Nadezhda**, Doctor of Biological sciences, Professor, Professor of the Department of Quality management and standardization

Additional education makes it possible to motivate children for a steady need for knowledge and creativity, as well as self-determination professionally and personally. Technical sports are a unique area of creative activity, they combine science, technology, sports, and also teach to think creatively and invent, to apply the acquired knowledge in practice.

It should be noted that today a lot of attention is paid to technological culture - it is a kind of foundation for a common culture, in addition, it underlies the development of modern society and production and it is its condition. The forms of the educational process that are being developed today give us an impetus to study the managing features of the quality of education.

Additional education, technological culture.

Система технологического образования только сейчас начала приобретать значение и является актуальной в данный момент. Наша исследовательская работа осуществляется на базе «Инженерно-

технологических классов», обучение в которых основывается на принципе технологического образования, где главной целью является развитие технической культуры.

Изучение процесса организации такого вида образования и система управления его качеством позволит нам выявить особенности и возможные ошибки образовательного процесса.

Для выявления причин, влияющих на качество образовательного процесса нами, была использована Диаграмма Исикавы.

Объектом нашего исследования являются дополнительные занятия – робототехника, ракетомоделирование и промдизайн, которые вливаются в общеобразовательный процесс.

Рисунок 1 – Диаграмма Исикавы «Качество дополнительных занятий»

На данной диаграмме (Рис.1) выделены 4 основных факторов, которые влияют на продуктивность и качество дополнительных занятий в системе «ИнжеТех».

Преподаватели – это важная часть в системе «ИнжеТех», от них зависит заинтересованность учеников, продуктивность и результаты проекта. В этом факторе мы выделили:

Опыт работы. Важен опыт работы с младшими школьниками и с группой, в которой 12 человек.

Мотивация. Одна из задач замотивировать преподавателей на развитие такого проекта как «ИнжеТех».

Личные качества. Очень важно, чтобы преподаватели обладали научной увлеченностью, глубокими познаниями в своей области преподавания, психологической подготовкой и многими другими умениями.

Процесс обучения – это фактор, который требует к себе наибольшего внимания и постоянной коррекции для улучшения качества. Были выделены следующие факторы:

Метод. Каждый модуль отличается своей направленностью и спецификой организации занятий. Важно обеспечить единство системы,

чтобы ученики могли полностью погрузиться в атмосферу технологического образования.

Мотивация учеников. Грамотный подход к системе мотивации позволит повысить успеваемость учеников. Должна быть обеспечена единая система мотивации в каждом модуле.

Измерения знаний. В системе дополнительного образования сложно оценивать результат учеников, но это необходимо для преподавателей и администрации. Внедрение системы оценивания позволит корректировать процесс обучения.

Менеджмент – грамотное расписание занятий и формирования групп серьезно влияет на продуктивность и качество получаемых знаний.

Расписания занятий. Расписание занятий, которое было на момент исследования являлось не оптимальным на наш взгляд.

время	класс	группа	пятница 2 апр	понедельн 5 апр	пятница 9 апр	понедельн 12 апр	пятница 16 апр	понедельн 19 апр	пятница 23 апр	понедельн 26 апр	пятница 30 апр	понедельн 3 май	пятница 7 май	понедельн 10 май	пятница 14 май	понедельн 17 май	пятница 21 май
9.25 - 10.10	1 "И"	группа 1 "Космики"	Ракетомоде	LEGO-маст	Ракетомоде	LEGO-маст	Ракетомоде	LEGO-маст	Ракетомоде	LEGO-маст	Ракетомоде	Выходной	LEGO-маст	Выходной	Ракетомоде	LEGO-маст	Ракетомоде
		группа 2 "Звездочки"	LEGO-маст	Ракетомоде	LEGO-маст	Ракетомоде	LEGO-маст	Ракетомоде	LEGO-маст	Ракетомоде	LEGO-маст	Выходной	Ракетомоде	Выходной	LEGO-маст	Ракетомоде	LEGO-маст
10.20 - 11.05	2 "И"	группа 1 (Старцев Е.)	Ракетомоде	LEGO-маст	LEGO-маст	Ракетомоде	Промдизай	LEGO-маст	Ракетомоде	Ракетомоде	Промдизай	Выходной	LEGO-маст	Выходной	Промдизай	LEGO-маст	Ракетомоде
		группа 2 (Сергунов Н.)	LEGO-маст	Ракетомоде	Промдизай	LEGO-маст	LEGO-маст	Ракетомоде	Промдизай	LEGO-маст	Ракетомоде	Выходной	Промдизай	Выходной	LEGO-маст	Ракетомоде	Промдизай
11.20-12.05	3 "И"	группа 1	Ракетомоде	LEGO-маст	LEGO-маст	Ракетомоде	Промдизай	LEGO-маст	Ракетомоде	Ракетомоде	Промдизай	Выходной	LEGO-маст	Выходной	Промдизай	LEGO-маст	Ракетомоде
		группа 2	LEGO-маст	Ракетомоде	Промдизай	LEGO-маст	LEGO-маст	Ракетомоде	Промдизай	LEGO-маст	Ракетомоде	Выходной	Промдизай	Выходной	LEGO-маст	Ракетомоде	Промдизай

Рисунок 2 – Расписание дополнительных занятий «ИнжеТех» апрель-май 2021 г.

Исходя из представленного расписания (Рисунок 2) мы можем сделать выводы, что занятие длится 45 минут. В системе дополнительного образования, где присутствует творческая деятельность требуется больше времени. Так как занятие условно можно разделить на изучение новой темы подготовку рабочего места, основную работу и уборку рабочего места. А также требуется настрой и фокусировка обучающегося на занятие

Формирование групп. В 2020-2021 году формирование групп представляло собой очень сложную систему. Один из важных факторов, это деление класса пополам, так как для продуктивности очень важен индивидуальный подход преподавателя к каждому ребенку. Группы менялись каждую неделю между собой. Когда одна группа детей уходила на занятие по «Ракетомоделированию», то вторая уходила на «Lego» или «Промдизайн» очень часто группы путались между собой и на занятия попадали второй раз подряд. И конечно один из важных факторов дети успевали забыть изученный материал, так как попадали на занятия модуля

один раз в неделю. Для детей младшего школьного возраста сложно переключаться с одного модуля на другой и проявлять себя в каждом из них в полной мере.

Люди – данный фактор несет под собой коммуникативный аспект. Были выделены следующие элементы:

Администрация – это единственный орган, который курирует работу преподавателей и несет полное обеспечение деятельности. В данном случае очень важно обеспечить постоянное взаимодействие администрации и преподавателей.

Родители – это заказчики, которые должны видеть результат работы с их детьми. Исходя из этого возникает потребность в информировании родителей об успехах и сложностях, возникших на занятиях.

Исходя из этого анализа были предложены следующие рекомендации.

Для единства занятий и качественного проведения урока было принято решение, что каждый урок будет сопровождаться презентацией по теме урока. Это позволит окрасить урок яркими картинками по теме урока, а также решить ряд других задач. Например, в каждой презентации должны присутствовать не только слайды по теме урока, но и слайды, которые включают детей в урок до начала изучения новой темы:

1. Обсуждение правил поведения в начале урока позволят преподавателю задать серьезный тон на занятие и систематизировать некоторые аспекты. А яркая картинка быстрее отложится в памяти у детей (Рисунок 3).

Рисунок 3 – Правила на уроке «ИнжеТех»

2. Система мотивации с ее критериями. Напоминание о системе мотивации в начале урока позволит детям позитивно настроится на занятие, и сосредоточится на продуктивной работе (Рисунок 4).

Рисунок 4 – Система мотивации учеников «ИнжеТех»

3. Тренировка мозга. Данная часть урока представляет собой различные упражнения на активизацию внимания, логики, восприятия и т.д. Упражнения подбираются по возрасту и при возможности по специфики модуля. Такие упражнения помогают настроить ребят на работу. На рисунке 5 изображено задание для первого класса, подразумевавшие развитие логического мышления. В данном упражнении ребятам нужно исключить лишний предмет в каждом ряду.

Рисунок 5 – Упражнение на развитие логического мышления для первого класса

4. Основную часть занятия составляет тема урока, которая также сопровождается визуальным оформлением. Например, на рисунке 6

представлен один из слайдов на тему «Построение одноступенчатой модели ракеты без двигателя» - модуль «Ракетомоделирование». В данной теме пошагово описано и визуализировано построение ракеты, на представленном сладе показано как склеивать стабилизатор ракеты. Несомненно, все визуализированное сопровождается комментариями преподавателя и вниманием к каждому ученику в процессе выполнения задания.

Рисунок 6 – Слайд из презентации на тему урока «Построение одноступенчатой модели ракеты без двигателя»

5. Заключительным этапом является рефлексия, где ученики с преподавателем обсуждают вопросы, представленные на рисунке 7.

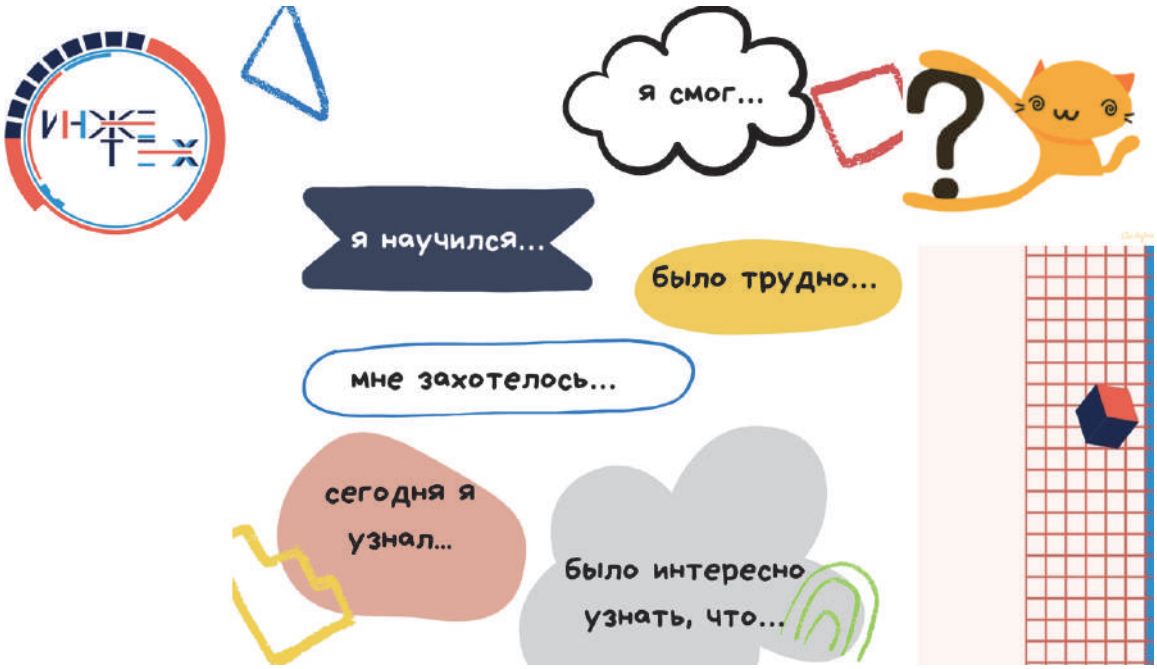


Рисунок 7 – Заключительный слайд из презентации для занятий в школе «ИнжеТех»

Для мотивации учеников рекомендована единая система, которая должна использоваться в преподавании каждого модуля. Это позволит ученикам не путаться в разных системах поощрения и наказания у каждого из преподавателей, что положит начало эффективности предложенной системы. Представленная система подразумевает сбор наклеек за урок без замечаний, и тот ученик, который соберет наибольшее количество за пройденный модуль получит ценный приз. Критерии оценки для выдачи наклейки подразумевают два аспекта:

1. *Поведение на уроке.* Сюда мы относим соблюдение тех правил, которые оговариваются в начале урока.
2. *Выполнение задания*. В данном аспекте оценивается старание, аккуратность, интерес ученика в процессе выполнения заданий. Очень важно на данном этапе преподавателю суметь объективно оценить стремление или нежелание.

Если ученик получил несколько замечаний, необходимо это пометить в журнале. Мы должны быть честны со своими учениками и поэтому система, оценивая поведения должна быть прозрачной. В конце урока преподаватель наклеивает наклейки на специальный лист, который постоянно висит на доске. Если ученик отзанимался без замечаний он получает наклейку с эмблемой «ИнжеТех», если же у ученика есть замечания, то преподаватель озвучивает их и клеит наклейку с вопросительным знаком. Задача учеников набрать как можно больше наклеек с эмблемой.

№	ФИО	Урок 1	Урок 2	Урок 3	Урок 4	Урок 5	Урок 6	Урок 7	Урок 8	Урок 9	Урок 10	Урок 11	Урок 12	Урок 13	Урок 14	Урок 15	Урок 16
1.	А. А.																
2.	Б. А.																
3.	В. А.																
4.	В. С.																
5.	Д. М.																
6.	Е. Н.																
7.	К. С.																
8.	К. А.																
9.	Ш. К.																
10.	Ш. С.																
11.	Ш. С.																

Рисунок 8 – Лист для системы мотивации учеников «ИнжеТех»

Для измерения знаний, мы предлагаем внести систему оценивания в каждом модуле самим преподавателем. Так как преподаватель точно знает, как можно оценить знания, полученные в их модуле. А по итогу пройденной программы проанализировать и сделать выводы.

Один из важных моментов в корректировке является расписание занятий. Так как прежнее расписание не удовлетворяло все запросы, было предложено скорректировать его следующим образом.

У 2, 3, 4 класса занятие длится 2 урока, это позволит полноценно охватить тему урока.

Модули «Лего-Мастер» и «Ракетомоделист»:

- в 1 «И» классе занятия в группе 12 человек, по одному уроку в понедельник и пятницу, 2 раза в неделю;
- во 2, 3 и 4 «И» классах – занятия в группе до 12 человек, спаренные уроки, 1 раз в неделю.

Модуль «Азбука дизайна»: **класс полный**, 1 урок каждую неделю.

Таблица 1 – График занятий обучающихся инженерно-технологических классов «ИнжеТех»

<table>
<tr><th>Время уроков</th><th>понедельник</th><th>вторник</th><th>среда</th><th>четверг</th><th>пятница</th></tr>
<tr><td>8.30 – 9.15</td><td>-</td><td>-</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>9.25 – 10.10</td><td rowspan="2">2 класс:
Лего-Мастер (1 гр.) /Ракетомоделист (2 гр.)</td><td rowspan="2">3 класс:
Лего-Мастер (1 гр.) /Ракетомоделист (2 гр.)</td><td>-</td><td>-</td><td rowspan="2">4 класс:
Лего-Мастер (1 гр.) /Ракетомоделист (2 гр.)</td></tr>
<tr><td>10.20 – 11.05</td><td>-</td><td>2 класс (полный класс)
«Азбука дизайна»</td></tr>
<tr><td>11.20 – 12.05</td><td>1 класс:
Лего-Мастер (1 гр.) /Ракетомоделист (2 гр.)</td><td>-</td><td>-</td><td>3 класс (полный класс)
«Азбука дизайна»</td><td>1 класс:
Лего-Мастер (1 гр.) /Ракетомоделист (2 гр.)</td></tr>
<tr><td>12.15 – 13.00</td><td>-</td><td>-</td><td>-</td><td>4 класс (полный класс)
«Азбука дизайна»</td><td>-</td></tr>
</table>

Изменения коснулись и формирования групп. Было принято решение, что пока одна группа не закончит обучение одного модуля она не переходить к освоению следующего модуля. Первое полугодие группа посещает модуль «Лего-Мастер», а второе полугодие модуль «Ракетомоделист».

Такое решение позволит полностью погрузиться ученикам в один из модулей и полученные знания не перемешаются между собой.

Для продуктивного взаимодействия администрации и преподавателей рекомендовано организовывать собрания не реже одного раза в месяц. Это позволит оперативно обсудить возникшие проблемы и вопросы.

Информирование родителей, как способ включения в образовательный процесс. Предполагается внедрить краткий отчет после каждого занятия, из которого родители будут иметь представление о успехах детей. Такое информирование может осуществляться в чате класса и сопровождаться фотографиями с занятий.

Литература

1. Ефимов, В. В. Средства и методы управления качеством: учебное пособие [Текст] / В.В. Ефимов. — М. : КНОРУС, 2014. — 232 с.

2. Коротков, Э. М. Управление качеством образования [Текст] : учеб. пособие для вузов / Э. М. Коротков. - 2-е изд. - М. : Акад. Проект, 2007. – 317с.

ХАРАКТЕРИСТИКИ ОБСЛУЖИВАНИЯ ПРИЁМА ПОТОКА ДАННЫХ НА ЛОКАЛЬНУЮ СЕТЬ ФИРМЫ НА ПРИМЕРЕ МНОГОКАНАЛЬНОЙ СМО С НЕОГРАНИЧЕННОЙ ОЧЕРЕДЬЮ В ПРОГРАММЕ «SMATH STUDIO»

Каримов Наиль Анварович, Зиненко Андрей Игоревич, магистранты 2 курса кафедры информационных технологий и управляющих систем
Научный руководитель: **Логачева Надежда Вадимовна,** к.т.н., доцент кафедры информационных технологий и управляющих систем

Система массового обслуживания (СМО) — это система, которая производит обслуживание поступающих в неё требований из любой отрасли и системы, как с ограниченной очередью, так и с неограниченной очередью. В данной статье будет рассмотрено многоканальное СМО с неограниченной очередью для приёма потока данных. Обработка данных ведётся по очерёдно и данные поступают без ограничений.

Локальная сеть, SMath Studio, методы, сети, поток данных, СМО.

CHARACTERISTICS OF THE SERVICE OF RECEIVING A DATA STREAM ON THE COMPANY'S LOCAL NETWORK ON THE EXAMPLE OF A MULTI-CHANNEL QUEUING SYSTEM WITH AN UNLIMITED QUEUE IN THE SMATH STUDIO PROGRAM

Zinenko Andrey, **Karimov Nail,** 2nd year graduate students of the Department of Information technologies and control systems
Scientific adviser: **Logacheva Nadezhda,** Candidate of Technical sciences, Associate professor of the Department of Information technologies and control systems

A queuing system (QS) is a system that services incoming requests from any industry and system, both with a limited queue and with an unlimited queue. This article will consider a multi-channel QS with an unlimited queue for receiving a data stream. Data processing is carried out one by one and the data is received without restrictions.

The local network, SMath Studio, methods, networks, data stream, Queuing System (CMO).

СМО – как аббревиатура расшифровывается как Система Массового Обслуживания. То есть, это система, которая производит обслуживание поступающих в неё требований неважно какой отрасли. Обслуживание требований в СМО осуществляется специальными обслуживающими

приборами. Классическая СМО содержит от 1 до бесконечного числа приборов.

В зависимости от наличия возможности ожидания поступающими требованиями начала обслуживания СМО делятся на:

- системы с потерями, в которых требования, не нашедшие в момент поступления ни одного свободного прибора, теряются;
- системы с ожиданием, в которых имеется накопитель бесконечной ёмкости для буферизации поступивших требований, при этом ожидающие требования образуют очередь;
- системы с накопителем конечной ёмкости (ожиданием и ограничениями), в которых длина очереди не может превышать ёмкости накопителя; при этом требование, поступающее в переполненную СМО (отсутствуют свободные места для ожидания), теряется [1].

Основные понятия в СМО следующие: это требование, то есть заявка - запрос на обслуживание, далее это входящий поток требований - совокупность требований, поступающих в СМО, затем идёт время обслуживания - это период времени, в течение которого обслуживается требование и математическая модель СМО - это совокупность математических выражений, описывающих входящий поток требований, процесс обслуживания и их взаимосвязь.

СМО можно разделить на следующие категории и классификации:

По числу обслуживающих каналов:

Одноканальные СМО - СМО с одним каналом обслуживания.

Многоканальные СМО - СМО с несколькими каналами обслуживания.

По времени пребывания требований в очереди до начала обслуживания:

СМО с отказами — это СМО, в которой заявка, поступающая в момент, когда все каналы заняты, получает отказ, покидает СМО и в дальнейшем в процессе обслуживания не участвует.

СМО с ожиданиями (очередью) — это СМО, в которой заявка, пришедшая в момент, когда все каналы заняты, не уходит, а становится в очередь на обслуживание. В свою очередь СМО с ожиданием (очередью) подразделяются на: СМО с ограниченной очередью; СМО с неограниченной очередью; СМО с ограниченным временем ожидания; СМО с неограниченным временем ожидания.

По приоритетности обслуживания:

СМО со статистическим приоритетом.

СМО с относительным приоритетом.

СМО с абсолютным приоритетом.

СМО со смешанным приоритетом.

По принципу обслуживания:

СМО с обслуживанием по принципу "первый пришел - последний обслужен" (например, СМО с обслуживанием по принципу "первый пришел - последний обслужен").

СМО с обслуживанием по принципу "первый пришел - последний обслужен".

В зависимости от способа генерации заявок:

Открытые СМО — это СМО, где циркулирует конечное, обычно постоянное количество требований, которые после завершения обслуживания возвращаются в источник.

Замкнутые СМО — это СМО, где источник генерирует бесконечное число требований [1].

После изучений типов и видов СМО, а также их подгрупп среди множества выбора типажей СМО в данной статье выбор был сделан в пользу многоканального СМО с неограниченной очередью. Так как данная СМО отлично подходит под выбранную тему. Потому что характеристики обслуживания приёма потока данных в сетях, в частности, уже на определённых компьютерах измеряются в неограниченной очереди, так как заранее спрогнозировать количество информации и потока данных на один рабочий компьютер, скажем, директора фирмы или компании за день практически невозможно. Из краткой теории про систему массового обслуживания можно заметить почему она так называется: пусть в n-канальную систему массового обслуживания (СМО) поступает с интенсивностью простейший поток требований. Длительность обслуживания распределена по показательному закону со средним временем обслуживания. Если же все каналы обслуживания заняты, то вновь поступившее требование становится в очередь за ранее поступившими не обслуженными требованиями. Освободившийся канал приступает к обслуживанию очередного требования из очереди. Так как число требований, стоящих в очереди, может быть бесконечно большим, то и число состояний системы также может быть бесконечно большим. Схематично данная теория изображена на рисунке 1 [2]:

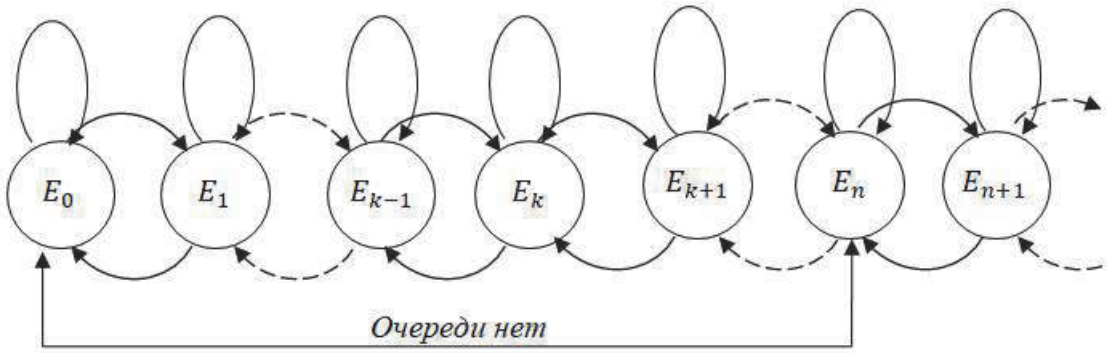


Рисунок 1 – Многоканальная СМО с неограниченной очередью

Для постановки определённой задачи возьмём случайную фирму А для примера в рассмотрении данной статьи. В данной фирме работают 3 главных сотрудника, для примера, директор, главный бухгалтер и финансист. Приём потока данных на локальную сеть фирмы образует простейший поток требований с интенсивностью 90, условно, писем / заказов в час. Интенсивность обслуживания одного компьютера составляет 60 человек в час. Необходимо найти характеристики обслуживания локальной сети.

При подготовке к решению задачи рассмотрим n-канальную систему массового обслуживания с неограниченной очередью, в которую поступает простейший поток заявок с интенсивностью λ; интенсивность обслуживания μ, т.е. в среднем непрерывно занятый канал будет выдавать p= λ/μ обслуженных заявок в единицу времени.

Здесь, длительность обслуживания – это случайная величина, подчиненная показательному закону распределения. А поток обслуживания является простейшим пуассоновским потоком событий. Заявка, поступившая в момент, когда все n каналов заняты, становится в очередь и ожидает обслуживания по теории СМО с неограниченной очередью [3].

В качестве показателей эффективности многоканальной СМО с неограниченной длиной очереди будем рассматривать следующие значения, которые будут встречаться в решении задач, это:

A - абсолютная пропускная способность СМО;

Q - относительная пропускная способность;

$P_{ОТК}$ - вероятность отказа;

$P_{Оч}$ - вероятность образования очереди;

$K_{ЗАН}$ - среднее число занятых каналов;

$L_{СИСТ}$ - среднее число находящихся в системе заявок;

$T_{СИСТ}$ - среднее время пребывания заявки в системе;

$L_{Оч}$ - средняя длина очереди;

$T_{Оч}$ - среднее время ожидания в очереди [1].

Размеченный граф состояний неограниченной очереди представлен на рисунке 2 [3]:

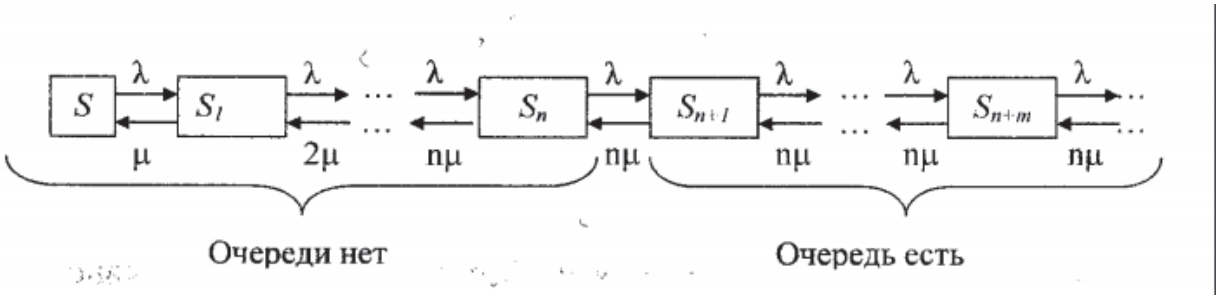


Рисунок 2 – Граф очереди в многоканальной СМО

По этому графу видно, где есть очередь, а где её нет. По условным обозначениям, представленным на рисунке 2, можно сказать следующее:

S_0 - все каналы свободны, k = 0;
S_1 - занят один канал, остальные свободны, k = 1;
S_n - заняты все n каналов, очереди нет, k = n;
S_{n+1} - заняты все n каналов, одна заявка в очереди k = n + 1;
S_{n+m} - заняты все n каналов, r заявок в очереди, k = n + m;

Далее известно, что поскольку ограничение на длину очереди отсутствует, то любая заявка может быть обслужена, поэтому $P_{обс} = 1$, следовательно, относительная пропускная способность $Q = P_{обс} = 1 \Rightarrow P_{отк} = 0$, а абсолютная пропускная способность $A = \lambda Q = \lambda$ [3].

Предельные вероятности высчитываются по формулам: [4]

$$P_0 = \left(1 + \frac{p}{1!} + \frac{P^2}{2!} + \cdots + \frac{p^{n-1}}{(n-1)!} + \frac{P^n}{n!} \cdot \frac{1}{n-p}\right)^{-1};$$

$P_1 = pp_0$, $P_2 = \frac{P^2}{2!}$, P_0, … , $p_n = \frac{P^n}{n!} P_0$

Вероятность образования очереди:

$$p_{оч} = \frac{p^{n+1}}{n!\,(n-p)} Po$$

Среднее число занятых каналов:

$K_{ЗАН} = A / \mu$

Средняя длина очереди:

$$L_{оч} = \frac{p^{n+1}}{nn!\left(1 - \frac{p}{n}\right)^2} \cdot p_0$$

Среднее время ожидания в очереди:

$$T_{оч} = \frac{E_{оч}}{\lambda}$$

Среднее число заявок в системе:

$L_{СИСТ} = L_{оч} + p$

Среднее время пребывания заявки в СМО:

$$T_{СИСТ} = \frac{L_{СИСТ}}{\lambda}$$

Если p < n, то процесс обслуживания устойчив. Если p > n следовательно СМО работает неустойчиво [4].

По ходу решения следует, что

$p = \frac{\lambda}{\mu} = \frac{60}{30} = 2$ – вбиваем значение альфа и бета – и получаем ответ 2. По условию p<n, следовательно, очередь не будет возрастать до бесконечности и в системе наступает предельный стационарный режим работы (см. рисунок 3).

Для начала найдём вероятность того, что компьютер не получает данные совсем, то есть $P_0 = 0{,}111$ (см. рисунок 4).

После этого сделаем такой же шаг, только на этот раз найдём вероятность того, что в компьютере одновременно обслуживаются в одно время один, два или три потока данных. Возьмём, к примеру, 5 информативных данных в обслуживании и высчитаем вероятность каждого случая от p_1 до p_5 и выходят значения в 0,222; 0,222; 0,148; 0,0987; 0,0658 соответственно (см. рисунок 5).

Далее находим значение вероятности того, что заявка окажется в очереди и определяем её по формуле: $p_{\text{оч}} = \frac{p^{n+1}}{n!(n-p)} Po$ и получаем значение в 0,296, следом высчитываем среднее число занятых компьютеров по формуле: $K_{\text{ЗАН}} = A / \mu$ и получаем ответ 2 (см. рисунок 6).

Затем по формуле $L_{\text{Оч}} = \frac{p^{n+1}}{nn!\left(1-\frac{p}{n}\right)^2} \cdot p_0$ определяем среднее число потока данных в очереди и получаем ответ в 0,888. Расчёт и график представлен на рисунке 7.

Среднее число данных, обслуживаемых компьютерами и стоящих в очереди в одно время равно ~ 2,888 письма – определяется по формуле: $L_{\text{СИСТ}} = L_{\text{Оч}} + p$. На рисунке 8 представлено подробное описание.

На заключительном этапе высчитывается среднее время пребывания заявки в очереди и среднее время пребывания заявки в системе. На рисунке 9 представлен график и расчёты среднего времени пребывания заявки в очереди, что равно 0,0148 и рассчитывалась по формуле: $T_{\text{Оч}} = \frac{E_{\text{Оч}}}{\lambda}$. А на рисунке 10 показаны расчёты и график среднего времени пребывания заявки в системе = 0,0481. Данное значение появилось благодаря формуле $T_{\text{СИСТ}} = \frac{L_{\text{СИСТ}}}{\lambda}$ [5].

Далее будут продемонстрированы скриншоты программы SMath Studio версии 0.99.7822 [6], где изображены решения данной задачи, а также некоторые графики. Про описание следующих рисунков было сказано выше настоящей статьи.

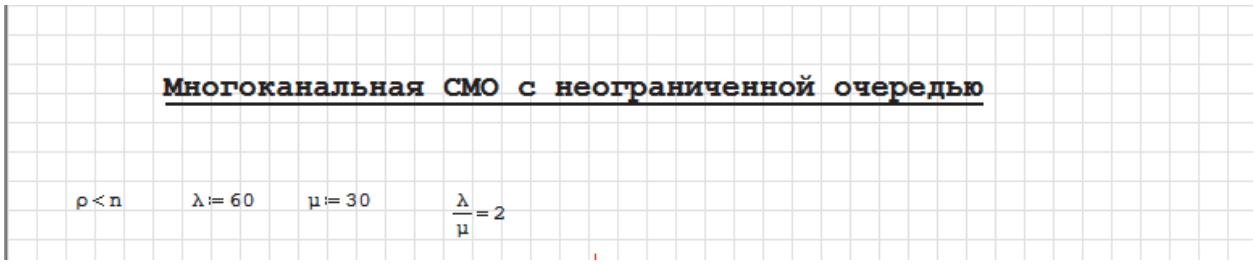


Рисунок 3 – Данные задания

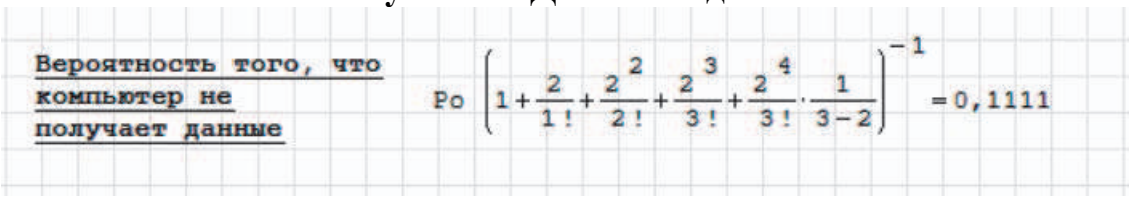


Рисунок 4 – Определение вероятности того, что компьютер не получает данные

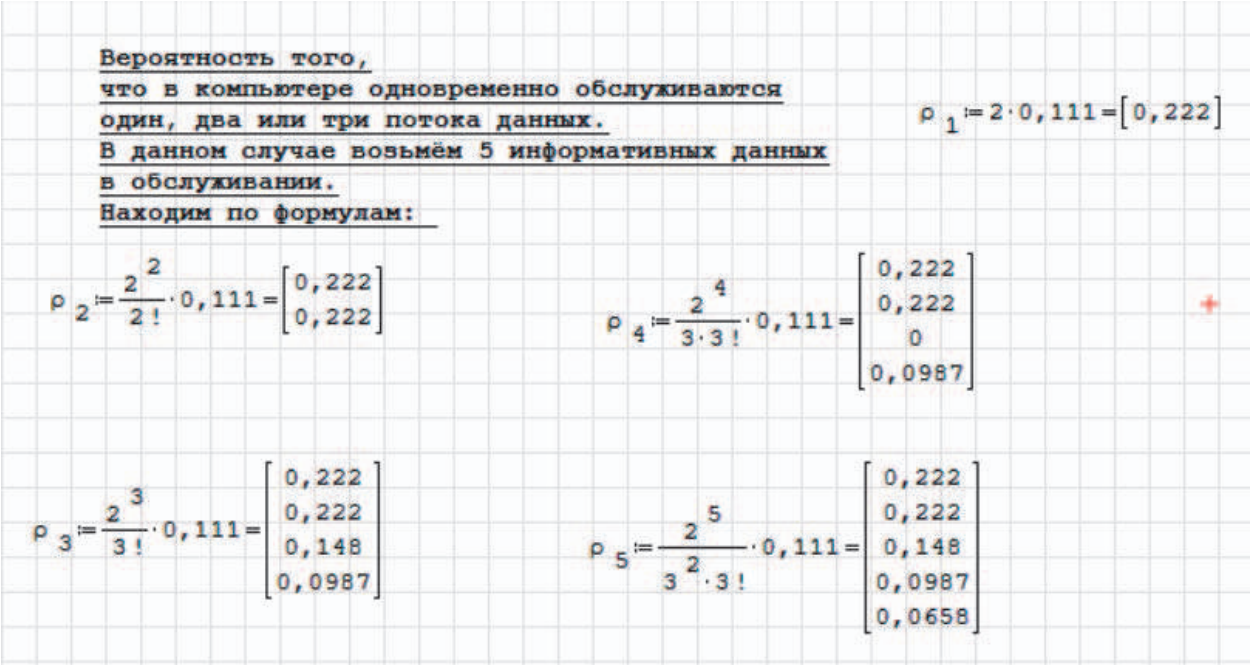


Рисунок 5 – Вероятность того, что компьютер получил 5 информативных данных

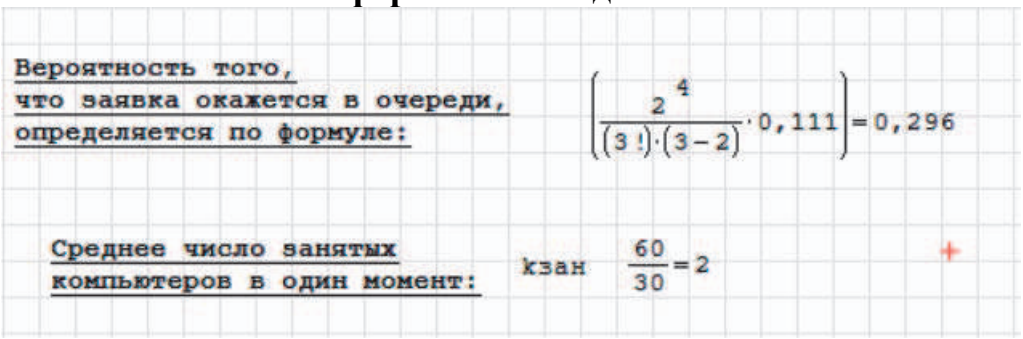


Рисунок 6 – Вероятность того, что заявка в очереди и число занятых компьютеров

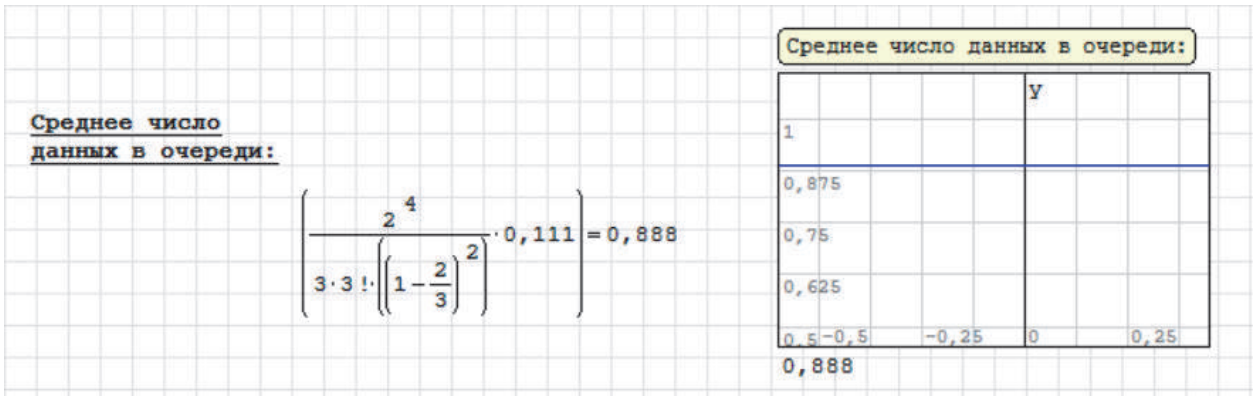


Рисунок 7 – Среднее число данных в очереди

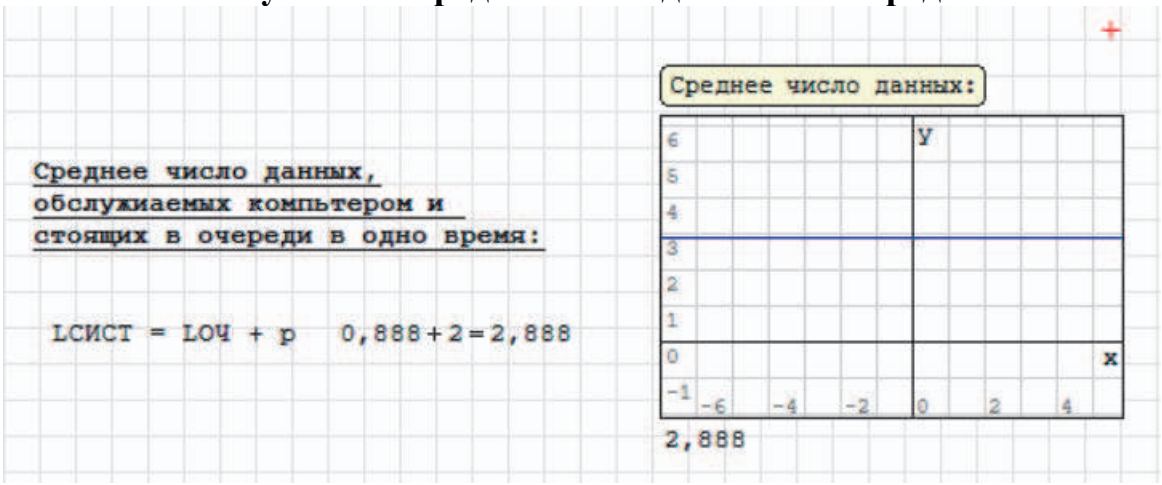


Рисунок 8 – Среднее число данных

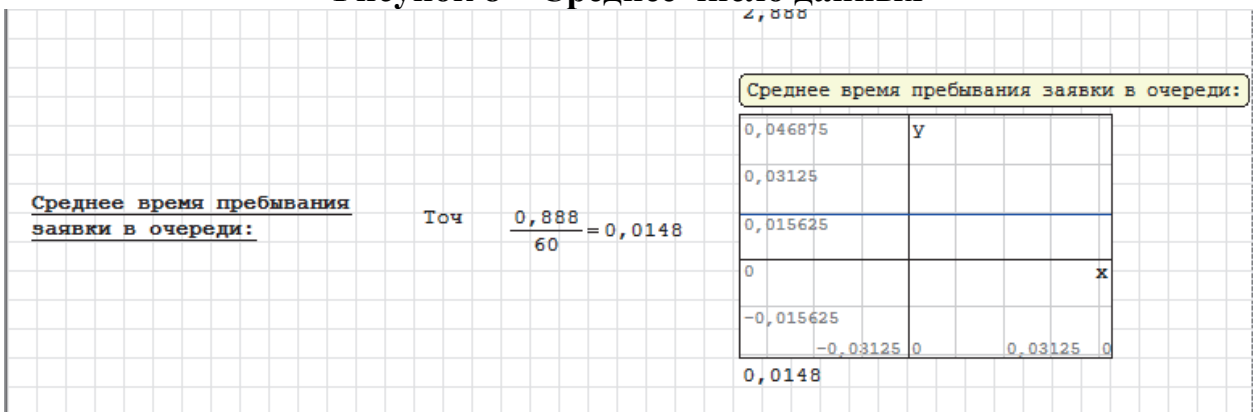


Рисунок 9 – Среднее время пребывания заявки в очереди

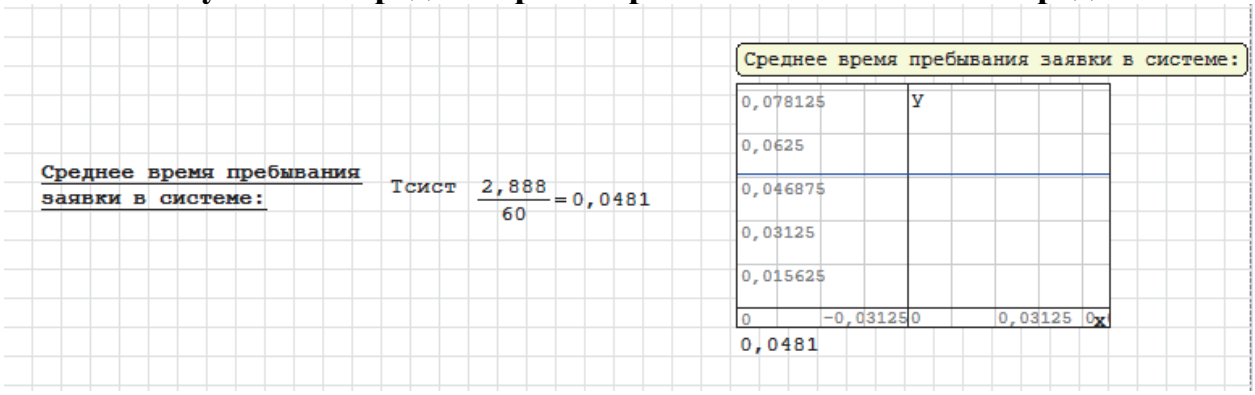


Рисунок 10 – Среднее время пребывания заявки в системе

Заключение

В данной работе был произведен сравнительный анализ типов систем массового обслуживания и был сделан выбор в пользу многоканального СМО с неограниченной очередью. Также, был описан выбор данного СМО и краткая теория с книги о том, что такое СМО [5].

После этого была поставлена задача для решения в данной работе, где было необходимо найти характеристики обслуживаний компьютеров в некотором офисе, что было сделано. В работе представлены формулы, по которым решалась данная задача, а также подробный отчёт в виде скриншотов о ходе работы. Данная задача была решена и результат достигнут

Литература

1. Н.В. Кошуняева, Н.Н. Патронова Теория массового обслуживания (практикум по решению задач) // Учебно-методическое пособие // 2013. - 110с. / С. 16-18. Режим доступа: https://docplayer.com/26536357-Teoriya-massovogo-obsluzhivaniya-praktikum-po-resheniyu-zadach-9-40-7-l.html#show_full_text (дата обращения 23.02.2022)

2. Методы оптимальных решений - задачи с решением. решение задач линейного программирования и других моделей // Многоканальная СМО с неограниченной очередью // С. 6. Режим доступа: https://100task.ru/sample/97.aspx (дата обращения 22.02.2022).

3. Осипов Г.С. Научная электронная библиотека // Многоканальные СМО с ожиданием // Математическое и имитационное моделирование систем массового обслуживания. 2017. С. 17. Режим доступа: https://monographies.ru/ru/book/section?id=13537 (дата обращения 22.02.2022).

4. Лаврусь О.Е., Миронов Ф.С. Теория массового обслуживания. Методические указания, учебная программа и задания для контрольных работ № 1, 2 для студентов заочной формы обучения специальности 071900 “Информационные системы в технике и технологиях”. - Самара: СамГАПС, 2002.- 38с. / С. 24 Режим доступа: http://window.edu.ru/resource/208/29208/files/samiit225.pdf (дата обращения 22.02.2022)

5. Романенко Владимир Алексеевич Оптимизация управления технологическими процессами узлового аэропорта как системы массового обслуживания с нестационарными потоками и частичной взаимопомощью каналов // УБС. 2012. №36. Режим доступа: https://cyberleninka.ru/article/n/optimizatsiya-upravleniya tehnologicheskimi-protsessami-uzlovogo-aeroporta-kak-sistemy-massovogo-obsluzhivaniya-s-nestatsionarnymi (дата обращения: 23.02.2022).

6. Программа Smath Studio / версия 0.99.7822 - Стабильная (опубликовано 2021-06-01) // Режим доступа: https://ru.smath.com/обзор/SMathStudio/резюме (дата обращения 21.02.2022)

ПЕРСПЕКТИВНЫЕ ТУГОПЛАВКИЕ КОМПОНЕНТЫ ДЛЯ УЛУЧШЕНИЯ КЕРАМИЧЕСКОЙ СОСТАВЛЯЮЩЕЙ МАТРИЦЫ КОМПОЗИЦИОННЫХ МАТЕРИАЛОВ

Козлова Мария Александровна, магистрант 1 курса кафедры управления качеством и стандартизации
Научный руководитель: **Воейко Ольга Александровна**, к.т.н., доцент, заведующий кафедрой управления качеством и стандартизации

Существующие высокотемпературные конструкционные материалы (например, МКУ4М-7-СМС (ТУ 1916-515-56897835-2011) и УККМ марки КМК-МС (ТУ 1916-449-56897835-2003) состава C/SiC) не могут обеспечить работоспособность теплонагруженных деталей конструкции ЛА во всем интервале температур (до 2700°С), возникающих в полете. Начиная с температуры 1850 °С указанные композиты показывают значительную потерю массы и линейный унос, не позволяющие создавать из них детали и узлы ЛА. Поэтому актуальна разработка новых материалов с бóльшей температурой работоспособности в окислительных средах.

Композиционный материал, высокотемпературные материалы, тугоплавкие компоненты, ультравысокотемпературная керамика.

PROMISING REFRACTORY COMPONENTS FOR IMPROVING THE CERAMIC COMPONENT OF THE MATRIX OF COMPOSITE MATERIALS

Kozlova Maria, 1st year graduate student of the Department of Quality management and standardization
Scientific adviser: **Voeyko Olga**, Candidate of Technical sciences, Associate professor, Head of the Department of Quality management and standardization

Existing high-temperature structural materials (for example, MKU4M-7-SMS (TU 1916-515-56897835-2011) and UKKM brand KMK-MS (TU1916-449-56897835-2003) composition C/SiC) cannot ensure the performance of heat-loaded structural parts Aircraft in the entire temperature range (up to 2700 □) arising in flight/ Starting from a temperature of 1850 □, these composites show a significant weight loss and linear carryover, which does not allow the creation of aircraft parts and assemblies from them. Therefore, the development of new materials with a higher working temperature in oxidizing environments is relevant.

Composite material, high-temperature materials, refractory components, ultra-high temperature ceramics.

Наиболее перспективными материалами для создания несущих конструкций, обладающих повышенной окислительной стойкостью, применяемых в ракетно-космической и авиационной технике являются углерод–керамические композиционные материалы (УККМ), которые обладают высокими прочностными и жесткостными характеристиками, стойкостью к тепловому и окислительному потокам, малой плотностью по сравнению с металлическими. В УККМ керамическая матрица обладает высокой термостойкостью, а наполнитель, в виде углеродного каркаса, обеспечивает необходимую прочность и жесткость [1].

Известно, что матрица в композиционных материалах должна обеспечивать эффективную совместную работу отдельных элементов наполнителя, например, волокон, армирующих композит в разных направлениях, отдельных слоев ткани и т. д. То есть, одной из важных функций матрицы является равномерное перераспределение напряжений между соседними армирующими элементами. Современные технологии производства ракетно-космических конструкций и изделий из углерод-керамических композиционных материалов – многостадийные и включают множество операций, а также отличаются разнообразными вариантами формирования матричного материала и схемами армирования, в зависимости от ряда факторов и требований. Использование лишь углеродной матрицы не позволяет обеспечить высокую работоспособность конструкций при температурах выше 500 °С в окислительной среде. Применение керамической матрицы хоть и позволяет значительно повысить эксплуатационные температуры конструкций из УККМ, но снижает их термоциклическую стойкость из-за отсутствия разделительного барьера между углеродным каркасом и керамической матрицей [2]. Термостойкость снижается вследствие возникновения термонапряжений на границе «волокно-матрица» из-за различных коэффициентов линейного термического расширения, иногда отличающихся в несколько раз.

На основе вышесказанного целесообразно использовать так называемую ультравысокотемпературную керамику (УВТК), о которой существуют данные об успешном применении в окислительной среде до температуры
2700 °С.

Относительно небольшое количество тугоплавких оксидов являются стабильными в окислительной среде при температуре выше 2000°С.Среди таких материалов можно отметить диоксид циркония (ZrO_2) и гафния (HfO_2), которые имеют самые высокие температуры плавления, не более 2750 °С и не более 2950 °С [2], соответственно. Хотя они являются стабильными и химически инертными, они чувствительны к тепловым нагрузкам и имеют высокие показатели ползучести и фазовые переходы при более высоких температурах [3]. УВТК были широко исследованы в качестве инновационных систем тепловой защиты для аэрокосмических аппаратов, а

также в ряде других применений, где требуется сопротивление окислению или эрозии, тепловым нагрузкам при температурах выше 2000 °C. Эти материалы включают в себя диборид гафния (HfB_2), диборид циркония (ZrB_2),карбид гафния (HfC), карбид циркония (ZrC), карбид тантала (TaC), нитрид гафния (HfN), нитрид цирония (ZrN), нитрид тантала (TaN) и др.(Рисунок 1), у которых температура плавления близка или превышающая 3000 °C, и сохраняют прочность и термостойкость при умеренных температурах, что позволяет повысить аэродинамическую эффективность и маневренность транспортного средства при применении таких материалов в качестве обтекателя спускаемых аппаратов.

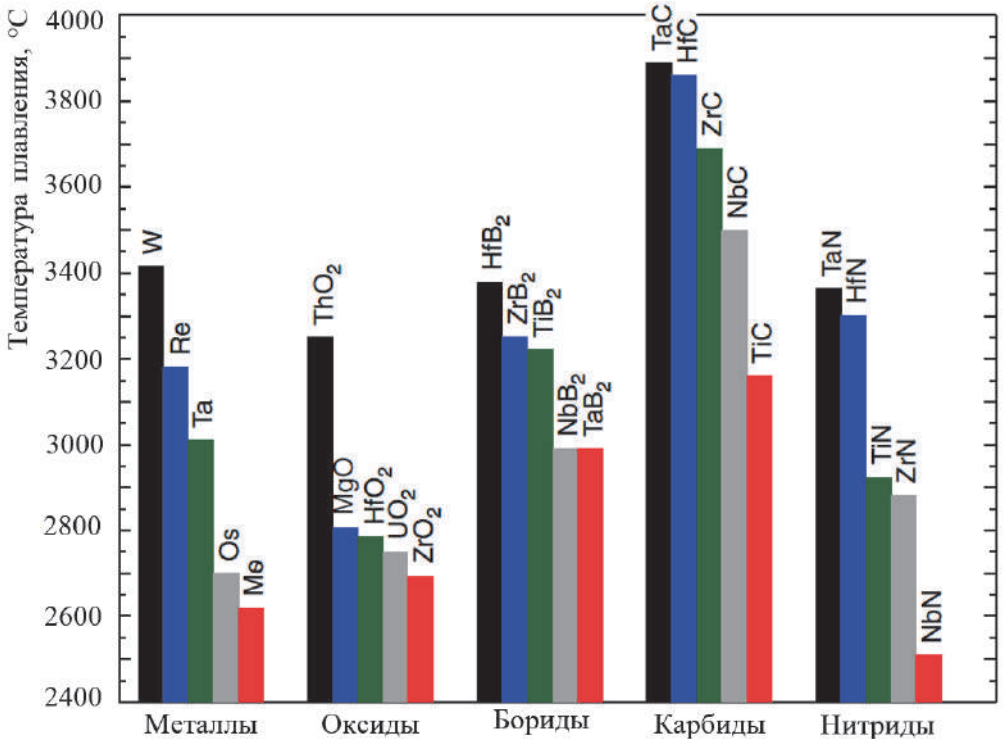


Рисунок 1 – Высокотемпературные материалы

Ниже в таблице 1 приведены свойства основных ультравысокотемпературных керамик [4].

Таблица 1 – Свойства ряда химических соединений

Свойства	**C**	**HfC**	**TaC**	**NbC**	**ZrC**	**SiC**	**B4C**	**TiC**
Температура плавления, °C	3827	3890	3880	3500	3540	2987	2347	3065
Молекулярная масса, г/моль	12,01	190,54	192,96	104,92	103,23	40,10	55,26	59,89
Плотность, г/см3	2,25	12,70	14,50	7,79	6,59	3,21	2,52	4,94
КЛТР, 10-6, 1/K	1,0	6,8	6,6	6,9	7,3	5,3	5,6	7,9
Теплопроводность, Вт/(м·K)	150	22	22	30	20	120	30	50
Удельная	0,84	0,20	0,19	0,35	0,37	0,67	0,96	0,56

Свойства	**C**	**HfC**	**TaC**	**NbC**	**ZrC**	**SiC**	**B4C**	**TiC**
теплоемкость, кДж/(кг·К)								
Кристаллическая структура	HEX	FCC	FCC	FCC	FCC	FCC	RDL	FCC
Предел прочности на сжатие, МПа	-	-	400	400	-	-	-	-
Модуль Юнга, ГПа	-	510	560	580	440	440	460	450
Коэффициент Пуассона	-	0,18	0,24	0,21	0,191	0,21	0,17	0,19
Температура работы на воздухе, °C	500	500	800	800	800	1650	1100	400

HEX – гексагональная
FCC – гранецентрированная кубическая
RDL – ромбоэдрическая

К перспективным тугоплавким компонентам можно отнести цирконий, гафний и соединения на их основе. Такие компоненты должны обладать высокой температурой плавления, высокой теплотой сублимации, формировать на поверхности КМ вязкую оксидную стеклофазу. Стеклофаза в свою очередь должна блокировать диффузию кислорода из рабочей атмосферы в объем КМ. На этом эффекте основана превосходная работоспособность УККМ составов C/SiC, температура работоспособности которых определяется скоростью испарения и сдува оксидной SiO_2 стеклофазы. Так, например, двуокись циркония (ZrO_2), сформированная при окислении карбида кремния (ZrC), имеет температуру плавления не более 2750 °C. Однако, представляется неопределенным по своей значимости эффект диффузии кислорода сквозь оксиды ZrO_2, HfO_2. Вероятно, и это подтверждают приведенные далее результаты испытаний, этот эффект весьма значителен. Для снижения диффузии кислорода многочисленные коллективы ученых по всему миру стремятся к получению трех и более компонентных оксидных систем $ZrSiO_4$ (циркон), $HfSiO_4$ (гафнон), Hf(Zr)-Ta-Si-O и др. [5].

Дибориды циркония (ZrB2) и гафния (HfB2) относятся к диборидам тугоплавких переходных металлов 4-6 групп периодической таблицы. Большинство подобных диборидов имеют температуру плавления выше 3000 °C, высокую теплопроводность и электрическую проводимость, инертность по отношению к расплавам металлов, а также хорошую стойкость к термоудару, что делает их перспективным вариантом для применений в ультравысокотемпературных композитах (УВТКМ).

Композиты, включающие в себя дибориды циркония и гафния, можно условно разделить на три типа:

-чисто керамические композиты на основе диборида циркония или гафния с карбидами и дисилицидными частицами, такие как ZrB2-SiC, HfB2-SiC, ZrB2-MoSi2, HfB2-MoSi2;

- композиты с матрицей на основе ZrB2 или HfB2, армированные короткими углеродными или карбидокремниевыми волокнами;

- композиты с матрицей на основе ZrB2 или HfB2, армированные непрерывными углеродными или карбидокремниевыми волокнами.

Таким образом, с учетом выше представленной информации, в работе под термином ультравысокотемпературный окислительностойкий композиционный материал (УВТОКМ) предлагается понимать композиционный материал на основе непрерывного углеродного армирующего каркаса и керамической матрицы, содержащей тугоплавкие металлы (Zr, Hf, Ti) или соединения тугоплавких металлов. Керамическая матрица для УВТОКМ может быть сформирована на основе многокомпонентных сплавов, карбидов, нитридов, боридов или других соединением на основе Zr или Hf.

Литература

1. Получение и свойства фрикционных углерод-керамических материалов класса c/sic / Известия Самарского научного центра Российской академии наук, т. 13, №4(3), 2011

2. Неметаллические композиционные материалы в элементах конструкций и производстве авиационных газотурбинных двигателей: Учеб.пособие для вузов/ Ю.С. Елисеев, В.В. Крымов, С.А. Колесников, Ю.Н. Васильев.– М.: Изд-во МГТУ им. Н.Э.Баумана, 2007.– 368 с.

3. Тимофеев А.Н. и др. Способ получения карбидокремниевого покрытия на углеграфитовых материалах. Патент РФ № 2053210. – Заявл. 05.11.1992, опубл. 27.01.1996.

4. Буланов И.М., Воробей В.В. Технология ракетных и аэрокосмических конструкций из композиционных материалов. – М.: Изд-во МГТУ им. Н.Э. Баумана, 1998. – 516 с.

5. Справочник по композиционным материалам: В 2-х кн./ под. ред. Дж. Любина. М.: Машиносроение.1988. – 448 с.

МЕТОДИКА СОЗДАНИЯ ПРАВИЛ СЕРВЕРНОЙ ФИЛЬТРАЦИИ ТРАФИКА ДЛЯ ОРГАНИЗАЦИИ ЗАЩИТЫ ОТ “DDOS” АТАК

Круглов Максим Сергеевич, магистрант 1 курса кафедры информационной безопасности
Научный руководитель: **Сухотерин Александр Иванович**, к.воен.н., доцент кафедры информационной безопасности

В данной статье предлагается метод серверной фильтрации для предотвращения DDoS-атаки. Несколько методов фильтрации применяются в двух архитектурах брандмауэров для эффективного предотвращения DDoS-атак. Алгоритм фильтрации PRO и метод строгой фильтрации счетчика переходов применяются путем анализа путей передачи пакетов. Пакеты проверяются, чтобы отличить ненормальные пакеты от обычных пакетов. Система политики безопасности отслеживает сеансы каждого пользователя, и, если трафик превышает пороговое значение, система блокирует сеанс на некоторое время.

DDoS, брандмауэр, фильтрация пакетов.

METHODOLOGY FOR CREATING RULES FOR SERVER-SIDE TRAFFIC FILTERING TO ORGANIZE PROTECTION AGAINST “DDOS” ATTACKS

Kruglov Maxim, 1st year graduate student of the Department of Information security
Scientific adviser: **Sukhoterin Alexander,** Candidate of Military sciences, Associate professor of the Department of Information security

Abstract — This article proposes a method of multifiltration to prevent DDoS attacks. Several filtering methods are applied in two firewall architectures to effectively prevent DDoS attacks. The PRO filtering algorithm and the strict hop counter filtering method are applied by analyzing packet transmission paths. Packets are checked to distinguish abnormal packets from normal packets. The security policy system monitors each user's sessions, and if the traffic exceeds the threshold, the system blocks the session on the appointed time.

DDoS, firewall, packet filtering.

Методы защиты от Ддос атак

DDoS-атака означает "Распределенная атака с отказом в обслуживании (DDoS)" и представляет собой киберпреступление, при котором

злоумышленник заполняет сервер интернет-трафиком, чтобы помешать пользователям получить доступ к подключенным онлайн-сервисам и сайтам.

Мотивы для проведения DDoS-атаки сильно различаются, как и типы отдельных лиц и организаций, стремящихся совершить эту форму кибератаки. Некоторые атаки совершаются недовольными людьми и хактивистами, желающими вывести из строя серверы компании просто для того, чтобы сделать заявление, повеселиться, воспользовавшись кибер-слабостью, или выразить неодобрение.

Другие распределенные атаки типа "отказ в обслуживании" имеют финансовую мотивацию, например, конкурент нарушает или закрывает онлайн-операции другого бизнеса, чтобы тем временем украсть бизнес. Другие связаны с вымогательством, при котором злоумышленники нападают на компанию и устанавливают на ее серверы программы-носители или программы-вымогатели, а затем заставляют их заплатить крупную финансовую сумму за возмещение ущерба.

Число DDoS-атак растет, и даже некоторые крупнейшие мировые компании не застрахованы от "DDoS-атак". Крупнейшая атака в истории произошла в феврале 2020 года на Amazon Web Services (AWS), обогнав предыдущую атаку на GitHub двумя годами ранее. Последствия DDoS-атаки включают падение законного трафика, потерю бизнеса и ущерб репутации.

По мере развития Интернета вещей (IoT) растет число удаленных сотрудников, работающих из дома, а также количество устройств, подключенных к сети. Безопасность каждого устройства Интернета вещей может не всегда поддерживаться на должном уровне, что делает сеть, к которой оно подключено, уязвимой для атак. Таким образом, важность защиты от DDoS-атак и смягчения их последствий имеет решающее значение

Распределенная атака типа "отказ в обслуживании" является подкатегорией более общей атаки типа "отказ в обслуживании" (DoS). При DoS-атаке злоумышленник использует одно подключение к Интернету, чтобы атаковать цель поддельными запросами или попытаться использовать уязвимость в системе кибербезопасности. DDoS-атаки более масштабны. Он использует тысячи (даже миллионы) подключенных устройств для достижения своей цели. Огромный объем используемых устройств значительно затрудняет борьбу с DDoS-атаками.

Распределенные атаки типа "отказ в обслуживании" могут парализовать даже самую хорошо структурированную сеть на несколько дней, что приведет к потере продаж на миллионы долларов, замораживанию онлайн-сервисов и нанесению ущерба репутации компании.

Согласно исследованию, CSI/FBI по компьютерной преступности и безопасности за 2022 год, DDoS-атаки являются вторым по стоимости киберпреступлением и единственными, число которых увеличилось в 2022 году.

Интернет может быть опасным местом, где DDoS-атаки становятся излюбленным оружием хакеров, политических активистов и международных кибертеррористов. Кроме того, с появлением в арсенале хакеров все более мощных инструментов запускать DDoS-атаки становится все проще. Каждый месяц появляются новые вирусы и черви, поэтому компании должны быть готовы отразить эту постоянно растущую угрозу безопасности.

DDoS-атаки используют преимущества открытости Интернета и его преимущества в доставке пакетов данных практически из любого источника в любое место назначения. Что делает DDoS-атаки такой сложной задачей, так это то, что незаконные пакеты данных практически неотличимы от законных. Типичные типы DDoS-атак включают атаки на пропускную способность и атаки приложений.

При атаке с пропускной способностью сетевые ресурсы или оборудование потребляются большим количеством пакетов. При атаке приложения ресурсам TCP или HTTP не разрешается обрабатывать транзакции или запросы.

Методы защиты от DDoS-атак

Есть несколько подходов, которые вы можете предпринять для защиты от DDoS-атаки:

Black-holing или sink-holing: Этот подход блокирует весь трафик и перенаправляет его в пустоту, где он отбрасывается. Недостатком является то, что весь трафик отбрасывается - как хороший, так и плохой – что может вызвать проблемы с работоспособностью интернет ресурсов. Аналогичным образом, меры по фильтрации пакетов и ограничению скорости просто отключают все, лишая доступа законных пользователей.

Маршрутизаторы и брандмауэры: Маршрутизаторы могут быть настроены для остановки простых ping-атак путем фильтрации несущественных протоколов, а также могут останавливать недопустимые IP-адреса. Однако маршрутизаторы, как правило, неэффективны против более сложных поддельных атак и атак на уровне приложений с использованием действительных IP-адресов. Брандмауэры могут отключить определенный поток, связанный с атакой, но, как и маршрутизаторы, они не могут выполнять антиспуфинг.

Системы обнаружения вторжений: Решения IDS обеспечат некоторые возможности обнаружения аномалий, чтобы они могли распознавать, когда в качестве средства атаки используются действительные протоколы. Они могут использоваться в сочетании с брандмауэрами для автоматического блокирования трафика. С другой стороны, они не автоматизированы, поэтому они нуждаются в ручной настройке экспертами по безопасности, и они часто генерируют ложные срабатывания.

Серверы: Правильная настройка серверных приложений имеет решающее значение для минимизации последствий DDoS-атаки. Администратор может явно определить, какие ресурсы может использовать

приложение и как оно будет отвечать на запросы клиентов. В сочетании с устройством для предотвращения DDoS-атак оптимизированные серверы имеют шанс продолжить работу в результате DDoS-атаки.

Устройства для предотвращения DDoS-атак: Несколько компаний либо создают устройства, предназначенные для очистки трафика, либо встраивают функции предотвращения DDoS-атак в устройства, используемые в основном для других функций, таких как балансировка нагрузки или брандмауэр. Эти устройства имеют разный уровень эффективности. Ни одино из них не идеалено. Часть законного трафика будет отброшена, а часть незаконного трафика попадет на сервер. Серверная инфраструктура должна быть достаточно надежной, чтобы обрабатывать трафик и, при этом, продолжать корректно обслуживать законных клиентов.

Избыточное выделение ресурсов: или покупка избыточной полосы пропускания или резервных сетевых устройств для обработки резких скачков спроса может быть эффективным подходом к борьбе с DDoS-атаками.

Одним из преимуществ использования аутсорсингового поставщика услуг является то, что вы можете покупать услуги по требованию, такие как прерывистые схемы, которые обеспечивают вам большую пропускную способность, когда вам это нужно, вместо того, чтобы делать дорогостоящие капиталовложения в резервные сетевые интерфейсы и устройства.

Метод двойной серверной фильтрации

В данной работе предложен метод эффективного предотвращения и обнаружения DDoS-атак на основе двойной, серверной фильтрации трафика.

Предлагаемый способ использует два брандмауэра, первый брандмауэр анализирует пакеты, поступающие извне, для более строгой фильтрации пакетов.

Вторичный брандмауэр проверяет данные тех пакетов, которые прошли через первичный брандмауэр, чтобы различать обычные пакеты и аномальные пакеты и проверяет, превышают ли пакеты общий порог трафика. Он также проверяет трафик каждого пользователя на предмет того, превышает ли он пороговое значение, выделенное пользователю.

Также используется ACL (Список контроля доступа)

ACL - это наиболее распространенная технология управления трафиком, используемая в сетевых системах. Несмотря на то, что этот метод способен предотвращать ненормальный трафик на основе IP-адресов, служебных портов или содержимого, он становится причиной снижения производительности, создавая большую нагрузку на сетевое оборудование, если нет специального ASIC (специфичного для конкретного приложения Интегральная схема) модуль.

В случае организаций, которые управляют многими сетевыми системами, им приходится создавать разные сценарии для каждой системы или входить в систему индивидуально и изменять свои настройки для обновления доступа политики управления для этих систем. Фильтрация

пакетов с использованием счетчика переходов поскольку поддельный IP-пакет имеет значение количества переходов исходного IP-адреса, когда он прибыл в пункт назначения, IP -пакет может быть идентифицирован, является ли он поддельным или обычным.

В этой структуре пакеты сначала фильтруются с помощью анализа пути маршрутизатора и снова фильтруются с использованием значений TTL (Время ожидания). Чтобы исправить проблему задержек в процессах фильтрации, необходимо получить информацию о пакетах для отдельных существующих IP-адресов, среднее значение, рассчитанное с помощью статистического анализа на основе в предыдущих действиях, используется TTL (TTLm).

Когда пакеты прибыли, из их исходных и конечных IP-адресов извлекаются значения TTL. После этого информация о сохраненных начальных значениях TTL и средних значениях TTL берется из таблицы IP. Значение количества переходов каждого пакета вычисляется с использованием начального значения TTL в таблице и конечного значения TTL пакета. Вычисленное значение сравнивается со средним значением TTL, чтобы решить, является ли пакет обычным или нет.

Когда пакет, наконец, передается значение числа переходов пакета и сохраненные значения счетчика переходов сравниваются друг с другом, чтобы решить, является ли пакет обычным.

В этом случае существует диапазон ошибок между средним значением TTL и вычисленным значением количества переходов пакета. Граница ошибки существует между вычисленным значением количества переходов входного пакета и значением количества переходов, которое уже сохранено в таблице.

Пакеты, прошедшие через маршрутизатор по одному и тому же пути, имеют одно и то же значение имени пути. Значения имени пути формируются путем маркировки пакетов, когда пакеты проходят через маршрутизатор. Когда пакет поступает на маршрутизатор, маршрутизатор отмечает последние n битов IP-адреса в позиции битовой строки 16-битного поля идентификатора пакета.

Позиция битовой строки, которая должна быть отмечена, вычисляется с использованием значения TTL (Time to Live). Поскольку значения, помеченные как таковые, имеют разное значение в зависимости от путей, передаваемых пакетами, поддельные IP-адреса могут быть идентифицированы на основе их значения имени пути.

Используя значение имени пути, хост-жертва может составить черный список атакующих пакетов, чтобы отфильтровать атакующие пакеты, вставленные в хост-жертву, если система состоит из злоумышленника, жертвы и маршрутизаторов.

С помощью базового метода маркировки маршрутизаторы помечают последние n битов своих IP-адресов в полях идентификации IP вставленных

пакетов. Чтобы определить позицию, в которой должно быть отмечено имя пути, 16 бит делятся на n секций (16/n), а значения TTL пакетов используются в качестве индексов (TTL mod [16/n]).

Маршрутизаторы вставляют последние n битов своих IP-адресов в позиции для маркировки. Жертва использует эти значения имени пути для блокирования атакующих пакетов. Поскольку метод имени пути разработан очень просто, у этого метода есть преимущества, заключающиеся в том, что он не создает накладных расходов для маршрутизаторов и что жертва может немедленно фильтровать пакеты без помощи верхних маршрутизаторов.

Пакеты проверяются, чтобы проверить, превышает ли определенный IP-трафик источника и определенный трафик сеанса пороговое значение.

Использование системы мониторинга и политики безопасности

Система мониторинга отслеживает системные ресурсы, выделенные каждому пользователю в соответствии с политикой безопасности, определенной администратором, и принимает решение о приостановке, блокировка и разрешение в режиме реального времени.

Политика безопасности, относящаяся к системе мониторинга, устанавливается путем статистического анализа после определения порогового значения, которое может обрабатываться существующими серверами. Пороговое значение трафика сеанса и количество сеансов для каждого пользователя управляются во втором брандмауэре.

Отключение сервера и незаконные действия предотвращаются путем применения политики безопасности к действиям пользователя и действиям сервера. Устанавливаются политики безопасности для ограничений ресурсов, соответствующих назначенным ролям пользователей и классу ролей, а также пороговые значения чтобы пользователи могли использовать ресурсы, соответствующие их ролям.

Когда пользователь выполняет действие, которое отклоняется от определенной политики безопасности, пользователь сначала остается в статусе прерванного на три минуты, и, если та же ситуация повторяется, IP-адрес блокируется.

Злоумышленники могут изменить начальное значение TTL, чтобы сделать другое значение метки имени пути вставленным из того же пути. Чтобы справиться с этим трюком, хост-жертва может проверьте значения TTL, чтобы определить самую старую позицию маркировки в пакете, и можете повернуть остальные значения на основе позиции, чтобы получить значения маркировки имени пути из измененных значений TTL.

По большей части компании заранее не знают о грядущей DDoS-атаке. Характер атаки часто меняется на полпути, требуя от компании быстрого и непрерывного реагирования в течение нескольких часов или дней.

Поскольку основным результатом большинства атак является потребление вашей пропускной способности Интернета, хорошо

оборудованный управляемый хостинг-провайдер располагает как пропускной способностью, так и устройствами для смягчения последствий атаки.

Заключение

DDoS-атаки - это разрушительное скрытое оружие, которое может остановить бизнес. Наша зависимость от Интернета продолжает расти, а угроза DDoS-атак продолжает расти. Организациям необходимо обеспечить непрерывность работы и доступность ресурсов с помощью бдительного подхода к предотвращению DDoS-атак, если они хотят вести "обычный бизнес".

Ранее, поскольку Интернет быстро развивался, DDoS-атаки также были диверсифицированы за счет использования новых методов атаки. В последнее время, по мере увеличения частоты DDoS-атак, требуются более жесткие системы реагирования, чем современные системы защиты. Современные методы предотвращения DDoS-атак устанавливают пороговые значения путем сбора и анализа трафика за определенный период времени. Однако эти методы обнаружения DDoS-атак не могут обнаруживать DDoS-атаки в начале атаки, так что жертвы получают повреждения или жертва не может эффективно реагировать на атаки, даже если атаки обнаруживаются, потому что жертва уже повреждена.

В данной работе предлагается система предотвращения DDoS, которая усиливается за счет использования эффективных методов фильтрации пакетов. Чтобы определить возможность атак пакетами, поступающими извне, установлен строгий метод фильтрации пакетов R-PA (Router Path Analysis).

С помощью этого метода процессы фильтрации пакетов могут быть улучшены, а коэффициенты ложного обнаружения также могут быть уменьшены из-за проблемы задержки метода фильтрации количества переходов, для которого требуется пакет информация по отдельным существующим IP-адресам частично раскрыта.

Также данные пакетов проверяются для классификации пакетов на нормальные и ненормальные, и на то, превышают ли пакеты лимит трафика и превышает ли трафик сеанса пользователя пороговое значение, чтобы определить, следует ли передавать пакеты как обычные или их следует удалить.

Литература

1. Доктрина информационной безопасности Российской Федерации (№ 646 от 05.12.2016 г.)

2. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации

3. Федеральный закон "О персональных данных» от 27 июля 2006 года № 152-ФЗ

4. Искусство управления информационными рисками. Астахов А.М, ГлобалТраст, Изд. ДМК Пресс, 2009

5. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие. М.: Гостехкомиссия России, 1998. - 320 с.

6. Хорев А.А. Методы и средства поиска электронных устройств перехвата информации. - М.: МО РФ, 1998. – 224 с.

7. Хорев А.А. Способы и средства защиты информации. - М.: МО РФ, 1998. – 316 с.

8. Хорев А.А. Техническая защита информации: учеб. Пособие для студентов вузов. В 3 т. Т1. Технические каналы утечки информации. – М.: НПЦ «Аналитка», 2008. – 436 с.

9. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ТИД Диа Софт, 2002.

10. The ROI of Data Loss Prevention (DLP), A Websense Whitepaper;

РАЗВИТИЕ ЛАЗЕРНЫХ СИСТЕМ АКУСТИЧЕСКОЙ РАЗВЕДКИ

Кузин Михаил Алексеевич, магистрант 1 курса кафедры информационной безопасности
Научный руководитель: **Воронов Александр Николаевич,** к.воен.н., доцент кафедры информационной безопасности

На протяжении всей истории существования человечества информация являлась и является одним из главных ресурсов, используемых для достижения определенных целей. Методы и средства для добычи информации развиваются и идут рука об руку с технологическим развитием человечества. Например, те методы, что требовали непосредственное участие человека в добыче информации, при современном технологическом развитии могут быть заменены автоматическими комплексами, действующими удаленно. Развиваются как средства разведки, так и меры противодействия. В настоящее время определены каналы утечки информации, одним из которых является оптико-электронный канал утечки информации.

Оптико-электронный канал утечки информации, лазерные микрофоны, средства акустической разведки.

DEVELOPMENT OF LASER ACOUSTIC RECONNAISSANCE SYSTEMS

Kuzin Mikhail, 1st year graduate student of the Department of Information security
Scientific adviser: **Voronov Alexander,** Candidate of Military sciences, Associate professor of the Department of Information security

Throughout the history of humankind, information has been and is one of the main resources used to achieve certain goals. Methods and means for extracting information are developing and go hand in hand with the technological development of humankind. For example, those methods that required the direct participation of a person in the extraction of information, with modern technological development, can be replaced by automatic systems operating remotely. Both reconnaissance means and countermeasures are being developed. Currently, information leakage channels have been identified, one of which is an optoelectronic information leakage channel.

Optoelectronic leakage channel, laser microphone, acoustic reconnaissance systems.

Хотя добыча информации происходила и раньше, документированная история шпионажа насчитывает несколько веков. С технологическим развитием человечества у корпораций и государств появляется все больше методов и средств для добычи информации, обнаруживаются новые каналы утечки информации. Но в настоящее время то, что было доступно только на высшем уровне (спецслужбы, международные компании) из-за своих сложности исполнения, доступности и стоимости, с развитием технологий стало доступным более широкому кругу лиц, стало коммерческим продуктом.

Одним из известных каналов утечки информации является оптико-электронный. В настоящее время в действующих руководящих и методических документах Российской Федерации [1-2] по защите конфиденциальной информации оптико-электронный канал утечки информации не рассматривается, поэтому требований для закрытия данного канала при разработке систем для обеспечения защиты информации нет. В данной статье рассмотрены виды лазерных микрофонов, применяющихся в качестве систем акустической разведки, и их развитие.

В первую очередь необходимо описать принцип действия утечки информации через данный канал. Акустический речевой сигнал, распространяясь в воздушной среде, воздействует на поверхности помещения (в том числе отражающие, например, оконные стекла, зеркала и т.п.) и предметов, которые в нем находятся и вызывает вибрацию этих поверхностей. С помощью специального оборудования (лазерных микрофонов) вибрирующие отражающие поверхности облучаются лазерным лучом, отраженное лазерное излучение которого модулируется по фазе и амплитуде и принимается приемником лазерного микрофона. При демодуляции принятого излучения выделяется речевая информация [3-5] (рис.1).

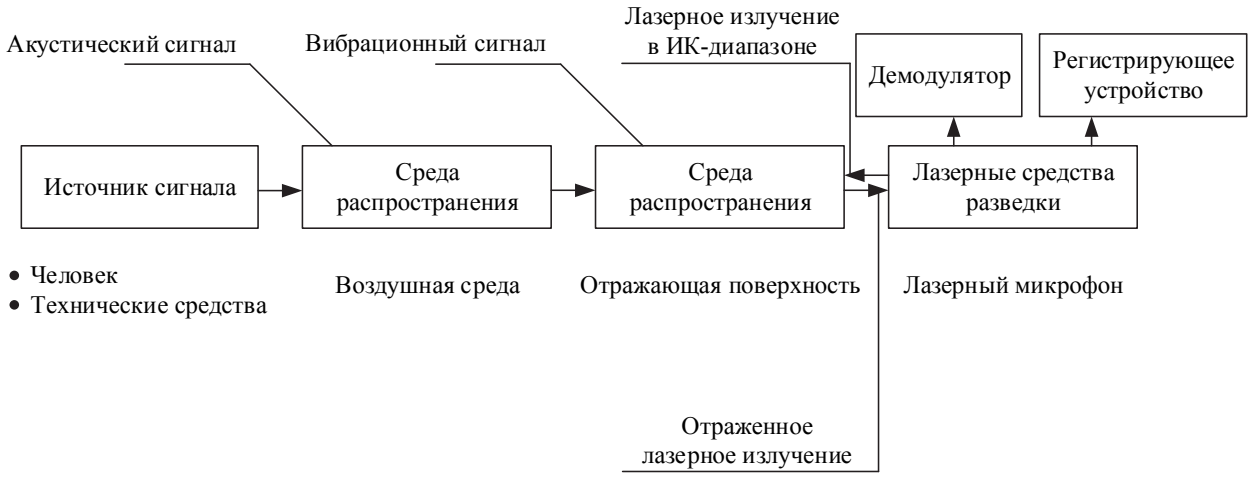


Рисунок 1 – Схема утечки информации через оптико-электронный канал

В первых системах акустической разведки вместо лазеров использовался инфракрасный луч. Одной из первых разработок систем акустической разведки, являющейся разновидностью лазерных микрофонов, считается «Буран». Принцип действия и считывания информации с отражающих поверхностей помещения аналогичен описанному выше, но в качестве лазера использовалось инфракрасное излучение. Изобретателем системы является советский ученый Лев Сергеевич Термен. Данная система была эффективной на расстоянии до 500 м., но в случае дождя или тумана не работала должным образом. Полученный сигнал проходил обработку с помощью аналоговых технологий, доступных в то время [6]. Также в то время существовала практика внедрения в стекло окна миниатюрных призм, почти невидимых для обычного взгляда, для улучшения чувствительности лазера и помощи в его позиционировании [7]. Так как в подавляющем большинстве случаев системы для ведения разведки применяются спецслужбами государств, доказательства и факты их применения редко придаются огласке, а многие из тех, что существуют на данный момент нельзя однозначно подтвердить или опровергнуть.

Рассмотрим различные варианты исполнения и использования подобных систем.

В общем виде лазерный микрофон состоит из лазера, приемника и демодулятора (рис. 2). Луч лазера падает под некоторым углом на стекло окна, которое под воздействием акустического речевого сигнала создает вибрацию. Отраженный луч модулируется и принимается приемником, далее производится демодуляция, при которой выделяется речевая информация. Система довольно проста в своем исполнении, но требует тщательной настройки.

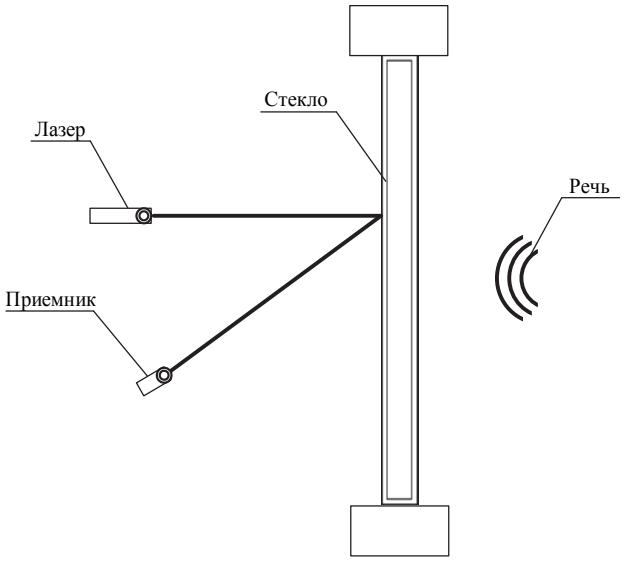


Рисунок 2 – Принцип действия лазерного микрофона

Данную систему можно улучшить с помощью сплиттера (делителя). Он необходим для повышения чувствительности системы. Его применение позволяет совместить приемник с лазером, для сведения падающего и отраженного луча в одну точку (рис. 3).

Возможно создание любительских систем из комплектующих и элементной базы, находящихся в свободном доступе. Конечно, качество таких систем (чувствительность, дальность, качество передаваемой информации), по сравнению с профессиональным оборудованием, будет невелико, но они могут дать общее представление о функционировании лазерных микрофонов, и в каких-то случаях вероятно их использование.

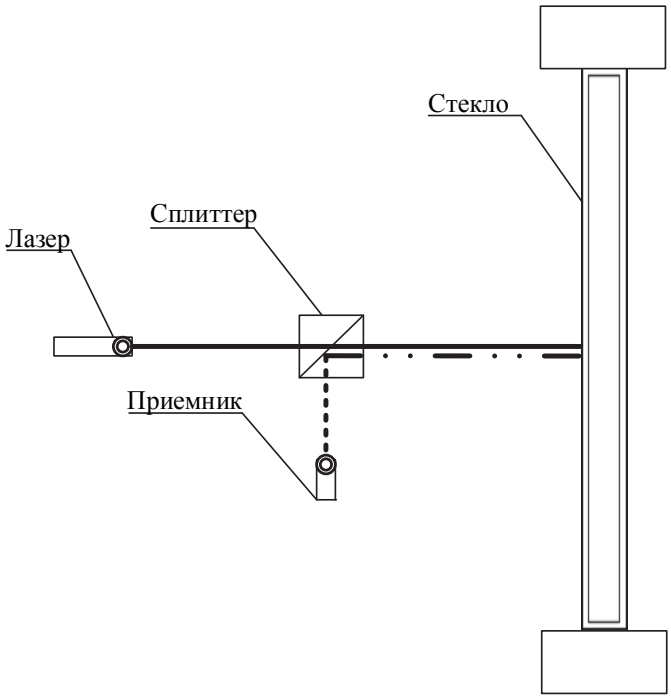


Рисунок 3 – Лазерный микрофон с применением сплиттера

Можно получить еще более высокую чувствительность, чем в предыдущей схеме если использовать интерферометрию (рис.4). Данный подход имеет несколько недостатков. Наиболее бросающийся в глаза – большие различия в длине плеча. В идеале оба плеча должны быть одинаковой длины. При этом способе многократно возрастает сложность настройки, так как отраженные лучи должны приниматься согласованными по фазе, если этого не происходит, то интерференционная картина смазывается или вообще отсутствует, и это приводит к падению чувствительности.

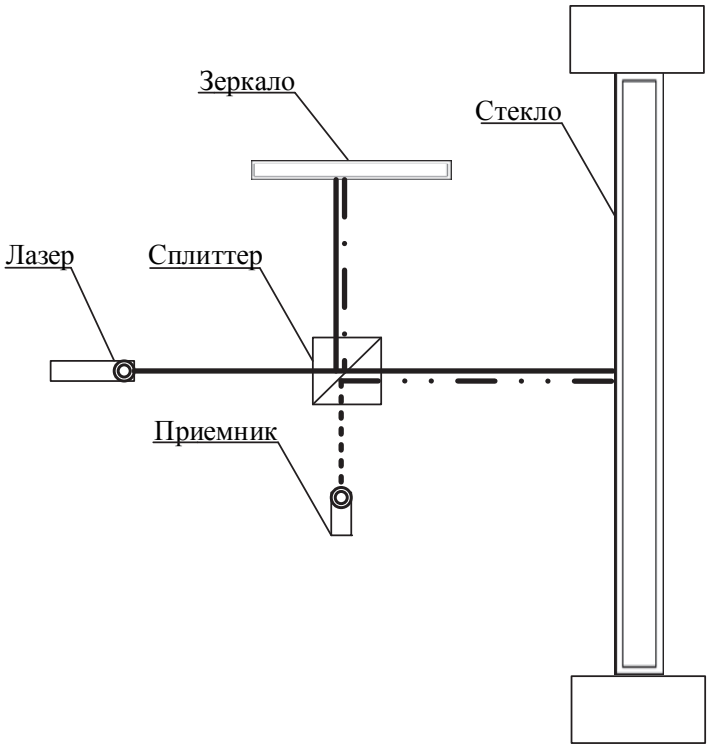


Рисунок 4 – Использование интерферометрии в лазерных микрофонах

Наиболее совершенный вариант исполнения – интерферометр, с плечами равной длины (Dual Beam Laser Mic) (рис.5). В этом исполнении лазерного микрофона применяется дифференциальный метод измерения акустической вибрации. Информация снимается с малоразмерной секции стекла, вследствие чего сильно ослабляется синфазная помеха, вызываемая низкочастотными колебаниями стекла.

Очевидно, что создание любительских систем в данном исполнении маловероятно в виду сложности и отсутствия некоторых компонентов в свободном доступе. Принципиальные схемы профессиональных систем лазерной акустической разведки невозможно найти в открытом доступе, в виду тематики использования устройств, но можно предположить, что по крайней мере ранние модели работали по схожему принципу действия.

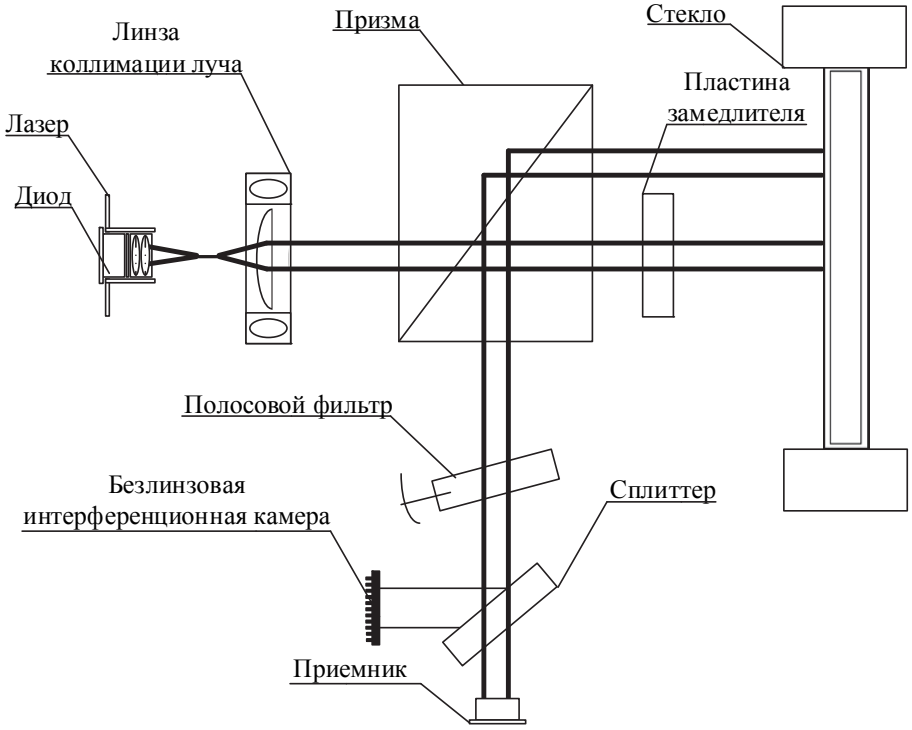


Рисунок 5 – Интерферометр

Технические характеристики и надежность лазерных систем акустической разведки улучшаются с развитием лазерных технологий. При анализе данных из открытых источников, где указаны характеристики лазерных микрофонов (табл. 1) было выявлено, что максимальная дальность работы устройств – 1000 м, но при этом стоит учитывать, что испытания проводились в идеальных условиях.

Таблица 1 – Существующие модели лазерных микрофонов

Модель	Производитель	Страна	Сайт	Дальность
SIM-LAMIC	SIM Secure Information Management	Германия	sim-secure.de	500
Laser-3000	PKI Electronic Intelligence	Германия	pki-electronic.com/	500
Laser-3500	PKI Electronic Intelligence	Германия	pki-electronic.com/	500
HP-150	Hewlett-Packard	США	hp.com	1000
LAS-MIC	Endoacustica	Италия	endoacustica.com	800

На качество полученной информации влияет множество факторов, таких как:

1. Характеристики применяемого лазера:
- Рабочая длина волны лазерного излучения
- Выходная мощность (интенсивность)

- Синфазность

2. Характеристики применяемого приемника:

- Спектральная чувствительность
- Избирательность по длинам волн

3. Качество поверхности
4. Погодные условия:

- Ветер
- Грязь
- Туман
- Дождь

5. Уровень акустических шумов
6. Уровень источника сигнала

Рассмотрим преимущества и недостатки лазерных систем акустической разведки.

Преимущества:

- Сложность выявления канала утечки
- Высокая дальность
- Применение в системе защиты информации организации мер, направленных на закрытие оптико-электронного канала маловероятно.

Недостатки:

- Высокая стоимость систем
- Зависимость от множества внешних факторов
- Развертывание системы требует высококвалифицированного специалиста

Стоит заметить, что новейшие лазерные микрофоны (табл. 2), называемые оптоакустическими, имеют меньшую паспортную максимальную дальность чем свои предшественники. Но при этом они лишены многих недостатков, присутствующих в предыдущих моделях, а также обладают значительными преимуществами.

Таблица 2 – Оптоакустические лазерные микрофоны

PKI 2510	PKI Electronic Intelligence	Германия	pki-electronic.com/	150
PKI 3100	PKI Electronic Intelligence	Германия	pki-electronic.com/	300
OAM-2000	SIM Secure Information Management	Германия	sim-secure.de	300

Отличия новейших лазерных микрофонов от старых моделей:

- Позволяют снимать информацию через окно или небольшое отверстие с предметов, находящихся внутри помещения
- Не зависят от угла падения луча

- В оптическом блоке размещены излучатель и приемник, что облегчает управление
- Окружающие шумы между датчиком и целью не влияют на качество передачи информации
- Работают при минимальных вибрациях поверхностей

Чтобы обеспечить защищенность организации от утечки информации с помощью лазерных микрофонов применяется комплекс организационных и технических мер. Технические меры подразумевают использование активных и пассивных средств защиты для воздействия на канал перехвата информации [8, С. 112].

Организационные меры включают в себя:

- использование погодных условий
- проведение переговоров в помещениях, обеспечивающих за их пределами наибольший уровень фонового шума
- проведение переговоров в помещениях, где отсутствуют окна (подвальные помещения и т.п.)
- использование помещений, в которых расстояние до границ контролируемой зоны превышает радиус действия средств разведки

Технические меры включают в себя:

- применение активных средств акустической защиты
- применение ставней, экранов на окнах, виброштор

Новые модели лазерных микрофонов (оптоакустические) отличаются от старых моделей предыдущего поколения. Направленные лазерные микрофоны фокусировались на преломлении лазерного луча от оконного стекла, тогда как новые модели, к примеру, проницают его, нацеливаясь на предметы внутри помещения. Таким образом установки вибровозбудителей на окна недостаточно для защиты помещения от оптоакустических лазерных микрофонов, необходим комплексный подход с применением вибровозбудителей, экранов (ставней, виброштор).

Литература

1. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). – М.: Гостехкомиссия России, 2001.
2. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержден приказом ФСТЭК России от 29 апреля 2021 г. № 77.
3. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. – М.: Гостехкомиссия России, 1998.

4. Герасименко В.Г., Лаврухин Ю.Н., Тупота В.И. Методы защиты акустической речевой информации от утечки по техническим каналам. – М.: РЦИБ «Факел», 2008.

5. Хорев А.А. Способы и средства защиты информации. – М.: МО РФ, 2000.

6. Glinsky A. Theremin: Ether Music and Espionage. – M: University of Illinois Press, Urbana, IL, 2000.

7. Wallace R., Melton H. K., Schlesinger H.R. Spycraft: The Secret History of the CIA's Spytechs, from Communism to Al-Qaeda. – M.: Dutton/Penguin Group, New York, NY, 2008.

8. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами. Учебное пособие. – М.: ИТМО Санкт-Петербург, 2012 С. 112-115.

ОЦЕНКА ЭФФЕКТИВНОСТИ ИНВЕСТИЦИЙ И ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В 2023 ГОДУ

Кузина Анна Владимировна, магистрант 2 курса кафедры информационной безопасности
Научный руководитель: **Дедюрина Мария Сергеевна**, преподаватель кафедры информационной безопасности

В данной статье изложены основные методы оценки эффективности инвестиций в информационную безопасность и проанализирована их обоснованность. Результаты анализа показывают, что, используя комбинацию этих методов, можно добиться максимальной эффективности инвестиций в информационную безопасность.

Информационная безопасность, методы оценки инвестиций в информационную безопасность, эффективность инвестиций в информационную безопасность.

EVALUATION OF THE EFFECTIVENESS OF INVESTMENTS AND PROMISING DIRECTIONS OF DEVELOPMENT IN INFORMATION SECURITY IN 2023

Kuzina Anna, 2nd year graduate student of the Department of Information security
Scientific adviser: **Dedyurina Maria**, Lecturer of the Department of Information security

This article discusses the main methods used to assess the efficiency of investment in information security, the analysis was made and the evaluation of efficiency of their application was given. The results of the analysis showed, that the achievement of the efficiency of investment in information security con be attained by using the methods in combination.

Information security, methods of evaluation of investment in information security, efficiency of investment in information security.

Одним из немногих вопросов информационной безопасности (ИБ) в бизнесе является анализ экономической составляющей технологии, используемой для защиты информации [1]. Инвестиции могут быть включены в основные уровни этой оценки.

Инвестиции - это капитал, вложенный с целью получения прибыли от какой-либо деятельности [4]. При рассмотрении инвестиций в деятельность

систем информационной безопасности (СИБ) используются определенные методы, позволяющие эффективно расходовать средства на информационную безопасность и ее внедрение в бизнес. Однако инвестиции не всегда эффективны, даже если средства выделяются в ИУ на основе различных методов анализа затрат [3].

Предприятия все больше осознают растущую потребность инвестировать в надежные меры безопасности, способные защитить ценные данные компании в условиях постоянно растущего количества угроз. Но перед лицом бюджетных ограничений, некоторые компании изучают и взвешивают все за и против инвестирования в обнаружение угроз, по сравнению с их предотвращением. Можно ли добиться надежной защиты, инвестируя только в обнаружение или предотвращение? Что сегодняшние предприятия должны сделать приоритетными с точки зрения инвестиций в безопасность и почему? Каково соответствующее соотношение расходов на безопасность, которое должно быть направлено на меры по предотвращению и обнаружению?

Есть разные точки зрения, которые рассмотрены и изучены авторами работы. Тем не менее, это один из самых насущных вопросов, стоящих сегодня перед предприятиями, поскольку компании стремятся сократить расточительные расходы и снизить затраты на ИТ, одновременно повышая уровень своей безопасности.

Среди работ российских ученых, посвященных оценке эффективности инвестиций в информационную безопасность, можно выделить работы Ясенева В.Н., Астахова А.М., Бедрана А., Муравьева Д., Постоева А., а также работы зарубежных ученых, таких как Гордон Л.А., Виллемсон Дж., Шим В., в своих работах находятся различные решения проблемы оценки затрат с точки зрения эффективности информационной безопасности. Отсутствие стандартных методов оценки затрат и выгод в области информационной безопасности затрудняет принятие необходимых решений специалистами по ИБ, и это одна из основных проблем нашего анализа.

Инвестиции в информационную безопасность должны основываться на:

- Оценке уязвимости системы.
- ФСА (функционально-стоимостный анализ).
- Бизнес-климате.
- Рекомендациях аудиторских компаний.

Инвестиции в ИБ должны основываться на функционально-стоимостном анализе и надежном экономическом обосновании. ФСА представляет собой технологию анализа затрат на выполнение изделием его функций, а цель данного метода минимизации издержек производство, не теряя качества. Решения, основанные на рекомендациях аудита, будут носить рекомендательный характер и не смогут полностью удовлетворять ключевым целям и задачам бизнеса. Оценка уязвимости полезна, но она не сможет

отразить, оправданы ли затраты, хотя при помощи оценки угроз, можно спрогнозировать возможные убытки.

При разработке систем информационной безопасности (СИБ) специалисты решают несколько последовательных задач, одна из которых - эффективность, надежность и безопасность. Однако на этапе проектирования СИБ разработчикам приходится сталкиваться с проблемой распределения ресурсов. Прежде чем инвестировать в проект, используются определенные методы для оценки эффективности инвестиций.

Рисунок 1 – Алгоритмы оценки инвестиций

В ИБ предприятия выделяется следующие методы оценки экономической эффективности (рис. 1):

1. методы оценки экономической эффективности инвестиций в информационную безопасность:
   - совокупная стоимость владения (Total Cost of Ownership, TCO);
   - возврат инвестиций (Return On он Investments, ROI).
2. стандартные методы оценки экономической эффективности инвестиций (отдача инвестиций).

Все стандартные методы оценки экономической и эффективности инвестиций можно подразделить:

1. на статические методы оценки:
   – срок окупаемости (Payback Period –PP);
   – суммарный доход (D);
2. Динамические методы оценки:
   – чистый дисконтированный доход (Net Present Value gh– NPV);
   – индекс доходности инвестиций (Profitability Index, PI);
   – внутренняя норма доходности (Internal кот Rate of gh Return, IRR);
   – модифицированная внутренняя норма и доходности (Modified jov Internal Rate of Return, MIRR);

– дисконтированный срок окупаемости инвестиций (Discounted payback period, DPP).

Помимо этого, существует так же обобщенный свод методов оценки эффективности инвестиций, которые представлены на рисунке 2.

Рисунок 2 – Простые методы оценки инвестиций

В настоящее время в развитых странах с большим, средним и малым оборотом инвестиций преобладают современные технологии оценки инвестиций с учетом времени и риска. Динамические методы часто систематически называют методами дисконтирования, поскольку каждый из них чаще всего применяется для установления защитной стоимости современных индикативных (т.е. полученных простым дисконтированием) методов для предполагаемых денежных потоков, связанных с реализацией инвестиционного проекта.

Статистические методы чаще всего применяются для кластеризации проектов и первичного анализа. Одним из основных превосходств прогнозных расчетов, к которым стремятся более статичные методы оценки доходов, является несложность оценки при большом распределении собственных значений их отдельных коэффициентов. Они включают прогнозы, необходимые для расчета коэффициентов для статических добавочных показателей. В их пользу говорит специфичность, преимущество, достаточно высокое для однозональных методов, и тот факт, что их введение не связано с потерями проекта.

Динамические методы оценки рассматриваются с точки зрения экономической отдачи инвестиций, для которых доступна дисконтированная информация.

1. Метод управления коэффициентами. Однако в этом методе отсутствует возможность расчета возврата инвестиций в инфодинамическую безопасность (или ROI, или прогнозируемый возврат). Для оценки эффективности инвестиционного подхода к безопасности в снижении потерь при внедрении используется выражение для рассматриваемого возврата инвестиций (security ROI) и коэффициент, определяющий потери как отношение стоимости попытки к величине выигрыша в случае успеха.

Эффективный ROI = (средний доход + меры риска + рассчитанные AddLosses) / произведенные инвестиции.

Где доход - это различные вариации дохода, полученного в результате управления внедрением классификации системы оценки защиты на основе информации.

Риск - это еще один параметр, AddLosses, рассчитываемый в денежном выражении, учитывающий в среднем не только время, затраченное на защиту от потенциальных потерь, возникающих из-за угрозы отказа от инвестиционной системы, AddLosses, но и вероятностную стоимость отражения ее взаимосвязанной реализации.

AddLosses - Потери, связанные со стоимостью недоинвестирования в систему защиты.

Инвестиции - показывает инвестиции в систему защиты, которая обычно является эффективной.

Недостатком этого подхода является то, что расчеты могут производиться на основе различных методов, что делает невозможным сравнение данных и может ввести в заблуждение.

2. Для этих компаний управление своими затратами позволяет оценить общую стоимость инвестиций в ИТ, чтобы получить максимальную отдачу от управления ими. Общая стоимость владения рассчитывается как сумма затрат. Для компании это значение затем сравнивается с рекомендуемым значением. Стоимость владения можно снизить за счет: максимально возможной централизации управления безопасностью, уменьшения количества специализированных элементов, настройки приложений безопасности и т.д.

TCO = он DE + IC1 + IC2,

где DE (direct expenses) – прямые расходы;

IC1, IC2 (indirect costs) – косвенные расходы первой и второй группы соответственно.

Преимущества:

позволяет делать выводы о жизнеспособности проекта информационной безопасности только на основании оценки затрат.

предполагает оценку не только первоначальных затрат на создание ИБ, но и затрат, которые могут возникнуть на различных этапах жизненного цикла системы.

Недостатки:

компаниям стоит более тщательно подходить к анализу и исчислению затрат на ИТ;

требуется более глубокое понимание затрат, а именно их динамики и поведения в привязке к видам деятельности;

не учитывает риски и не позволяет кот соотнести технологию со стратегическими целями дальнейшего развития бизнеса и решением задачи повышения конкурентоспособности.

Анализ затрат на корпоративную информационную безопасность и методов оценки показывает, что эти методы ограничены оценкой чистой приведенной стоимости информационных активов HP и оценкой риска нарушения корпоративной информационной безопасности. Основной недостаток этих методов заключается в том, что эффективность инвестиций в информационную безопасность может быть достигнута только при их комбинированном использовании.

Согласно исследованию MarketsandMarkets, мировой рынок кибербезопасности растет и, по оценкам, достигнет $217,9 млрд в 2021 году." В ближайшем будущем успех социально-экономического и оборонного развития страны во многом будет зависеть от эффективности и скорости разработки и внедрения перспективных информационных технологий. Стратегия реализации национальной безопасности, принятая в июне того же года, позволяет нам думать в этом направлении. В нем также говорится, что разработка и внедрение этих технологий должны осуществляться с учетом соответствующих требований и методов информационной безопасности. «Технологии искусственного интеллекта (ИИ) можно охарактеризовать как технологии реализации того же самого», — сказал заместитель министра цифровой экономики Александр Шортов на заседании президиума Российской академии наук.

По подсчетам аналитиков Anti-Malware.ru, российский рынок кибербезопасности оценивается примерно в 142,6 млрд рублей и будет расти с ежегодным темпом 16-20% до 2023 года. gih MegaTrends оценивает мировой рынок кибербезопасности в 156,24 млрд долларов США в 2020 году и ожидается, что он достигнет 352,25 млрд долларов США в 2020 году. млрд, со среднегодовым темпом роста 14,5%.

Нападения на компании

По данным опроса более 4700 руководителей компаний из 23 отраслей с годовым объемом продаж не менее 1 млрд долларов США в 18 странах, проведенного консалтинговой компанией Accenture в марте-апреле этого года, за последние годы компании подвергались в среднем 270 кибератакам, что на 31% больше, чем в 2021 году. По сей день организации все чаще

сталкиваются с кибер-атаками, а потенциальная стоимость простоя, потери данных и цифрового выкупа заставляет владельцев бизнеса перераспределять ИТ-бюджеты в пользу повышения безопасности. Например, по данным исследования Gartner (проведенного среди 2 387 ИТ-директоров в 85 странах), 66% респондентов планируют увеличить инвестиции в кибербезопасность и внедрение информационной безопасности в 2022 году.

В прошлом году около 3% мирового ВВП было потрачено на борьбу с кибератаками, вызванными пандемиями, и компенсацию ущерба, нанесенного ими частным лицам и компаниям. По данным Cybersecurity jVentures, глобальные затраты на устранение последствий киберпреступлений будут расти на 15 процентов в год в течение следующих пяти лет и к 2025 году достигнут 10,5 трлн долларов США в год по сравнению с 3 трлн долларов США в 2015 году. К 2023 году ущерб, нанесенный хакерами, может достичь 6 триллионов долларов США.

В 2021 году США была подвержена нескольким громким кибератакам, в том числе атак на Colonial Pipeline, Управление пароходства Массачусетса, JBS (крупнейший в мире упаковщик мяса) и Департамент столичной полиции Вашингтона, округ Колумбия. Это были атаки программ-вымогателей, которые стали более частыми и изощренными, что подчеркивает важность кибербезопасности в нашем обществе. Атаки, подобные этим, могут значительно нарушить или даже отключить критически важную инфраструктуру, создавая дефицит, увеличивая стоимость товаров/услуг, финансовые потери из-за остановки операций и потери денег из-за необходимости платить выкуп хакеры. В Отчете о глобальных рисках Всемирного экономического форума за 2021 г., была произведена оценка, согласно которой «нарушение информационной безопасности» соотносят как четвертую наиболее вероятную угрозу миру после инфекционных заболеваний, финансового кризиса и природных катаклизмов.

По мере роста угрозы кибератак, защита компьютеров, сетей, программ и данных от несанкционированного или непреднамеренного доступа становится как никогда важной. В Вашингтоне Белый дом и Конгресс США обозначили проблему кибербезопасности важным вопросом национальной политики. В мае президент Байден издал «Распоряжение об улучшении национальной кибербезопасности», призвав внести ряд изменений в то, как страна реагирует на кибератаки и защищается от них, а также провозгласив, что «предотвращение, обнаружение, оценка и устранение киберинцидентов являются главным приоритетом и имеют важное значение для национальной и экономической безопасности». В дополнение к исполнительному распоряжению президент и лидеры Конгресса добавили ряд положений, связанных с кибербезопасностью, в законопроект об инфраструктуре. Более того, отчеты показывают, что расходы, связанные с кибербезопасностью, продолжают расти в правительственных федеральных агентствах и

вооруженных силах (Министерство обороны (DoD)). Расходы на кибербезопасность также выросли за пределами Вашингтона, отчасти из-за роста тенденции работы на дому, которая вынуждает компании платить за дополнительные протоколы и процессы для защиты конфиденциальных данных. Bloomberg сообщает, что к 2024 году расходы на кибербезопасность превысят 200 миллиардов долларов. Кроме того, недавнее исследование, проведенное IBM совместно, показало, что средняя общая стоимость утечки данных в 2021 году составляет 4,24 миллиона долларов, что больше, чем 3,86 доллара в 2020 году. Это исследование также показывает, что здравоохранение, финансовая и фармацевтическая отрасли в настоящее время имеют самые высокие затраты на утечку данных на компанию среди всех отраслей.

Увеличение частоты кибератак в сочетании с ростом финансовых потерь и сбоев, связанных с каждой из них, привело к тому, что кибербезопасность стала серьезной проблемой для инвесторов. На самом деле, многие системы экологического, социального и управленческого контроля (ESG) теперь рассматривают кибербезопасность в качестве основного компонента «S» или социальной составляющей.

С каждым годом растет не только количество киберпреступлений, но и уровень ущерба, наносимого компаниям". Несомненно, спрос на информационную безопасность будет только расти по мере дальнейшей цифровизации общества, а сектор кибербезопасности станет одним из ключевых секторов цифровой экономики", - сказал Руслан Мучипов, генеральный директор Tinkoff Capital.

Инвестиционная привлекательность сектора

Согласно исследованию PwC, 65% российских компаний ожидают увеличения расходов на кибербезопасность в 2022 году по сравнению с 52% в 2021 году. По данным исследования, 69% организаций ожидают увеличения бюджетов на кибербезопасность в 2022 году по сравнению с 55% в предыдущем году. Более четверти глобальных респондентов (26%) ожидают роста на 10% и более, по сравнению с 8% в 2011 году.

Рынок сейчас очень перспективен. Например, один из крупнейших в мире игроков, компания Palo Alto Networks, основанная в 2005 году, за три года заработала $3,1 млн и к 2021 году планирует достичь более $4 млрд. С момента IPO в 2012 году рост компании никогда не был ниже двузначного числа, и только однажды - во время Covid 2020 - он был ниже 20%.

Выход на биржу

На внутреннем и международном публичных рынках пока нет крупных российских игроков в сфере кибербезопасности, в отличие от их зарубежных коллег. Однако компания Positive Group (Positive jn Technologies), известная своей корпоративной кибербезопасностью, вышла на биржу в конце 2021 года.

Среди всех размещений АО "Positive Group" выделяется своей объективной и интересной историей развития, перспективами роста в сфере кибербезопасности и тем, что стала первой российской компанией в этом секторе, вышедшей на биржу. Клиентами компании являются более 2 000 компаний в России и СНГ.

Операционный директор компании, Максим Пустовой, рассказал на Московском веб-форуме "Противостояние", что компания рассматривает возможность выхода на биржу в конце этого года. Пустовой сказал, что нынешние и бывшие сотрудники компании, всего около 1 500 человек, будут владеть акциями в ходе IPO. По его словам, суть этого решения заключалась в том, чтобы стимулировать ключевых сотрудников компании и привлечь интерес талантливых людей со всей отрасли.

Прогноз по рейтингу Positive Group был недавно установлен на уровне "ruA-" рейтинговым агентством "Эксперт РА", как подчеркивается в отчете агентства. Данный уровень прогноза указывает на высокую вероятность повышения рейтинга в течение следующих 12 месяцев.

Подытожив, можно сказать, что в 2021-2022 году было большое количество целенаправленных атак, даже на российские банки.

В первую очередь при принятии бизнес-решений сравнивается разница между отражения кибератак, расходов и стоимостью подготовки. Как мы убедились, что даже малые утечки информации, которые не заинтересованы широкой публикой, могут дорого обойтись компаниям и влиять на её работу. Ещё одной причиной роста затрат служит изменение в законодательствах не как по России, но и по зарубежным странам. Компании или рискуют несоблюдением правил или адаптируются под новые правила. В таких обстоятельствах учитываются затраты и все возможные последствия. Возможно и по этой причине многие Российские и зарубежные компании увеличивают бюджет на информационную безопасность. Из-за роста ущерба от случаев атак именно те компании, которые считают вложения как инвестиции в безопасность и готовы тратить на их безопасность денежные средства будут лучше подготовлены к различным неприятностям. Так же инвестиции в информационную безопасность, в частности в кибербезопасность — это горячая ниша технологической индустрии, поэтому знание того, как инвестировать в них, может принести большую прибыль в предстоящее десятилетие.

Литература

1. Баранова Е. К. Информационная безопасность и защита информации // Учебное пособие, РИОР, 2021. – 336 с.

2. Гиротра, Каран Оптимальная бизнес-модель. Четыре инструмента управления рисками / Каран Гиротра. - М.: Альпина Диджитал, 2020. - 752 с.

3. Гришина, Н. В. Информационная безопасность предприятия. Учебное пособие / Н.В. Гришина. - М.: Форум, 2021. - 240 с.

4. Олькова А. Е. Финансовое моделирование инвестиционных проектов // Учебно-методическая литература — 2020. — 80 с.

5. Савчук В.П. Учебник «Оценка эффективности инвестиционных проектов» – Днепропетровск. Режим доступа: http://www.cfin.ru/finanalysis/savchuk/index.shtml (дата обращения: 22.04.2022).

СОВРЕМЕННЫЕ МЕТОДЫ ФОРМИРОВАНИЯ СТРАТЕГИИ РАЗВИТИЯ ОРГАНИЗАЦИИ

Кузьмин Александр Викторович, магистрант 2 курса кафедры управления
Научный руководитель: **Нефедьев Вячеслав Владимирович,** к.т.н., с.н.с., доцент кафедры управления

В современном обществе вопрос формулирования стратегии организационного развития имеет первостепенное значение в связи с новыми вызовами и обстоятельствами, с которыми сталкиваются компании в настоящее время. В данной статье рассматриваются современные подходы к формированию стратегий организационного развития. Особое внимание уделяется анализу существующих методов и выделению особенностей формирования текущей стратегии развития бизнеса.

Стратегия развития, методы, подходы, управление.

MODERN METHODS OF FORMING THE STRATEGY OF ORGANIZATION DEVELOPMENT

Kuzmin Alexander, 2nd year graduate student of the Department of Management
Scientific adviser: **Nefediev Vyacheslav**, Candidate of Technical sciences, Senior researcher, Associate professor of the Department of Management

In modern society the question of formulating an organizational development strategy is of utmost importance due to the new challenges and circumstances that companies face at the present time. In this article modern methods of formation of strategy of organizational development are considered. The special attention is given to the analysis of existing approaches and highlighting of features of the formation of the strategy of development of enterprises at the present time.

Development strategy, methods, approaches, management.

Современная теория стратегического менеджмента предлагает четыре основных подхода к созданию стратегии развития компании.

Разработка стратегии развития предприятия.

К. Эндрюс, А. Чандл, И. Ансофф, Д. Бавильски и другие исследователи этого подхода, имена которых здесь не упоминаются, стали его основателями. Суть этого метода заключается в предположении, что высшее руководство, используя имеющиеся данные, систематизирует их по степени важности и организует логистическую систему правил процесса

организационной деятельности. В результате планируется создать построчный процесс принятия решений [1, с.28].

Наиболее важными представителями этого подхода являются П. Друкер, Ф.-Котлер. Согласно этому подходу, в принятии управленческих решений можно выделить следующие этапы:

1) определение проблемы;

2) анализ ситуации;

3) принятие решения.

Проблема определяется как разница между желаемым и фактическим состоянием объекта или процесса. Чтобы решить проблему, необходимо определить цели, которых нужно достичь.

С точки зрения среднего, низшего, младшего и внешнего персонала (аутсорсеров), результат не ожидается. Сотрудники этих отделов должны следовать всем инструкциям и правилам, данным им в ходе работы. На основе этих инструкций, правил и рекомендаций по логически и стратегически организованной схеме работы должны быть разработаны более высокие разделы. В настоящее время готовится стратегия, которая будет касаться только высшего руководства и не будет иметь отношения к остальным. Это требует соблюдения строгой иерархии в компании [1, с.58].

На данный момент можно выделить следующие виды разработки стратегии развития организации, представленные на рисунке 1.

Исходя из данного подхода, стратегии разделяются по методам воздействия – внешние и внутренние. Внешние охватывают внешние факторы, которые влияют на организацию, внутренние же учитывают процесс протекающие непосредственно внутри организации.

Такой подход к разработке стратегии не является не этичным, поскольку вся информация о ситуации доступна каждому уровню управления. Однако существует риск, что стратегия, основанная на ограниченной информации, может оказаться недостаточно эффективной в определенных ситуациях (например, при сбое контроля).

Дж. В. Куинн предложил другой подход. Они сохранят свою должность и продолжат влиять на развитие бизнеса. Независимо от этого, данный подход является более инвазивным и инклюзивным, чем корпоративный подход. По сути, руководство решает все, но оно также определяет стратегию компании. Высшее руководство - это человек, который организует и оптимизирует процесс. Этот метод можно назвать итерационным подходом [1, с. 81].

Как мы знаем из вышесказанного, современная теория стратегического менеджмента выделяет четыре основных подхода к разработке корпоративной стратегии. Планируется, что разработка стратегии будет осуществляться высшим руководством без участия сотрудников.

Рисунок 1 – Виды корпоративных стратегий

Этот подход основан на том, что стратегия обычно представляет собой набор "стратегических идей", которые могут быть реализованы на практике. Эти идеи могут быть сформулированы в виде конкретных целей и стратегических планов. В любом случае, стратегия конкретизируется в план, который разрабатывается и реализуется каждой бизнес-единицей. В этом случае для реализации данного подхода необходимо лидерство высшего руководства: итеративное планирование требует достаточно высокой культуры стратегического мышления среди старших и младших менеджеров.

Следующий метод аналогичен методу Дж.У. Куинна. За исключением того, что вместо глобальных и просчитанных целей планирования устанавливаются простые правила и низкие цели, чтобы организовать более простой и надежный процесс. Интуитивный подход к процессу работы с клиентами предполагает постоянную адаптацию переговорного процесса. Необходимо разработать руководящие принципы для этого подхода и предпринимать небольшие шаги и регулярно их отрабатывать.

Таким образом, данный подход предполагает, что стратегия обычно представляет собой набор "стратегических идей", которые могут быть реализованы на практике. Индивидуальная стратегическая программа разрабатывается в каждом конкретном случае.

В любом случае формирование стратегии связано с прохождением этапов стратегического планирования, данные этапы представлены на рисунке 2.

Рисунок 2 – Этапы стратегического планирования

Как видно из рисунка, все начинается с постановки цели и определения миссии, поэтому бизнес-стратегии должны быть достаточно гибкими, чтобы адаптироваться к требованиям рынка, экономическим и культурным изменениям. Фактически, интуитивный подход основан на том, что менеджеры принимают решения на основе интуиции, а не логики. Такой подход уместен в ситуациях, когда менеджеры хорошо знают свой рынок, конкурентов и клиентов. Процесс принятия решений должен быть максимально интуитивным и отвечать на вопросы:

- С какими проблемами сталкивается организация.
- Каковы сильные и слабые стороны организации.
- Возможности и угрозы, которые могут возникнуть на рынке.
- Существующие изменения в окружающей среде, которые влияют на организацию [1, с.53].

Основываясь на следующем подходе, Р. Ричардсон и Б. Ричардсон предлагают, что стратегия должна заключаться в том, что каждое решение должно рассматриваться и приниматься на основе этих вопросов и лиц и приниматься независимо. Однако, как таковое это решение нельзя назвать

типом планирования. Этот тип планирования чаще всего практикуется в хаотичном порядке и используется относительно редко.

Таким образом, в целостном виде формирование стратегии развития предприятия можно рассмотреть на рисунке 3.

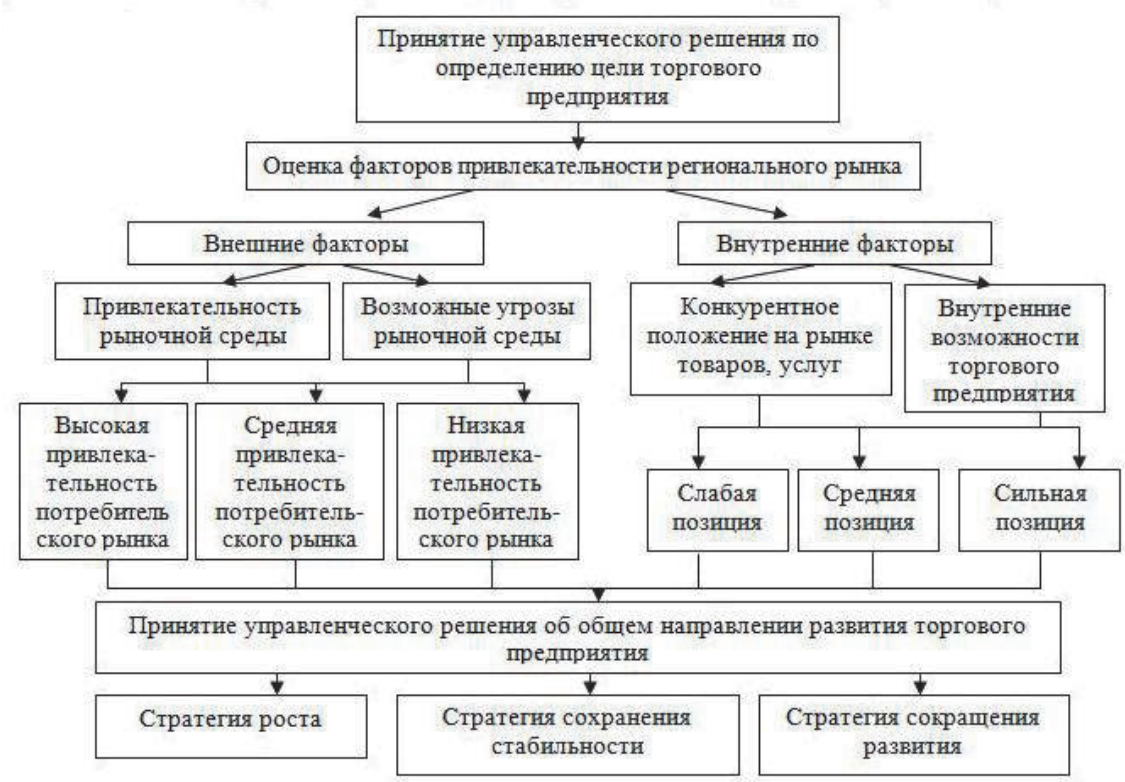


Рисунок 3 – Этапы принятия управленческого решения по определению стратегии предприятия

Для достижения целей в условиях неопределенной конкурентной среды необходимо выбрать направление, в котором будет двигаться компания, а также определить проблемы, которые могут возникнуть в ходе деятельности компании. Следует иметь в виду, что у каждой компании свои проблемы. Однако ни один из них не следует полностью игнорировать. Если это произойдет, это может привести к потере их конкурентоспособности. Однако существуют определенные категории проблем, которые характерны для каждой компании.

Это требует выбора направления - определения целей и задач компании. Это связано с тем, что в зависимости от размера компании или отрасли у компании могут быть разные проблемы и, соответственно, разные цели для достижения. У компании также может не быть четкой цели. Здесь цели необходимо выбирать из ряда целей, которые ставятся перед компанией.

Таблица 1 – Стратегия развития предприятия к реализации и формированию со стороны методических подходов различных учёных [2, с. 109-115]

Автор подхода	Процесс формирования и реализации стратегии
И. Ансофф	- внутренняя оценка компании; оценка внешних возможностей; формулировка целей и выбор целей; решения по портфельной стратегии; конкурентная стратегия; разработка, выбор и реализация альтернативных проектов.
С. Вутон, Т.Хорн	- стратегический анализ: анализ внешней среды; анализ; внутренняя среда; совокупная оценка внешней и внутренней среды. - выбор стратегического направления: прогнозирование; определение миссии и целей; выявление стратегических несоответствий между прогнозами и целями. - реализация стратегии: рассмотрение альтернатив стратегии; анализ каждой альтернативы с точки зрения конкурентоспособности, совместимости, осуществимости, риска и т.д.; разработка плана реализации стратегии.
А. Томпсон, Д.Стрикланд.	- определение сферы деятельности и формулирование стратегических направлений. - постановка стратегических целей и задач для их достижения. - формулирование стратегий для достижения операционных целей и результатов. - реализация стратегического плана - оценка эффективности и изменение плана и/или способа его реализации.
М.Мескон	- выработка миссии; определение целей организации; оценка и анализ внешней среды; изучение сильных и слабых сторон менеджмента; анализ стратегических альтернатив; реализация и оценка стратегии.
В. Маркова, С. Кузнецова	- определение цели - анализ «пробелов», включающий оценку внешнего и внутреннего окружения - формулирование стратегии, с учетом рассмотрения альтернативных вариантов - реализация стратегии на основе составления планов и бюджетов
О. Виханский	- анализ среды; определение миссии и целей; выбор стратегии; выполнение стратегии; оценка и контроль реализации стратегии
О.П. Коробейников	- анализ: оценка внешнего и внутреннего окружения; определение миссии; формулировка целей - планирование - реализация: разработка планов; проведение структурных изменений - контроль: формирование бюджетов; оперативное управление; оценка и контроль

Следует помнить, что цели компании и цели конкретных отделов могут не совпадать. Например, цели отдела могут быть связаны с достижением общекорпоративных целей, а общекорпоративные цели могут быть связаны с целями отдела. Выбор корпоративных целей - это процесс, который начинается с выбора целей отделов и заканчивается определением общих целей организации [2, с.10].

Однако важно отметить, что цели - это инструмент для мониторинга положения компании и управления ее развитием.

Как уже упоминалось выше, такая точка зрения не учитывает вклад других подходов к организации предприятия с точки зрения планирования или, глядя на реалии планирования предприятия, многие организационные аспекты не принимаются во внимание. Он игнорирует итерационный подход, который подходит для данного случая. Иногда стратегия может возникнуть спонтанно из различных областей системы предприятия. Как правило, в большинстве случаев стратегия отсутствует, а действия предпринимаются без учета всех возможных сценариев. Полное отсутствие стратегического планирования.

В этой таблице обобщено отношение исследователей к различным подходам к методологии реализации стратегии.

Особенности, которые необходимо учитывать при анализе различных подходов к разработке стратегий эффективного развития бизнеса.

- Бизнес должен реагировать на внешние и внутренние изменения, следуя концепции Игоря Ансоффа, который рассматривает реализацию стратегии как две системы. Одна из систем должна реагировать на изменения и своевременно устранять их, а другая - управлять всей организацией при прогнозировании будущего развития событий.

- В каждой методологии есть этап анализа внешней и внутренней среды компании.

- Многие авторы включают оценку стратегических результатов в отдельный заключительный этап.

Как мы уже говорили, все эти стратегии и подходы к их реализации предполагают использование определенных инструментов, которые способствуют их полноценной реализации. Другие инструменты облегчают мониторинг ситуации на внутреннем рынке, на внешнем рынке. Некоторые инструменты, например, помогают изучать ситуацию в глобальной среде.

Несмотря на разнообразие подходов к стратегиям развития бизнеса, все они концептуально похожи и содержат схожий алгоритм, состоящий из трех этапов «анализ - разработка концепции - оценка эффективности концепции» [3, с. 151].

На адаптацию стратегии к специфике деятельности предприятия и требованиям рынка влияет выбор инструментов для анализа внешней и внутренней среды, формирование стратегии управления.

Литература

1. Мировая экономика и международные экономические отношения: современное состояние, проблемы и основные. тенденции развития: Учебник / Е. Д. Фролова, С. А. Лукьянова. – Екатеринбург: УрФУ, 2016. – 184 с

2. Коробейников, О.П. Стратегическое поведение: от разработки до реализации / О.П. Коробейников, В.Ю. Колесов, А.А. Трифилова. – Москва: ИНФРА М, 2020. – 1438 с.

3. Ефремов, В.С. Стратегия бизнеса. Концепции и методы планирования: учеб. пособие / В.С. Ефремов. – Москва: ИНФРА-М, 2018. – 112 с.

ПРОБЛЕМЫ ВЫБОРА СТРАТЕГИИ РАЗВИТИЯ ПРЕДПРИЯТИЯ

Кузьмин Александр Викторович, магистрант 2 курса кафедры управления
Научный руководитель: **Нефедьев Вячеслав Владимирович**, к.т.н., с.н.с., доцент кафедры управления

Новые вызовы и условия, которые возникли в современном обществе в следствии влияния множества факторов, в том числе пандемии COVID-19 вынуждают организации изменять или же разрабатывать новые стратегии организационного развития. В данной статье рассмотрены проблемы, с которыми сталкиваются организации при определении или коррекции стратегии своего развития.

Стратегия развития, методы, подходы, управление.

PROBLEMS OF CHOOSING THE ENTERPRISE DEVELOPMENT STRATEGY

Kuzmin Alexander, 2nd year graduate student of the Department of Management
Scientific adviser: **Nefediev Vyacheslav,** Candidate of Technical sciences, Senior researcher, Associate professor of the Department of Management

New challenges and conditions which emerged in modern society as a result of the impact of many factors, including the COVID-19 pandemic, force organizations to change or work out new strategies of organizational development. In this article the problems which organizations face at definition or correction of strategy of the development are considered.

Development strategy, methods, approaches, management.

В современной экономике стратегия является основой управления бизнесом, а качественная стратегия развития - залогом экономического роста. Долгосрочная стабильная деятельность компании, ее экономический рост, определяется квалифицированным выбором стратегии развития [1].

Для начала рассмотрим основные типы стратегий развития, представленные на рисунке 1.

Рисунок 1 – Основные виды стратегий развития организации

Для того чтобы оценить положение компании на рынке, необходимо оценить и понять будущие возможности с помощью стратегического анализа. Невозможно стандартизировать процесс разработки стратегии или создать стандартные модели поведения, применимые к различным экономическим агентам, поскольку деятельность, управление и ситуация каждого предприятия уникальны [4].

Однако в долгосрочной перспективе существуют фундаментальные факторы, которые позволяют компаниям выбрать правильную стратегию своего развития.

Стратегическая позиция, тенденции рынка и необходимый запрос на рынке — это самые важные показатели для анализа и что бы их понять необходимо провести анализ производственно-хозяйственной деятельности [6].

Корпоративная стратегия – это комплекс тактических мер, направленных для развития бизнеса и достижения соответствующих целей. Он должен быть разработан с учетом приоритетов поставленных целей и задач, которые определяются исходя из оценки текущих обстоятельств и перспектив развития компании. Стратегия – это четко сформулированный алгоритм действий, направленных на повышение эффективности деятельности предприятия. Обычно стратегия приносит положительные

результаты, когда в процессе принятия решений участвуют как собственники, так и сотрудники компании.

При разработке стратегии предприятия необходимо определить его будущую деятельность. Разработка стратегии включает в себя определение миссии фирмы, постановку долгосрочных целей и план действий с четким графиком.

Стратегия – это деятельность предприятия, направленная на использование имеющихся ресурсов для достижения различных результатов, влияющих на его положение в окружающей среде. Стратегия развития включает в себя несколько основных моментов: экономическое развитие, техническое и технологичное развитие, корпоративная культура, организационно-управленческое развитие. С точки зрения стратегии, основной аспект – это экономическое развитие.

Разработка общей корпоративной стратегии проходит в несколько этапов.

Первым этапом разработки стратегии является анализ макро- и микросреды, изучение внутренних и внешних факторов. Макросреда - факторы, которые не оказывают прямого влияния на деятельность организации [3]. Микросреда - субъекты (поставщики, клиенты, контактные группы), которые оказывают непосредственное влияние на деятельность компании [4].

Второй шаг в разработке стратегии - определение миссии, направления и целей предприятия. Заявление о миссии - это качественно выраженный набор основных целей и бизнес-задач организации, который определяет состояние организации и обеспечивает направление и руководство для постановки целей и стратегий на разных уровнях развития [1].

Последний этап - стратегический анализ, в ходе которого направления и цели бизнеса сопоставляются с результатами анализа внешней и внутренней среды. После сопоставления результатов анализа окружающей среды с целями компании разрабатываются возможные альтернативные варианты стратегии.

В современных экономических условиях стратегическое планирование является важным направлением для эффективного функционирования и дальнейшего развития компании в конкурентной рыночной среде. Стратегия определяет основные приоритетные направления развития компании и позволяет учесть основные возможности и угрозы, связанные с внешними факторами и внутренними процессами управления. Стратегическое планирование также способствует формированию конкурентоспособности и финансовой устойчивости предприятия. В связи с этим целью данной работы является изучение взаимосвязанных внутренних и внешних факторов для сравнительного анализа теоретических и методологических подходов к эффективному стратегическому планированию развития предприятия [1].

Стратегический анализ служит механизмом стратегического управления, способствующим оценке деятельности предприятия с целью определения наиболее приоритетных направлений инвестиционных ресурсов для дальнейшего развития предприятия. Это оптимальное распределение ресурсов для достижения поставленных целей, процесс постановки целей и задач, определение комплекса мер по их реализации. Реализация стратегического планирования требует соблюдения определенных принципов, наиболее важными из которых являются: комплексность, последовательность реализации, измеримость целей, осуществимость и эффективность. Существуют еще методологические подходы к оценке результатов реализации стратегических планов предприятий. Анализ существующих методик позволил нам систематизировать наиболее распространенные подходы, основанные на изучении официальных документов организаций (цели, задачи, мероприятия, механизмы реализации), анализе взаимодействия местных органов власти со стейкхолдерами (с местным населением и т.д.), анализе экспертных оценок и опросов, а также сравнительном анализе фактически достигнутых значений с запланированными [2, 3].

В. С. Жихаревич также провел углубленное исследование, посвященное анализу результатов эффективности стратегического планирования. В своем подходе он рассматривал следующие внутренние факторы: размер и статус города (района), органы власти, активность общества (местного населения), уровень квалификации специалистов, работников предприятий и заводов города (района), стратегическое планирование со стороны региональных властей, наличие программ со финансирования и другие.

Среди существующих научных работ стоит отметить исследовательскую работу Е. А. Илинбаев. В статье предлагается оценка эффективности региональных стратегий на основе экспертных оценок по качественным критериям, а именно: институционализация условий планирования, характеристики стратегических направлений, описание механизмов реализации стратегии, уровень достижения стратегических целей, доступность и полнота информации о стратегии [4, 5].

Проанализировав вышеперечисленные методологии и подходы ученых, к преимуществам данных методов относят оценку качественных характеристик стратегического планирования предприятия, практическую направленность, всесторонний охват процесса разработки и реализации стратегии, а к недостаткам - субъективность и высокую стоимость организации экспертных оценок [5].

Данный стратегический анализ производиться для более эффективной работы и реализации компании на рынке. Для этого изучается внешняя среда и проводится оценка ресурсов, которыми располагает сама компания и её

конкуренты. Эти данные определяют дальнейшее направление развития компании.

В ходе данного анализа на приводиться так же конкуренты для анализа слабых и сильных сторон [8].

Данный анализ проводится для улучшения эффективности выявления проблем в оптимизациях процесса и конкурентных решений что помогут улучшить положение на рынке. Этот анализ проводится с помощью оценки ресурсов, которыми располагает компания, рассматриваться перспективы роста и принимаются оптимальные стратегии. Путём данных махинаций усилия направляются на улучшения экономических показателей и улучшают конкурентные стратегии [3].

Выбор стратегий из всех возможных является процессом индивидуальным для каждой компании, где будет проводиться анализ. Выбор стратегии зависит от факторов, которые влияют на организацию рабочего процесса и зависит от основной деятельности компании, основной вид руководства и основной приоритет компании [2]. Так же необходимо учитывать возможные пути, с помощью которых осуществляется диверсификация производства.

На рисунке 2 алгоритм выбора стратегии для развития организации.

Рисунок 2 – Алгоритм выбора стратегии развития организации

Выбор стратегии подразумевает сравнение того какие результаты для данного момента были желаемы и ожидаемы. Данные сравнения показывают недостатки реализации стратегии или неправильный выбор стратегии. При правильной постановке целей и задач развития необходимо постоянно поддерживать конкурентное преимущество и четко определять цели.

Учитывать сильные и слабые стороны данного бизнеса и правильно их оценивать. Зная так же и внешние угрозы необходимо постоянно своевременно и к месту внедрять новейшие технологии, которые значительно улучшат выход данного направления [4]. Так же необходимо постоянно оценивать ситуацию и положения конкурентов, и не во всех случаях лидерство конкурентов является экономически не выгодно и необходимо проводить анализ для точного определения ситуации.

Для того что бы все вышеперечисленные анализы провести с последующим улучшением эффективности компании, компания должна выбрать основной сценарий развития стратегии, в которой первостепенным выступает основное конкурентное преимущество на рынке [5].

Так же необходимо не забывать о постоянной лабильности рынка и рассматривать альтернативные варианты развития выбранной стратегии может помочь сохранить конкурентное преимущество.

После выбора базовой, т.е. основной, стратегии бизнеса необходимо определить, как ее реализовать. В этом случае возможны следующие варианты: остаться на прежнем уровне, принять решение о выходе из определенных сегментов рынка, освоить новые сегменты рынка и рыночные ниши, спроектировать и разработать новые линейки продуктов, использовать проникновение на рынок, то есть продавать продукты с высоким экономическим эффектом.

После окончательного выбора направления реализации подхода к стратегии стоит приступить к выборам метода ее практической реализации и установлением методов ее действия.

Стоит принять во внимание три отличных от основных методов, которые предлагают Джонсон и Шоулз: франчайзинг, собственная разработка и собственное развитие.

Процесс открытия бизнеса означает вложения материальных, финансовых, и аналитических ресурсов. Человек инвестирует ресурсы в разработку, освоение рынка и производство новых услуг или продуктов.

Рассмотрение стратегических вариантов является следующим шагом для установки стратегии. Для определения лучших вариантов следует руководствоваться следующими критериями.

Пригодность – необходима ли данная стратегия для определённых целей и задач.

Приемлемость – стоит ли эта стратегия и её выгода поставленных рисков.

Осуществимость – то есть возможно ли при наличии имеющихся ресурсов применять данную стратегию.

Из всех данных критериев можно сократить количество критериев для выбора поставив один из них ключевым.

Последним этапом стоит установка стратегически продуманных целей развития и постановку оперативных целей. Экономические плановики следят

за ежедневным наличием небольших ежедневных целей и регулярных задач, что позволит обеспечить прибыльность компании в виде соблюдения плана организации бизнеса.

Именно поэтому каждый экономический субъект должен разработать свою собственную стратегию, учитывая индивидуальные особенности компании, ее положение на рынке и макроэкономические факторы. Это, в свою очередь, требует от компании наличия квалифицированных специалистов, способных применять современные методы стратегического управления, или привлечения внешнего персонала.

Любой из этих двух вариантов приведет к дополнительным расходам. Систематическая работа по разработке алгоритма разработки стратегии для конкретной компании может помочь снизить эти затраты в будущем и, что самое главное, повысить эффективность разрабатываемых и реализуемых стратегий. Такой алгоритм должен быть основан на процессном подходе, современных достижениях стратегического менеджмента и текущей бизнес-диагностике компании.

Литература

1. Болдырева Т.В., Плеханов С.В. Расстановка приоритетов компании в стратегическом планировании, как средство достижения конкурентного преимущества в условиях рынка / Сборник: Интеграционные процессы современного развития социально-экономических систем. Материалы всероссийской научно-практической конференции. Под общей редакцией И. В. Кузнецовой. 2018. С. 24-29.

2. Волошин И.П., Самойленко А.В. Эффективность SEO-оптимизации / В сборнике: Цифровые технологии в экономике и образовании. Сборник научных трудов по итогам межвузовской научно-практической конференции. 2019. С. 65-69.

3. Ключников С.В. Особенности аналитического обеспечения сегментарной отчетности корпоративной группы // Управление экономическими системами: электронный научный журнал. 2019. No 12. (36). С. 56.

4. Кублин И.М., Санинский С.А. Проблемы управления предприятиями аграрного сектора и направления их решения // Вестник Саратовского государственного социальноэкономического университета. 2018. No 3 (52). С. 48-52.

5. Найденков В.И., Мартынович В.И., Миронов М.Г. Малое и среднее предпринимательство саратовской области: показатели развития и формы государственной поддержки // Вестник Саратовского государственного социально-экономического университета. 2019. No 5 (79). С. 67-71.

6. Кублин И.М., Махметова А.Ж.Е. Системная модернизация предприятий машино-строительной промышленности: категорийно-

понятийный подход// Известия Волгоградского государственного технического университета. 2012. No 7 (94). С. 51-54.

7. Соловьев А.Н., Найденков В.И. Влияние внешней среды на развитие малого предприятия // Наука и общество. 2019. No 1 (24). С.82-86.

8. Шарапов Ю.В., Юринская Ю.А. Стратегия мероприятий для поддержки и повышения эффективности хозяйственной деятельности предприятия // Инновации в науке. 2016.No10(59). С.189-196.

ИССЛЕДОВАНИЕ ИМПЛЕМЕНТАЦИИ ПАРСИНГА ТЕКСТОВОГО СОДЕРЖИМОГО ДЛЯ ОДНОСТРАНИЧНЫХ ВЕБ-ПРИЛОЖЕНИЙ

Лобанов Григорий Вячеславович, Строкин Александр Сергеевич,
магистранты 2 курса кафедры математики и естественнонаучных дисциплин
Научный руководитель: **Логачева Надежда Вадимовна**, к.т.н., доцент кафедры информационных технологий и управляющих систем

В ходе данной работы было проведено исследование имплементации парсинга текстового содержимого для одностраничных веб-приложений. Были описаны методы парсинга для веб-приложений с клиентским и серверным рендерингом, и выделена особенность, осложняющая получение данных при использовании клиентского рендеринга. Было разработано приложение, реализующее рендеринг веб-страницы на клиенте и выполняющее парсинг текстового содержимого страницы. Результаты исследования позволяют реализовать парсинг текстового содержимого для одностраничных веб-приложений с клиентским рендерингом.

Парсинг, рендеринг, веб-приложение.

RESEARCH ON THE IMPLEMENTATION OF TEXT CONTENT PARSING FOR SINGLE-PAGE WEB APPLICATIONS

Lobanov Grigoriy, Strokin Alexandr, 2nd year graduate students of the Department of Mathematics and natural sciences
Scientific adviser: **Logacheva Nadezhda**, Candidate of Technical sciences, Associate professor of the Department of Information technologies and control systems

In the course of this work, a study was made of the implementation of text content parsing for single-page web applications. Parsing methods for web applications with client and server rendering were described, and a feature was highlighted that complicates data acquisition when using client rendering. An application was developed that renders a web page on the client and parses the text content of the page. The results of the study make it possible to implement text content parsing for single-page web applications with client-side rendering.

Parsing, rendering, web application.

По мере развития сети интернет и роста актуальных требований к веб-сайтам происходит постоянное совершенствование подходов и технологий разработки современных веб-интерфейсов. В последнее время при разработке веб-интерфейсов всё чаще применяется подход одностраничных

веб-приложений. При таком подходе рендеринг веб-страниц выполняется на клиенте (в браузере пользователя) что отличается от классического сценария рендеринга на стороне сервера. Это препятствует получению и дальнейшему парсингу содержимого веб-страниц. В данной работе будет исследован метод, позволяющий обойти данное ограничение при парсинге одностраничных веб-приложений и будет реализовано простое приложение, для подтверждения работоспособности этого метода.

Среди ключевых преимуществ одностраничных веб-приложений выделяют возможность динамической генерации HTML-разметки с использованием языка программирования JavaScript. Это даёт возможность проектировать и реализовывать веб-интерфейсы, содержащие множество интерактивных элементов, состоянием которых можно удобно и производительно управлять. Всё взаимодействие с одностраничным веб-приложением выполняется на единственной HTML-странице, что является следствием динамического изменения разметки. Также к преимуществам этого подхода относят высокую производительность и практически моментальный переход по внутренним ссылкам веб-сайта.

Но, несмотря на описанные выше преимущества, одностраничные веб-приложения имеют некоторые ограничения: поскольку HTML-разметка таких веб-сайтов генерируется языком JavaScript в браузере, то получить содержимое страницы сразу, при обращении к серверу, невозможно. В ответ на запрос сервер вернёт только минимальную HTML-разметку страницы, как правило, содержащую секцию head, с минимальным набором мета-тегов, и body, внутри которой будет находиться элемент с id в котором будет происходить рендеринг самого веб-приложения на клиенте.

На данный момент эти ограничения можно обойти, используя при разработке одностраничного веб-приложения серверный рендеринг на JavaScript, с последующей регидратацией на клиенте. Это необходимо для корректной индексации веб-сайта роботами поисковых систем, а также для некоторого улучшения производительности веб-приложения при его первичной загрузке. Но технологии поисковых систем также активно развиваются. Поисковая система Google с 2015 года способна корректно обрабатывать сайты, использующие клиентский рендеринг. В случае поисковой системы Яндекс ситуация несколько сложнее — поисковик не способен на данный момент корректно анализировать веб-приложения с клиентским рендерингом и предлагает размещать копии страниц на сервере. Следовательно, имплементация парсинга одностраничных веб-приложений является актуальной задачей.

Для веб-приложений выделяют два основных типа рендеринга: клиентский и серверный.

"SSR (Server-Side Rendering, серверный рендеринг) — рендеринг на сервере клиентской части или универсального приложения в HTML" [2].

"CSR (Client-Side Rendering, рендеринг на клиенте) — рендеринг приложения на стороне клиента (в браузере), обычно с помощью DOM" [2].

При серверном рендеринге отправляется запрос на сервер, а он в ответ отправляет полностью сгенерированную HTML-разметку страницы, что позволяет исключить дополнительные запросы с клиента, потому что сервер берёт на себя основную задачу по формированию страницы.

Этот подход даёт возможность сократить время до первой отрисовки и первой содержательной отрисовки на клиенте. Исполнение логики по формированию страницы и рендеринг на стороне сервера сокращают объём JavaScript кода, пересылаемого пользователю, сокращая время до первой интерактивности веб-интерфейса. Серверный рендеринг хорошо себя зарекомендовал на широком диапазоне устройств и позволяет использовать браузерные оптимизации, например, потоковый парсинг документа.

Большинство современных фронтенд фреймворков и библиотек предоставляют возможности для рендеринга и на клиенте, и на сервере. Стоит отметить, что подобные решения относятся к отдельному классу, со своими преимуществами и недостатками.

Процесс рендеринга на клиенте предполагает формирование страниц с использованием JavaScript напрямую в браузере. Это даёт возможность частично разгрузить сервер и перенести всю логику или её часть, а также получение данных, шаблонизацию и маршрутизацию на клиент.

Этот тип рендеринга имеет один существенный недостаток – непросто сохранять высокую скорость работы на мобильных и непроизводительных устройствах. Чтобы ускорить рендеринг приложения и приблизиться к результативности серверного рендеринга требуется выполнить несколько серьёзных оптимизаций и соблюсти ряд ограничений. Схожей с серверной скорости рендеринга можно добиться, если сократить задержки при доставке критически важного JavaScript и данных, отправляя их с помощью протокола HTTP/2 Server Push или мета-тега <link rel=preload>, что позволит парсеру браузера заранее заняться подготовкой этих ресурсов. Также стоит обратить внимание на паттерн PRPL, объединяющий в себе все самые популярные практики по оптимизации загрузки страниц, так как они значительно ускоряют первую загрузку и переходы между страницами.

Главным минусом рендеринга на клиенте является требуемый для функционирования объём JavaScript, который растёт с развитием веб-приложения. Дополнительно ситуация усугубляется при использовании полифиллов, сторонних JavaScript библиотек и прочего внешнего кода, которые создают дополнительную вычислительную нагрузку на процессор и увеличивают расход оперативной памяти, в процессе формирования страницы, что также замедляет её отрисовку. Приложения, использующие этот тип рендеринга, должны озаботиться разделением JavaScript-бандла на меньшие части и использовать lazy loading, для этих частей, чтобы на клиент доставлялся только необходимый в текущий момент объём кода.

Ключевой проблемой современной сети Интернет является избыточность информации, которую человек не имеет возможности систематизировать вручную. Одним способов решения этой проблемы является парсинг.

"Парсинг — это автоматизированный сбор неструктурированной информации, ее преобразование и выдача в структурированном виде. Парсинг включает в себя множество аспектов: выборка необходимой информации с сайта-источника, распознавание и преобразование информации, создание структурированного хранилища" [1, С.214].

"Существует несколько способов создания программы или скрипта парсера. Принцип его действия зависит от наших целей. Парсер ищет на указанном нами сайте или страницах данные, соответствующие заданным нами параметрам, собирает полученную информацию, с которой производится первоначальная систематизация." [1, С.214]

"Независимо от выбора языка программирования, принцип действия парсера остается схож. Происходит формирование запросов в виде кода к XHTML документам (страницы сайта) или их отдельным элементам. Далее парсер извлекает необходимую нам информацию, указанную в коде-запросе (картинки, заголовки, текст) и сохраняет ее" [1, С.214].

В случае одностраничных веб-приложений с клиентским рендерингом такой же подход к парсингу, как в случае серверного рендеринга — невозможен, так как сервер не возвращает полную структуру веб-страницы. Для решения данной проблемы необходимо использовать предварительный рендеринг страницы на клиенте, что позволит получить полное содержимое веб-страницы и в дальнейшем парсить её содержимое.

Для реализации парсинга веб-сайтов с клиентским рендерингом было принято решение воспользоваться языком программирования C# по следующим причинам:

- Распространяется по лицензии MIT [3], что позволяет без ограничений распространять и писать приложения на основе платформы .NET;
- Обладает многоязычной и обширной документацией [4];
- Имеет свободный доступ к репозиторию платформы [5] и исходному коду языка [6];

Приложение было реализовано с использованием универсальной платформы Windows (UWP). Ключевым элементом управления, благодаря которому был успешно получен доступ к HTML-разметке веб-документа, является WebView.

WebView — это интерактивный компонент UI-библиотеки для UWP приложений, реализующий рендеринг веб-страниц. Загружаемый HTML-код может быть представлен как код веб-страниц с веб-сайтов, код локальных страниц или код HTML, который формируется программными средствами.

Данный компонент можно считать веб-браузером с ограниченным функционалом.

Следует отметить ряд особенностей WebView:

- "этот элемент не поддерживает большинство событий ввода, которыми обладают другие элементы управления;" [7]
- "для рендеринга он использует движок Microsoft Edge;" [7]
- "он не поддерживает элементы ActiveX, плагины, а также некоторые функциональности HTML5, в частности, AppCache, IndexedDB, программный доступ к буферу обмена, геолокацию; " [7]
- "он поддерживает навигацию по ресурсам, использующим протоколы HTTP, HTTPS, ms-appx-web и ms-appdata" [7]

Для проверки работоспособности метода было разработано простое приложение (рисунок 1). Оно получает на вход URL-адрес и по нажатию на кнопку «Выполнить рендеринг» выполняет рендеринг страницы в фоне. После завершения процесса HTML-разметка страницы выводится в текстовое поле. Далее после нажатия на кнопку «Парсинг заголовков» — выполняется парсинг разметки документа и выводится список полученных заголовков в текстовое поле.

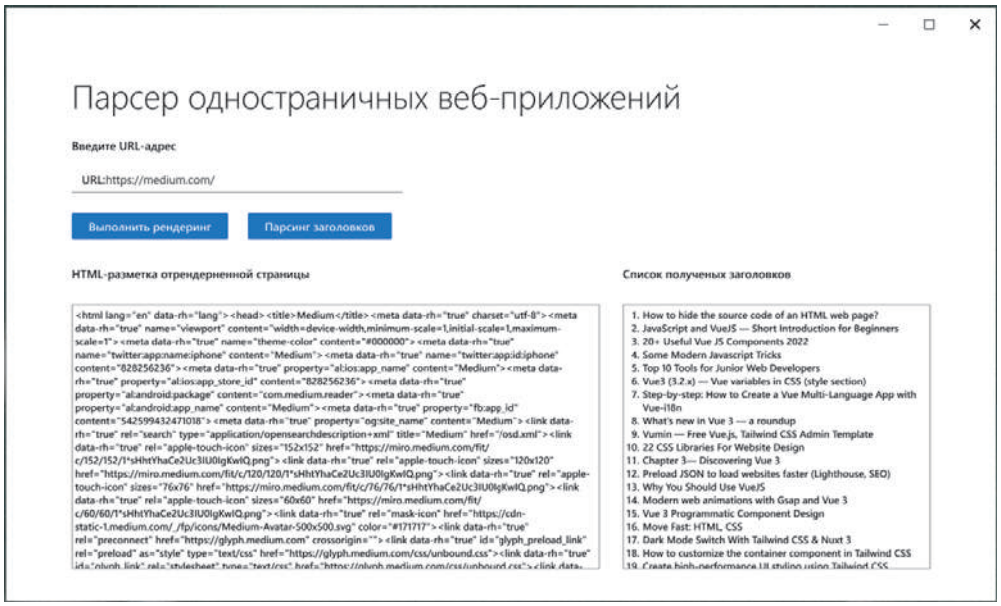


Рисунок 1 – Результат работы приложения

Изучение исходной HTML-разметки (рисунок 2) и полученной после рендеринга показало, что рендеринг страницы был успешно выполнен на клиенте. Это позволило выполнить парсинг страницы и получить список заголовков.

Рисунок 2 – Фрагмент исходной разметки страницы

Следовательно, опытным путём на примере парсинга заголовков была доказана возможность имплементации парсинга одностраничных веб-приложений. Данный метод отличается от парсинга приложений с серверным рендерингом, а именно клиентский рендеринг усложняет процесс парсинга и затрудняет доступ к данным.

Литература

1. Васильев, Н. С. Использование технологии парсинга в разработке новых материалов / Н. С. Васильев // Мавлютовские чтения: материалы XV Всероссийской молодежной научной конференции: в 7 томах , Уфа, 26–28 октября 2021 года. — Уфа: Уфимский государственный авиационный технический университет, 2021. — С. 214-216. — EDN LXHTSG.

2. Серверный или клиентский рендеринг на вебе: что лучше использовать у себя в проекте и почему [Электронный ресурс]. Режим доступа: https://tproger.ru/translations/rendering-on-the-web/ (дата обращения: 01.03.2022).

3. C Sharp [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/C_Sharp#Стандартизация (дата обращения: 08.03.2022).

4. C# documentation [Электронный ресурс]. Режим доступа: https://docs.microsoft.com/en-us/dotnet/csharp/ (дата обращения: 02.02.2022).

5. .NET Runtime [Электронный ресурс]. Режим доступа: https://github.com/dotnet/runtime (дата обращения: 08.03.2022).

6. References Source [Электронный ресурс]. Режим доступа: https://referencesource.microsoft.com/#mscorlib/system/console.cs (дата обращения: 12.03.2022).
7. WebView [Электронный ресурс]. Режим доступа: https://metanit.com/sharp/uwp/4.12.php (дата обращения: 17.03.2022).

ЦИФРОВИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО КОНТЕНТА – ВАЖНАЯ СОСТАВЛЯЮЩАЯ ВЫСОКОЭФФЕКТИВНЫХ НАЦИОНАЛЬНЫХ ИННОВАЦИОННЫХ СИСТЕМ

Малюсин Юрий Владимирович, магистрант 1 курса кафедры управления качеством и стандартизации
Научный руководитель: **Попова Юлия Сергеевна**, к.э.н., доцент кафедры управления качеством и стандартизации

В статье рассматривается информационное обеспечение, как важная составляющая качества образовательного контента, по средствам создания опорной инфраструктуры цифровой экономики. Стоит так же отметить важность участия государства и частного бизнеса в создании данной опорной инфраструктуры, в том числе безопасных линии связи и центров обработки данных. И не стоит забывать о цифровой грамотности и необходимости кратно увеличить выпуск специалистов в сфере цифровой экономики.

Цифровая экономика, цифровизация, инновационные системы.

DIGITALIZATION OF EDUCATIONAL CONTENT IS AN IMPORTANT COMPONENT OF HIGHLY EFFECTIVE NATIONAL INNOVATION SYSTEMS

Malyusin Yury, 1st year graduate student of the Department of Quality management and standardization
Scientific adviser: **Popova Yulia**, Candidate of Economic sciences, Associate professor of the Department of Quality management and standardization

The article considers information support as an important component of the quality of educational content, by means of creating the supporting infrastructure of the digital economy. It is also worth noting the importance of the participation of the state and private business in the creation of this core infrastructure, including secure communication lines and data centers. And do not forget about digital literacy and the need to multiply the output of specialists in the digital economy.

Digital economy, digitalization, innovative systems.

Одной из важнейших предпосылок развития промышленности, как и социально-экономического развития РФ в целом, являются высокоэффективные национальные инновационные системы. К их числу относятся информационные инфраструктуры, направленные на создание,

накопление, обработку, хранение и организацию использования ресурсов и технологий [4, 7, 9].

При этом определенной научной проблемой является то обстоятельство, что информационное обеспечение (ИО) промышленности (целевая инфраструктура, функции, необходимые для реализации и управления соответствующими производственными процессами) представляют лишь вспомогательный механизм, который не преследует каких-либо собственных конечных нормативных целей.

Такая нормативная цель и возможность выбора рациональных альтернатив создания и проектирования информационных инфраструктур возникает лишь только тогда, когда информационное обеспечение рассматривается в связке с информационной потребностью какого-либо субъекта.

При этом информационная потребность проявляется, когда фиксируется тот факт, что необходимое локальное знание о предмете не соответствует тому уровню знания, которое потенциально накоплено в настоящее время в отрасли (обществе).

Преодоление данной проблемы приводит к формированию в каждой такой типовой ситуации нормативной цели, которая может быть, в частности, направлена на получение инновационных результатов и необходимых средств информационного обеспечения.

В этом проявляется, собственно, проектно-процессный подход к разработке и созданию любых изделий.

Таким образом, процесс информационного обеспечения промышленности, как проектный процесс, не должен рассматриваться в качестве самостоятельной или какой-либо приоритетной альтернативы, он обязательно должен быть неотъемлемой частью процессов с конечным результатом в соответствующей области промышленности, который отождествляется с «центром» оптимизируемых затрат.

Следует отметить, что необходимым условием достижения экономического и социального эффекта является активное использование в структуре «поставщик информационных услуг – потребитель услуг» также таких неотъемлемых частей производственного процесса, которые представляют собой партнер и инноватор. Перечисленные компоненты реализуются в сфере современных средств коммуникаций, информационных технологий и их сетевых приложений: электронная почта, дистанционное обучение, мультимедиа, телевидение, телеконференции, визуализация, моделирование, компьютерная графика и другое [7, 11].

При проведении исследования необходимо учитывать положения национальной технологической инициативы (НТИ) — государственной программы мер по поддержке развития в России перспективных отраслей, которые в течение следующих 20 лет могут стать основой мировой экономики (одобрена 14 февраля 2017 года на заседании президиума Совета

по модернизации экономики и национальному развитию России). Отмечается, что в исследуемой сфере наиболее перспективным направлением является цифровое проектирование и моделирование, поэтапное формирование для этого необходимой инфраструктуры и условий создания и развития отраслевых компетенций для обучения специалистов, внедрения современных технологий на предприятиях, формирование стратегии развития информационных технологий до 2030 года.

Более того, в своем выступлении на Петербургском международном экономическом форуме президент России Владимир Путин центральное место отвел технологическому развитию и лидерству. Президент при этом заметил: «…Так, благодаря отличным школам в области математики, теоретической физики мы способны добиваться лидерства по ряду направлений так называемой новой экономики, прежде всего цифровой. Российские IT-компании, безусловно, глобально конкурентны. Отечественные специалисты не просто предлагают наилучшие уникальные программные решения, а, по сути, создают новую сферу знаний, новую среду для развития экономики и жизни [11].

Чтобы наращивать наши кадровые, интеллектуальные, технологические преимущества в сфере цифровой экономики, мы намерены действовать по направлениям, имеющим системное значение (рисунок 1). Что имеется в виду?

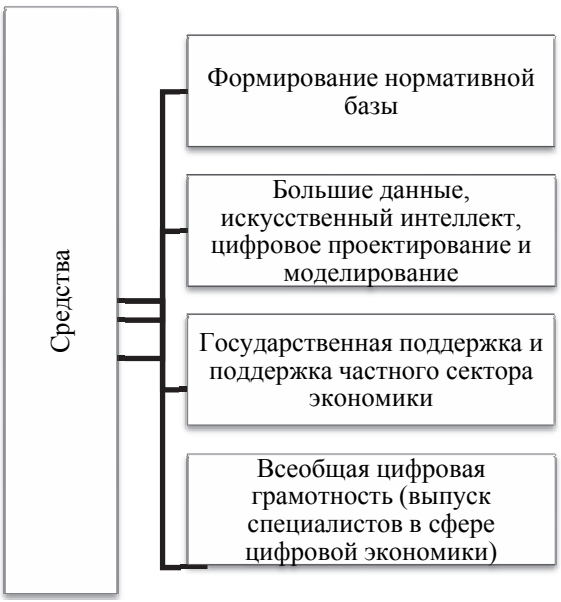


Рисунок 1 – Средства для создания опорной инфраструктуры цифровой экономики

Первое – необходимо сформировать принципиально новую, гибкую нормативную базу для внедрения цифровых технологий во все сферы жизни. При этом все решения должны приниматься с учётом обеспечения информационной безопасности государства, предприятий и граждан.

Второе – государство окажет поддержку тем компаниям, которые являются носителями разработок и компетенций в сфере цифровых технологий, имеющих так называемый сквозной межотраслевой эффект. Это: обработка и анализ больших массивов данных, искусственный интеллект и нейротехнологии, технологии виртуальной и дополненной реальности и ряд других.

Третье – с участием государства и частного бизнеса будем создавать опорную инфраструктуру цифровой экономики, в том числе безопасные линии связи и центры обработки данных. Кстати, обращаю внимание, это должна быть инфраструктура, основанная на самых передовых технологиях и разработках.

Четвёртое – намерены кратно увеличить выпуск специалистов в сфере цифровой экономики, а, по сути, нам предстоит решить более широкую задачу, задачу национального уровня – добиться всеобщей цифровой грамотности.

Для этого следует серьёзно усовершенствовать систему образования на всех уровнях - от школы до высших учебных заведений. И конечно, развернуть программы обучения для людей самых разных возрастов.

При этом возникает «пласт» прикладных научно-технических проблем, обладающих характерными особенностями для современного состояния отечественной промышленности.

Тривиальных методов решения этих проблем не существует. В ряде случаев могут использоваться проектно-процессные подходы, объектно-ориентированные подходы, системы менеджмента качества (стандарт ISO 9001), IDEF — методологии семейства ICAM (Integrated Computer – Aided Manufacturing), эффективно используемые в США, методы и средства интеллектуального управления, системы PLM (Product Lifecycle Management) и др. [1, 2, 3].

В целом же были использованы инструменты концептуального проектирования для:

- определения исходного состояния общей проблемы отраслевой ИТ и определения исходных данных и задач информационного обеспечения стадий создания и эксплуатации изделий;
- обоснования необходимости и мотивации инновационного развития информационного обеспечения;
- формирования требований к инновационному развитию информационного обеспечения с учетом прогнозирования динамики развития процессов;
- подготовки требований к ключевым элементам и инновационным технологиям информационного обеспечения (ИО) производственного процесса;
- разработки предложений по структуре требований к системе документирования и безопасности информации в работах с электронной

технической документацией на этапах жизненного цикла проектов создания и эксплуатации;

- определения направлений развития системы информационного обеспечения инновационного характера деятельности промышленности при создании продукции и эксплуатации изделий.

Применение проектно-программного подхода к управлению подготавливает основу успешной деятельности для предприятий России.

Основой технологического и инновационного развития станет усиление координации деятельности Правительства Российской Федерации, инновационных институтов развития, научных и образовательных организаций, промышленных предприятий в части формирования направлений приоритетных научных исследований и разработок, создания образцов конкурентоспособной инновационной продукции, коммерциализации разработок (где это целесообразно), технологического перевооружения предприятий, формирования спроса на инновационную продукцию, а также повышение эффективности механизма финансирования, направленного на стимулирование реализации наукоемких исследований, разработок и их внедрения в реальный сектор экономики и контроля за расходованием средств на научные исследования с привлечением общественности и частного капитала [8, 10, 11].

Литература

1. ISO 9001, Quality management systems – Requirements.
2. ISO/TS 9002, Quality management systems - Guidelines for the application of ISO 9001:2015.
3. ISO 9004, Managing for the sustained success of an organization - A quality management approach.
4. Безуглая Н.С., Абдулаев Ш.А. Национальные инновационные системы // Цифровизация: наука и образование в условиях современных вызовов, сборник материалов I международной межфилиальной научной конференции. Ташкент, 2021. Издательство: Российский экономический университет имени Г.В. Плеханова, Ташкентский филиал. С. 114-118.
5. Индекс глобальной конкурентоспособности: Информация об исследовании и его результаты. Гуманитарные технологии. Аналитический портал, 2019 [Электронный ресурс]. Режим доступа: https://gtmarket.ru/ratings/global-competitivenessindex/info (дата обращения: 20.04.2022).
6. Кропотина О.Е. Проектный и процессный подходы в управлении: достоинства и недостатки // Образование и право. 2019. №9. Режим доступа: https://cyberleninka.ru/article/n/proektnyy-i-protsessnyy-podhody-v-upravlenii-dostoinstva-i-nedostatki (дата обращения: 18.04.2022).
7. Крупнейшие компании России, реализующие инновационные проекты: ЭкспертРА, 2018 [Электронный ресурс]. Режим доступа:

http://www. raexpert.ru/researches/expert-inno/part5 (дата обращения: 20.04.2022).

8. Петровская А.В., Балашова И.В., Приходько К.С. Оптимизация региональной системы поддержки развития малого предпринимательства и обоснование разработанной методики оценки результативности региональной системы поддержки малого предпринимательства. Сфера услуг: инновации и качество. 2019. № 44. С. 99-116.

9. Петровский А.Б., Проничкин С.В., Стернин М.Ю., Шепелёв Г.И. Национальные инновационные системы: структуры, цели, функции, пути развития // Экономика. Информатика. 2018. №1. Режим доступа: https://cyberleninka.ru/article/n/natsionalnye-innovatsionnye-sistemy-struktury-tseli-funktsii-puti-razvitiya (дата обращения: 18.04.2022).

10. Российский статистический ежегодник / Росстат, 2019 [Электронный ресурс]. Режим доступа: http//www.gks.ru (дата обращения: 20.04.2022).

11. Цифровая Россия / РБК, 2019 [Электронный ресурс]. Режим доступа: http://digital-russia.rbc.ru/article-page_11.html (дата обращения: 20.04.2022).

ЛУЧШАЯ КИБЕРЗАЩИТА ОТ ВЫМОГАТЕЛЕЙ – МОДЕЛЬ НУЛЕВОГО ДОВЕРИЯ

Михайлин Иван Николаевич, магистрант 1 курса кафедры информационной безопасности
Научный руководитель: **Сухотерин Александр Иванович**, к.воен.н., доцент кафедры информационной безопасности

На фоне роста кибер атак на различные структуры, самым распространённым стали программы вымогатели, так как они довольно просты в использовании и приносят чуть ли 300% прибыль, однако даже такие вроде бы серьёзные последствия можно предотвратить если использовать модель нулевого доверия. Модель нулевого доверия может минимизировать влияние нарушения, обеспечить обнаружение угроз и улучшить защиту активов компании, а её главная цель затруднить распространение вредоносных программ внутри сети организации.

Информационная безопасность, программы вымогатели, модель безопасности, сетевая безопасность.

BEST RANSOMWARE CYBER PROTECTION - ZERO TRUST MODEL

Mikhailin Ivan, 1st year graduate student of the Department of Information security
Scientific adviser: **Sukhoterin Alexander**, Candidate of Military sciences, Associate professor of the Department of Information security

Against the background of the growth of cyber attacks on various structures, ransomware programs have become the most common, since they are quite easy to use and bring in almost 300% profits, but even such seemingly serious consequences can be prevented by using a zero trust model. A zero trust model can minimize the impact of a breach, detect threats, and improve the protection of a company's assets, and its main goal is to make it difficult for malware to spread within an organization's network.

Information security, ransomware, security model, network security.

Программы-вымогатели - это форма атаки, которая не позволяет пользователю получить доступ к компьютерным файлам, системам и сетям до тех пор, пока не будет выплачен выкуп. Это был самый распространенный вид кибератаки в 2021 году, составлявший 21% от общего числа, говорится в последнем индексе IBM X-Force Threat Intelligence Index.

Одна из причин, почему злоумышленникам нравится такой подход, заключается в том, что это эффективная бизнес-модель. Вам не нужно иметь собственный технический опыт для выполнения одной из этих атак. Теперь провайдеры «вымогателей как услуги» сделают это за вас.

Что такое вымогатель-как-услуга?

Криминальные «фирмы», обладающие техническим опытом, предоставляют партнерам готовые инструменты. Затем эти партнеры совершают нападение в обмен на процент от каждой выплаты выкупа. С одной банды, приходит прибыль в размере не менее 123 миллионов долларов в 2020 году, это действительно может быть очень прибыльным бизнесом.

Киберпреступники действуют как бизнес. Рост числа вымогателей-как-сервис демонстрирует тот факт, что наиболее успешные киберпреступники ведут свои атаки подобно бизнесу. Как и большинство предприятий, их целью является повышение доходности инвестиций (ROI) и максимизация прибыли. Фишинговые атаки являются предпочтительным подходом для злоумышленников-вымогателей и других киберпреступников, стремящихся войти в систему, на долю которых приходится 41% первоначальных атак, устраненных IBM X-Force в 2021 году. Проще и быстрее заставить кого-то дать вам свои учетные данные или нажать на вредоносную ссылку, чем взломать сложную сеть извне. Иными словами, окупаемость инвестиций больше. И как только преступник оказывается внутри системы, можно имплантировать программы-вымогатели и другие формы вредоносных программ. Аналогичным образом, желание максимизировать прибыль означает, что выбор целей киберпреступниками развивается. Пять-шесть лет назад преступники увидели шанс в реквизитах кредитных карт, которыми владели крупные ритейлеры (а многие до сих пор так и делают). Сегодня можно вызвать больше сбоев в бизнес-операциях и извлечь больше доходов за счет программ-вымогателей. В прошлом году цепочки поставок оказались под новым давлением. IBM обнаружила, что производство, которое играет важную роль в цепочках поставок, стало излюбленной мишенью киберпреступников. Она получила 23% атак (опередила финансы и страховку впервые с 2016 года). Ориентируясь на отрасли, которые не могут позволить себе простои, преступники увеличивают свои рычаги, чтобы заставить и быстро платить. Этот стиль атаки не только наносит ущерб одному предприятию, но и затрагивает целые бизнес-экосистемы. Иногда злоумышленники идут еще дальше и ставят свои прицелы на критически важную инфраструктуру.

Как DarkSide атаковал критическую инфраструктуру.

Стратегия, в которой преступники максимизируют свои рычаги воздействия, нацелившись на критически важную инфраструктуру, была показана в прошлом году, когда группа вымогателей DarkSide (которая работает по модели вымогателей как сервис) атаковала частный

колониальный трубопровод. Компания эксплуатирует нефтепроводы, протянувшиеся на 5500 миль от побережья Мексиканского залива до Нью-Йорка. Он поставляет 45% топлива, используемого на Восточном побережье США. Когда «Колониал» был вынужден закрыть трубопровод, у тысяч заправок закончилось топливо, что привело к паническим покупкам и скачку цен, когда водители в регионе примчались заполнять свои автомобили. Атака, ставшая результатом единого скомпрометированного пароля, обошлась «Колониалу» почти в 5 миллионов долларов в качестве выкупа. Но влияние ощущалось так далеко, как в Азии, потому что южнокорейская национальная пенсия является одним из совладельцев компании. Атака на «Колониал» также не была уникальной. Месяц спустя крупнейший в мире поставщик мяса подвергся вымогательству. Тем временем злоумышленники удерживали больницы для выкупа и целевые муниципальные системы в Атланте, Балтиморе и Массачусетсе, в каждом случае применяя давление на основные услуги, чтобы получить максимальную прибыль. Несмотря на широкое влияние атак вымогателей, большинство никогда не предается огласке. Это затрудняет обмен информацией, которая поможет компаниям бороться с этой угрозой. Многие из этих банд базируются в странах без четких правил выдачи или сотрудничества правительства в борьбе с нападениями. Так что сами преступники мало боятся быть привлеченными к ответственности, еще меньше - быть выданными. В настоящее время Ransomware является вредоносным ПО, наиболее благоприятствуемым киберпреступниками. Однако, как и любой бизнес, у них есть другие «продукты», которые они могут использовать для достижения своих целей. Например, распространение «умных» устройств, таких как холодильники и «умные» телевизоры, обеспечило злоумышленникам новые проемы. Фактически, IBM X-Force наблюдала увеличение использования вредоносных программ Интернета вещей на 3000% в период с третьего квартала 2019 года по четвертый квартал 2020 года. Так что же делать бизнесу? Важный первый шаг - практиковать мышление, как злоумышленник. Какие наиболее важные услуги могут привести к максимальным сбоям, если вы потеряете доступ к ним? Важно думать, как об услугах для клиентов, так и об услугах, которые поддерживают сотрудников и продукты. Кроме того, вы должны спросить: Какие системы могут служить шлюзом в корпоративной сети? Вам следует рассмотреть возможность применения модели безопасности с нулевым доверием, в которой вы устанавливаете наименее привилегированный доступ, постоянно проверяете и проверяете подлинность, а также принимаете решение о том, что нарушение, возможно, уже произошло. Модель нулевого доверия может минимизировать влияние нарушения, обеспечить обнаружение угроз и улучшить защиту активов компании. Цель состоит в том, чтобы затруднить распространение программ-вымогателей и других угроз даже после первоначального компромисса. Предприятия с нулевым доверием могут

повысить уровень безопасности при одновременном упрощении выполнения бизнес-требований. Несколько шагов к достижению нулевой доверительной среды включают в себя:

- Ограничение учетных записей администраторов домена и защита привилегированных учетных записей. Строго проверяйте, кто и когда получает доступ к учетным записям администраторов, и ищите подозрительные действия.
- Использование Active Directory для защиты критически важных паролей. Ограничение путей через сеть с помощью сегментации, где это возможно.
- Расширение стратегии нулевого доверия и использование архитектуры SASE для управления технологиями и инфраструктурными подходами из одного местоположения. Имея платформу управления, вы можете оптимизировать работу администратора, обмениваться данными и использовать аналитику для получения общей картины безопасности. SASE создает структуру, которая делает нулевое доверие гибким и простым в управлении. Защита данных и приложений благодаря сочетанию обоих принципов.

Никто не любит останавливаться на том, что может пойти не так. Но использование этих и других шагов может в значительной степени защитить вас от атаки вымогателей или утечки данных от рук злоумышленников.

Что такое модель нулевого доверия?

Модель нулевого доверия представляет собой целостный подход к сетевой безопасности, который требует проверки каждого человека и устройства при каждой попытке доступа к ресурсам в частной сети. Это остается верным, независимо от того, находится ли это устройство или человек уже внутри или за пределами периметра сети.

Модель нулевого доверия включает в себя набор принципов и рекомендует использовать соответствующие технологии и методы.

Каковы основные принципы модели нулевого доверия?

Вот основные принципы, определяющие внедрение нулевого доверия в организациях.

Строгая оценка контроля доступа.

Модель нулевого доверия предполагает, что потенциальные злоумышленники могут существовать внутри и вне сети и, следовательно, не доверяют им. Все пользователи или устройства, пытающиеся получить доступ к сетевым ресурсам, должны пройти проверку подлинности, а каждый запрос на доступ должен быть авторизован и зашифрован.

Разнообразие методов профилактики.

Для предотвращения нарушений и сведения к минимуму их ущерба существует целый ряд профилактических методов.

Многофакторная аутентификация является наиболее распространенным методом подтверждения личности пользователя. Он

требует, чтобы пользователь предоставил по крайней мере две формы доказательств для подтверждения достоверности. Они могут включать в себя вопросы безопасности, SMS или подтверждение по электронной почте и/или упражнения на основе логики. Чем больше средств требуется для доступа, тем лучше защищена сеть.

Ограничение доступа для пользователей, прошедших проверку подлинности, является еще одним уровнем, используемым для получения доверия. Каждый пользователь или устройство получает доступ только к минимальному количеству требуемых ресурсов, тем самым минимизируя потенциальную атакующую поверхность сети в любой момент времени. Все остальное остается заблокированным, тем самым отказывая в боковом движении доверенным объектам.

Микросегментация - это метод сетевой безопасности, который включает разделение сетей на зоны, каждая из которых требует отдельного доступа к сети. Ущерб, который может нанести хакер, даже если безопасность нарушена, остается ограниченным микросегментом, в который ему удалось проникнуть.

Мониторинг в режиме реального времени для выявления вредоносных действий.

Модель нулевого доверия в основном является превентивной. В дополнение к превентивным мерам, мониторинг в реальном времени важен, поскольку он может минимизировать время между первоначальным нарушением и моментом распространения угрозы на дополнительные системы в сети. Быстрый мониторинг обеспечивает обнаружение, расследование и исправление, закрывая окно возможностей для злоумышленников.

Пример реализации нулевого доверия: модель нулевого доверия Microsoft.

Корпорация Майкрософт поделилась подробностями о собственной реализации модели нулевого доверия. Реализация Microsoft с нулевым доверием сосредоточена на:

Корпоративные услуги, используемые в организации, включая приложения Office и бизнес-приложения;

Устройства под управлением Windows, Mac, iPhone и Android;

Управление устройствами осуществляется службой управления мобильными устройствами (MDM) Microsoft Intune.

Модель нулевого доверия Microsoft состоит из четырех этапов:

- Проверка подлинности - Microsoft требует двухфакторной проверки подлинности (2FA) для удаленного доступа к своим сетям. Метод аутентификации эволюционировал от физической смарт-карты к вызовам на основе телефона с помощью приложения Azure Authenticator. В будущем Microsoft стремится исключить пароли и перейти к полной биометрической аутентификации.

- Проверка работоспособности устройств - корпорация Майкрософт регистрирует устройства пользователей с помощью службы Intune MDM. Существует политика работоспособности устройств, которая определяет, что устройства должны управляться и быть работоспособными (исправлены и протестированы, чтобы быть свободными от вредоносных программ и уязвимостей), чтобы получить доступ к крупным производительным приложениям компании - Exchange, SharePoint и командам. Корпорация Майкрософт будет поддерживать неуправляемые устройства для особых случаев использования, предоставляя виртуализированные настольные компьютеры и приложения Windows.
- Проверка доступа - корпорация Майкрософт минимизировала доступ к корпоративным ресурсам и требует проверки подлинности и работоспособности устройств. Доступ к основным службам и приложениям будет переходить от прямого доступа к корпоративной сети, к Интернету плюс VPN, к Интернету-только - сокращая число пользователей, которым необходим доступ к корпоративной сети.
- Проверка служб - наконец, корпорация Майкрософт планирует добавить проверку работоспособности службы, гарантируя ее работоспособность перед началом взаимодействия с пользователями. В настоящее время это является доказательством концепции.

Каковы проблемы стратегии нулевого доверия?

Вот несколько проблем, с которыми вы, вероятно, столкнетесь при внедрении модели нулевого доверия в вашей организации и как их преодолеть.

- Текучесть пользователей и ролей.

Последние события изменили наш образ обучения, жизни и работы. В большей степени, чем когда-либо ранее, рабочее место как физическое место, в котором проживает большинство сотрудников компании, находится под угрозой. Все больше людей получают удаленный доступ к данным, используя домашние IP-адреса, маршрутизаторы, общедоступные службы WiFi и VPN.

Клиенты также получают доступ к информационным ресурсам организации. Интернет-покупатель должен получить доступ к инвентаризации, услугам доставки, демонстрациям и веб-сайту компании. Поставщики должны иметь доступ к операциям, безопасности и платежам.

База пользователей, которые должны получать доступ к ресурсам компании, является широкой и разнообразной, а число точек доступа постоянно растет. Для каждой группы лиц требуется определенный набор политик, для определения и ведения которых может потребоваться много времени. Учитывая высокие темпы текучести кадров и клиентов, группы безопасности могут быстро перегружаться.

- Распространение устройств.

За человеческим фактором лежит аппаратура. Существует огромное разнообразие мобильных устройств и персональных компьютеров, с помощью которых сотрудники, клиенты и поставщики взаимодействуют с системами компании. Привнесите собственные политики устройства (BYOD), оборудование Интернета вещей и «всегда включенные» политики, что приводит к увеличению количества свойств, требований и протоколов связи, которые должны отслеживаться и защищаться на постоянной основе.

- Распределенные данные и услуги.

Облачные среды являются глобально распределенными и доступными из любого места, что является как повышением, так и понижением. Компании хранят более конфиденциальные ресурсы, данные и приложения в облаке, а старая модель безопасности, в которой контролируемые компанией конечные точки и корпоративные сети могут быть надежно защищены, больше не используется.

С постепенным переходом на граничные вычисления ИТ-специалистам также придется перейти от нисходящих централизованных инфраструктур безопасности к децентрализованным моделям доверия. Пограничные системы представляют собой серьезный риск для модели нулевого доверия и должны рассматриваться как отдельные сети с собственными средствами контроля и политиками нулевого доверия.

Таким образом, Модель безопасности Zero Trust (нулевого доверия) решает многие проблемы традиционной модели сетевой безопасности, которая основывалась на концепции периметра безопасности. Доступ к сети жестко контролировался, но оказавшись внутри, соединения по умолчанию доверялись и злоумышленник мог нанести значительный ущерб. В современной распределенной среде, где данные и приложения работают на удаленных облачных сервисах, сотрудники работают дома или с личных устройств, а также все более широкое использование мобильных устройств и Интернета вещей, подход к периметру безопасности больше не действует и заменяется моделью нулевого доверия. Данная модель является как идеальным решением для бизнеса, включая в себя комплексную защиту информации и защиту финансовых активов, так и для гос. учреждение, так как обеспечивает защиту информации как внутри и вне сети.

Литература

1. Монаппа К.А. Анализ вредоносных программ // ДМК Пресс. 2019. С. 10–35.

2. Аткина В.С. Оценка Эффективности катастрофоустойчивых решений // Вестник Волгоградского Государственного Университета Инновационная Деятельность,2012. №7 С. 49

3. Классификация вредоносных программ // Лаборатория Касперского. [Электронный ресурс] Режим доступа: https://www.kaspersky.ru/blog/klassifikaciya-vredonosnyx-programm/2200/ (дата обращения: 12.04.2022)

ОЧИСТКА ГАЗОВ ОТ АЭРОЗОЛЬНЫХ ЧАСТИЦ В РАЗНОТЕМПЕРАТУРНЫХ КАНАЛАХ-КОНДЕНСАТОРАХ

Пейогло Кира Руслановна, магистрант 2 курса кафедры математики и естественнонаучных дисциплин
Научный руководитель: **Чаусова Ольга Владимировна**, к.ф.-м.н., доцент кафедры математики и естественнонаучных дисциплин

Настоящая работа посвящена исследованию процессов очистки газов в плоско-параллельном разнотемпературном канале-конденсаторе. Для вычисления оптимальной геометрии канала необходимо рассчитать скорость осаждения частиц примесей на одной из пластин. В работе решена задача о термофорезе крупной нелетучей аэрозольной частицы сферической формы. На основании полученных результатов выведена формула для расчета длины канала. Прослеживается зависимость характерного размера очистного сооружения от создаваемой разности температур, ширины зазора между пластинами, скорости подачи газа, а также физико-химических характеристик примесей.

Очистка газов, разнотемпературные каналы-конденсаторы, аэрозольные частицы.

PURIFICATION OF GASES FROM AEROSOL PARTICLES IN DIFFERENT-TEMPERATURE CONDENSER CHANNELS

Peyoglo Kira, 2nd year graduate student of the Department of Mathematics and natural sciences
Scientific adviser: **Chausova Olga**, Candidate of Physical and mathematical sciences, Associate professor of the Department of Mathematics and natural sciences

This work is devoted to the study of gas purification processes in a plane-parallel multi-temperature channel-condenser. To calculate the optimal channel geometry, it is necessary to calculate the rate of deposition of impurity particles on one of the plates. The problem of thermophoresis of a large non-volatile aerosol particle of a spherical shape is solved in this work. Based on the obtained results, a formula for calculating the channel length is derived. The dependence of the characteristic size of the treatment plant on the created temperature difference, the width of the gap between the plates, the gas supply rate, as well as the physicochemical characteristics of impurities is traced.

Gas purification, multi-temperature condenser channels, aerosol particles.

Экологические проблемы современного мира носят глобальный характер. В первую очередь, они связаны с деятельностью человека – работой различных предприятий и выбросами загрязненных веществ в окружающую среду. Антропогенное воздействие настолько велико, что естественные механизмы самоочищения являются недостаточными. В связи с этим актуальным представляется рассмотрение различных технологий очистки продуктов переработки производства.

Для очистки газов на предприятиях, как правило используются два типа каналов – каналы, в которых поддерживается постоянная температура, где происходят процесса тепломассообмена и разнотемпературные каналы-конденаторы. Проходящий через каналы первого типа газ нагревают и насыщают парами летучего вещества. Такие каналы не дают полной очистки газов. Для качественной отработки необходимо пропускать газы через систему каналов. Разнотемпературные же каналы имеют более высокую степень очистки.

Геометрия используемых для очистки каналов различна – встречаются плоско-параллельные и коаксиальные каналы-конденсаторы. В настоящей работе рассматривается первый тип канала. Для расчета эффективной длины канала необходимо знать распределение скоростей частиц внутри него.

Рассмотрим движение крупной аэрозольной капли. При движении такой частицы можно пренебречь влиянием слоя Кнудсена, не рассматривать скачки температуры вблизи поверхности капли.

Будем решать задачу в условиях установившегося движения, когда равнодействующая действующих на частицу термофоретических, термокаппилярных сил и сил вязкого сопротивления равна нулю [2]:

$$\vec{F} = \vec{F}_{TF} + \vec{F}_{\sigma} + \vec{F}_{v} = 0. \qquad (1)$$

Задача обладает центральной симметрией, поэтому решение проводим в сферической системе координат (r, θ, φ). Начало отсчета жестко связано с геометрическим центром капли, а ось аппликат z направлена в сторону градиента температуры $\vec{A}_T$. В такой постановке капля покоится и на нее набегает окружающая среда со скоростью $\vec{U} = -\overrightarrow{U_T}$, где $\overrightarrow{U_T}$ – скорость термофореза.

Динамика капли описывается осесимметричными дифференциальными уравнениями Стокса, непрерывности и Лапласа [3]:

$$\begin{array}{cc} \eta\Delta\vec{v}^{e} = \nabla p^{e} & \eta\Delta\vec{v}^{i} = \nabla p^{i} \\ div\ \vec{v}^{e} = 0 & div\ \vec{v}^{i} = 0 \\ \Delta T^{e} = 0 & \Delta T^{i} = 0 \end{array} \qquad (2)$$

Индексы «e» и «i» относятся к характеристикам среды вне и внутри капли соответственно.

Условия на бесконечности [1].

условие однородности осесимметричного потока внешней среды

$$v_r^e = \left|\vec{U}\right| cos\,\theta\,, v_\theta^i = -\left|\vec{U}\right| \sin\theta\,, p^e = p_0^e, \quad (3)$$

здесь $\vec{U}$ – скорость потока внешней среды на большом удалении от бактерии, p_0^e – невозмущенное значение давления при температуре T_0^e

1) На бесконечности температура есть функция координаты $z = r\cos\theta$

$$T^e = T_0^e + A_T r\cos\theta\,, \quad (4)$$

здесь T_0^e – невозмущенное значение температуры на бесконечности, $A_T = (\nabla T)_\infty$ - постоянный градиент температуры

Условия на поверхности частицы [1].

Разность касательных составляющих скорости вне и внутри капли равна тепловому скольжению

$$v_\theta^e - v_\theta^i = \frac{K_{TSl}}{T_0^e R}\frac{\partial T^e}{\partial\theta}, \quad (5)$$

здесь K_{TSl} – коэффициент теплового скольжения, R – радиус аэрозольной частицы.

условие непрерывности радиальной составляющей тензора тензора вязких напряжений

$$-p^e + 2\eta_0^e\frac{\partial v_r^e}{\partial r} - \frac{2}{R}\frac{\partial\sigma}{\partial T^i}\Big|_{T^i-T_0^i}\left(T^i - T_0^i\right) - \frac{2\sigma}{R}\Big|_{T^i-T_0^i} =$$

$$= -p^i + 2\eta_0^i\,\frac{\partial v_r^i}{\partial r}. \quad (6)$$

В этом выражении слагаемые $\frac{2}{R}\frac{\partial\sigma}{\partial T^i}\Big|_{T_i-T_0^i} - \frac{2\sigma}{R}\Big|_{T^i-T_0^i}$ описывают поверхностное натяжение на границе раздела капля – внешняя смесь. Вообще говоря, поверхностное натяжение σ можно разложить в ряд по малому параметру

$$\sigma = \sigma_0 + \frac{\partial\sigma}{\partial T^i}\Big|_{T^i-T_0^i}\left(T^i - T_0^i\right) + \cdots \quad (7)$$

η_0^e, η_0^i – коэффициенты динамической вязкости внешней среды и аэрозольной частицы

Условие непрерывности касательной составляющей тензора вязких напряжений

$$\eta_0^e\left(\frac{1}{r}\frac{\partial v_r^e}{\partial\theta} + \frac{\partial v_\theta^e}{\partial r} - \frac{v_\theta^e}{r}\right) + \frac{1}{R}\frac{\partial\sigma}{\partial T^i}\Big|_{T_i-T_0^i}\frac{\partial T^i}{\partial\theta} =$$

$$= \eta_0^i\left(\frac{1}{r}\frac{\partial v_r^i}{\partial\theta} + \frac{\partial v_\theta^i}{\partial r} - \frac{v_\theta^i}{r}\right) \quad (8)$$

В этом граничном условии выражение $\frac{\partial\sigma}{\partial T^i}\Big|_{T_i-T_0^i}\frac{\partial T^i}{\partial\theta}$ представляет собой производную $\frac{\partial\sigma}{\partial\theta}$, представленную в первом приближении по малому параметру.

Непроницаемость поверхности капли для внешней среды

$$v_r^e = 0 \tag{9}$$

Непроницаемость цитоплазмы капли во внешнюю среду

$$v_r^i = 0 \tag{10}$$

Непрерывность потока тепла

$$\kappa_0^e \frac{\partial T^e}{\partial r} = \kappa_0^i \frac{\partial T^i}{\partial r} \tag{11}$$

κ_0^e, κ_o^i – коэффициенты теплопроводности капли и внешней среды.

Непрерывность температуры:

$$T^e = T^i. \tag{12}$$

Индекс «0» у величин означает, что коэффициенты переноса принимаются как постоянные величины при температуре $T = T_0^e$.

Решение дифференциальных уравнений термофореза

Решения уравнений (1) представляются в виде разложений [4] по полиномам Лежандра n-го порядка $P_n(\theta)$:

$$v_r^e = \left|\vec{U}\right| \cos\theta + \frac{\gamma}{r} + \sum_{n=1}^{\infty} \left[-\frac{n+1}{r^{n+2}} A_{-n-1} + \frac{n+1}{2(2n-1)} \frac{B_{-n-1}}{r^n} \right] P_n(\theta),$$

$$v_\theta^e = -\left|\vec{U}\right| \sin\theta + \sum_{n=1}^{\infty} \left[-\frac{A_{-n-1}}{r^{n+2}} - \frac{n-2}{2(2n-1)} \frac{B_{-n-1}}{r^n} \right] \frac{dP_n(\theta)}{d\theta},$$

$$p^e = \eta_0^e \sum_{n=1}^{\infty} \frac{B_{-n-1}}{r^{n+1}} P_n(\theta) + p_0^e,$$

$$v_r^i = v_{r0}^i + \sum_{n=0}^{\infty} \left[n A_n r^{n-1} + \frac{n}{2(2n+3)} B_n r^{n+1} \right] P_n(\theta),$$

$$v_\theta^i = \sum_{n=0}^{\infty} \left[A_n r^{n-1} + \frac{(n+3)B_n}{2(n+1)(2n+3)} r^{n+1} \right] \frac{dP_n(\theta)}{d\theta},$$

$$p^i = \eta_0^i \sum_{n=0}^{\infty} B_n r^n P_n(\theta) + p_0^i,$$

$$T^e = T_0^e + \sum_{n=1}^{\infty} \frac{T_n^e}{r^{n+1}} P_n(\theta) + A_T \cos\theta + \frac{\varphi_1}{r},$$

$$T^i = T_0^i + \sum_{n=1}^{\infty} T_n^i r^{(n)} P_n(\theta)$$

В этих решениях $A_{-n-1}, B_{-n-1}, A_n, B_n, \varphi_1, T_n^e, T_n^i$ – неизвестные постоянные.

Полиномы Лежандра выражаются формулами и реккурентным соотношением:

$$P_0(x) = 1; \tag{13}$$

$$P_1(x) = x; \tag{14}$$

$$P_{n+1}(x) = \frac{2n+1}{n+1}\, x\, P_n(x) - \frac{n}{n+1} P_{n-1}(x) \text{ (при } n \geq 1) \tag{15}$$

Используя условие ортогональности полиномов Лежандра:

$$\frac{2n+1}{2} \int_0^{\pi} P_n P_m \sin\theta \, d\theta = \delta_{mn}, \tag{16}$$

где δ_{mn} – символ Кронекера, равный

$$\delta_{mn} = \begin{cases} 0, \text{при } m \neq n \\ 1, \text{при } m = n' \end{cases} \tag{17}$$

условия на бесконечности и условия конечности термодинамических характеристик в центре капли запишем полученные решения в виде:

$$v_r^e = \left(\frac{A}{r^3} + \frac{B}{r} + \left|\vec{U}\right|\right)\cos\theta + \frac{\gamma}{r}; \tag{18}$$

$$v_\theta^e = \left(\frac{A}{2r^3} - \frac{B}{2r} - \left|\vec{U}\right|\right)\sin\theta\,; \tag{19}$$

$$p^e = p_0^e + \eta_0^e \frac{B}{r^2}\cos\theta\,; \tag{20}$$

$$v_r^i = (Q + Dr^2)\cos\theta\,; \tag{21}$$

$$v_\theta^i = -(Q + 2Dr^2)\sin\theta \tag{22}$$

$$p^i = p_0^i + 10\,\eta_0^i Dr\cos\theta \tag{23}$$

$$T^e = T_0^e + A_T r\cos\theta + \frac{\mu_1}{r^2}\cos\theta + \frac{\varphi_1}{r} \tag{24}$$

$$T_i = T_0^i + \mu_2 r\cos\theta\,. \tag{25}$$

Здесь введены обозначения:

$$-2A_{-2} = A; B_{-2} = B, A_1 = Q, B_1 = 10D, T_1^e = \mu_1, T_1^i = \mu_2. \tag{26}$$

Остальные коэффициенты в рядах по полиномам Лежандра, через которые выражаются решения равны нулю.

Подставляя найденные решения (18)-(25) в граничные условия (5)-(12) определим неизвестные константы $\gamma, \varphi_1, \varphi_2, A, B, \left|\vec{U}\right|, Q, D, \mu_1, \mu_2$ и запишем выражения для скорости термофореза капли:

$$\vec{U} = -\frac{2k_0^e}{2k_0^e + k_0^i} \cdot \frac{\left(\frac{3k_{TSL}\eta_0^i}{T_0^e} + R\frac{\partial\sigma}{\partial T^i}\right)}{3\eta_0^i + 2\eta_0^e}\vec{A}_T$$

Знак «-» перед дробью указывает на то, что скорость термофоретического переноса направлена в сторону убывания температуры, в то время как градиент указывает в сторону наибольшего возрастания функции температуры.

Захват аэрозольных частиц в разнотемпературных плоско-параллельных каналах.

В практических инженерных приложениях может оказаться целесообразным использование разнотемпературных плоских каналов для доочистки газовых потоков (рис.1).

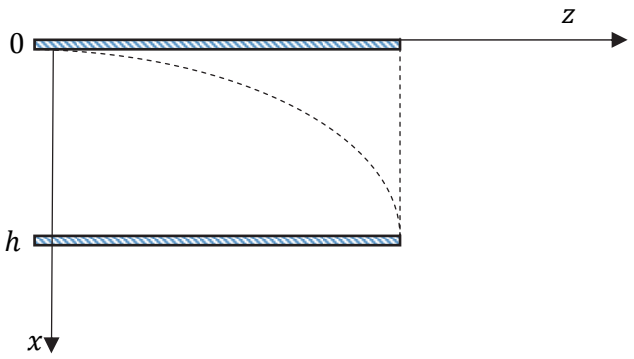


Рисунок 1 – Движение частицы в плоском разнотемпературном канале-конденсаторе

Рассматривается процесс улавливания аэрозольных частиц из ламинарного неоднородного по температуре и концентрации потока бинарной газовой смеси, проходящего в разнотемпературном плоском канале. Аэрозольные частицы, попадая в зазор между плоскими пластинами канала, начинают двигаться к поверхности нижней пластины.

Найдем время осаждения частицы, вошедшую в канал вблизи верхней (горячей) пластины:

$$t = \int_0^h \frac{dx}{U} = \frac{2k_0^e + k_0^i}{2k_0^e} \cdot \frac{3\eta_0^i + 2\eta_0^e}{\frac{3k_{TSL}\eta_0^i}{T_0^e} + R\frac{\partial\sigma}{\partial T^i}} \cdot \frac{h}{A_T}.$$

Зная скорость движения центра масс системы и максимальное время, необходимое для осаждения капли можно рассчитать необходимую длину пластины:

$$l = v_{\text{ц.м.}} \cdot t = \frac{2k_0^e + k_0^i}{2k_0^e} \cdot \frac{3\eta_0^i + 2\eta_0^e}{\frac{3k_{TSL}\eta_0^i}{T_0^e} + R\frac{\partial\sigma}{\partial T^i}} \cdot \frac{h}{A_T} \cdot v_{\text{ц.м.}}$$

Полеченная формула отражает зависимость длины канала от величины разности температур на его пластинах, зазора между пластинами и скорости подачи газа, а также от физико-химических характеристик газа и возможных примесей.

Литература

1. Чаусов Д.Н., Чаусова О.В. Вымывание летучих аэрозольных частиц испаряющимися каплями при числах Рейнольдса и Пекле, много

меньше единицы // НЕЛИНЕЙНЫЕ ВОЛНЫ – 2020. Тезисы докладов XIX научной школы. 2020 Изд.: Институт прикладной физики Российской академии наук (Нижний Новгород)

2. Яламов Ю.И, Ставцева О.В., Баринова М.Ф., Костицына Л.И. «Теория термо-диффузиофоретического переноса умеренно крупных летучих аэрозольных частиц при прямом учете влияния коэффициента испарения» Учебное пособие.- М.: Издательство МГОУ, 2008г, 65с.

3. Яламов Ю.И. Теория движения аэрозольных частиц в неоднородных газах.— Докторская диссертация.- М., 1968.

4. Brock I . R. Forces on Aerosols in Gas Mixtures // J. Colloid Sci. 1963. Vol. 18,-6. P.P. 489-501.

РАЗРАБОТКА ПРИКЛАДНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ 2D И 3D ГРАФИКИ

Перепелица Кирилл Алексеевич, магистрант 2 курса кафедры информационных технологий и управляющих систем
Научный руководитель: **Светушков Николай Николаевич**, к.т.н., доцент кафедры математики и естественнонаучных дисциплин

В статье приводится обзор построения нового алгоритма нахождения кратчайшего пути при использовании приложения AnyLogic. В статье приведен листинг некоторых функций программы, показан принцип работы алгоритма.

AnyLogic, оптимизация логистики, коммивояжер.

DEVELOPMENT OF APPLIED INFORMATION SYSTEMS USING 2D AND 3D GRAPHICS

Perepelitsa Kirill, 2nd year graduate student of the Department of Information technology and system management
Scientific adviser: **Svetushkov Nikolai**, Candidate of Technical sciences, Associate professor of the Department of Mathematics and natural sciences

The article provides an overview of the construction of a new algorithm for finding the shortest path using the AnyLogic application. The article provides a listing of some of the program's functions, shows the principle of the algorithm.

AnyLogic, logistics optimization, traveling salesman.

ВЕДЕНИЕ

Актуальность проекта обусловлена необходимостью оптимизации процесса доставки товара.

Научная новизна проекта заключается в:

— разработке нового эвристического алгоритма (перебора ограниченного набора вариантов для поиска оптимального пути;

— использовании средств программной среды имитационного моделирования AnyLogic для проведения облачных расчетов и представления результатов с привязкой к реальной карте местности.

Объектом научно-исследовательской работы является классическая задача оптимизации на графах, известная как задача коммивояжера, в условиях, когда необходимо не только найти минимальную длину пути (или минимальное время) для прохождения всех пунктов назначения, но и

уложиться в заданные для каждого пункта временные интервалы — время доступности клиентов-адресатов.

Цель исследования заключается в разработке эффективного алгоритма перебора ограниченного набора вариантов и нахождении оптимального с точки зрения заданного критерия (как известно, полный перебор всех вариантов даже на современных суперкомпьютерах при N>100 невозможен).

Задачи исследования:

— разработать интуитивно понятный интерфейс программного обеспечения для решения ЗМО в режиме реального времени;

— собрать статистические данные о работе программного комплекса и его возможностях для оперативной корректировки маршрута движения курьеров.

Практическая значимость проекта обусловлена актуальностью решения ЗМО для широкого круга задач, связанных с различного рода логистическими проблемами и возможностью применять для их решения предлагаемые подходы.

Описание работы алгоритма.

В программную среду AnyLogic вводятся данные о клиентах. Каждому клиенту присваивается свой индивидуальный номер, указывается его координаты местонахождения в пространстве. Перед запуском алгоритма пользователь указывает количество групп по оси координат X и по оси координат У. После алгоритм сортирует всех клиентов по группам. Принцип алгоритма показан на рисунке 1.

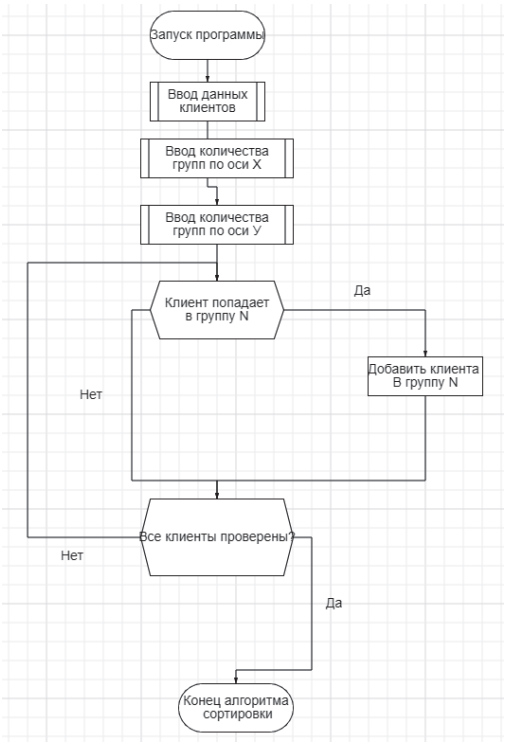


Рисунок 1 – Алгоритм сортировки клиентов

После выполнения сортировки программа отображает пользователю каким образом были поделены клиенты по группам (рис. 2).

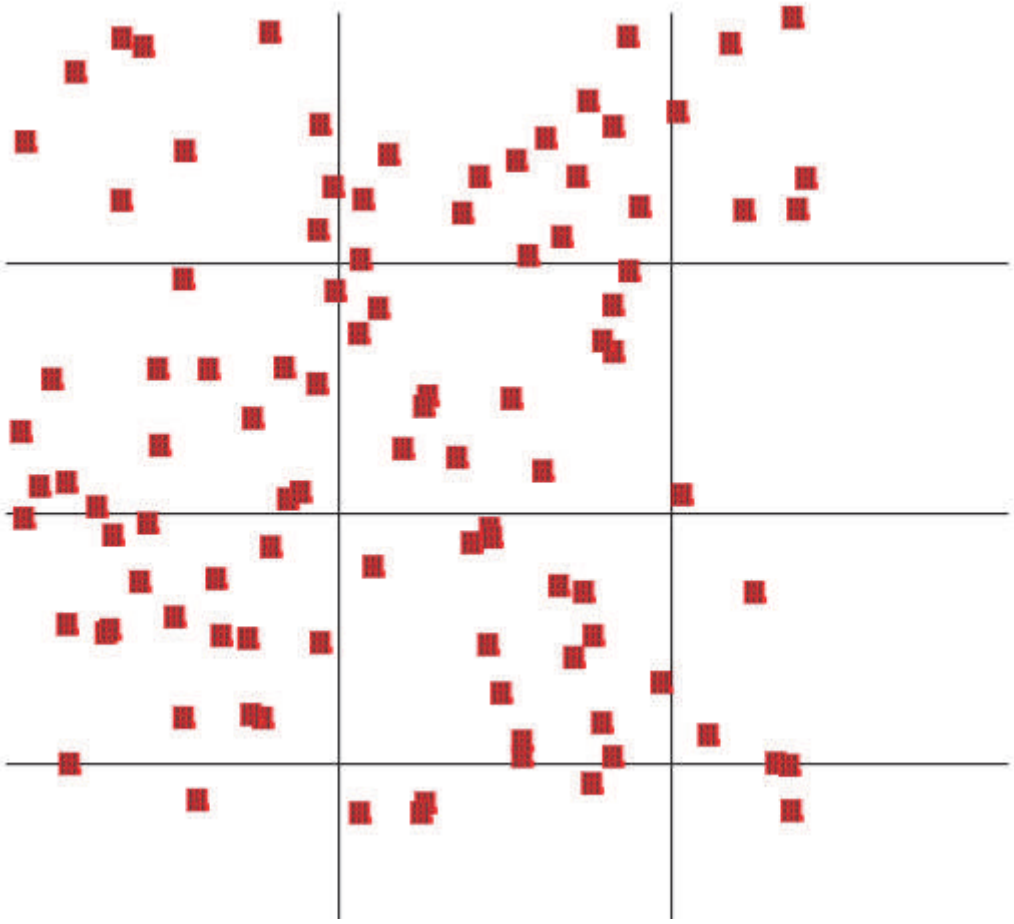


Рисунок 2 – Отображение деления клиентов по группам

Для большей наглядности группы выделяются в окружности, как показано на рисунке 3.

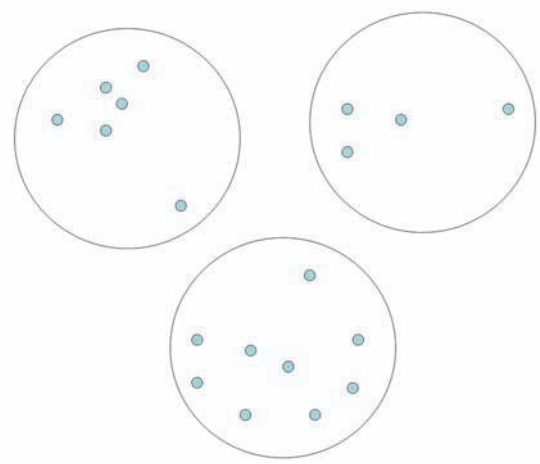


Рисунок 3 – Пример распределения общего количества клиентов по группам

Для каждой группы считается оптимальный маршрут. Оптимальным маршрутом считается минимальный путь, позволяющий обойти каждого клиента в группе. Конечный итог программы – постройка оптимального маршрута между всеми группами клиентов и отображение этого маршрута пользователю, как показано на рисунке 4.

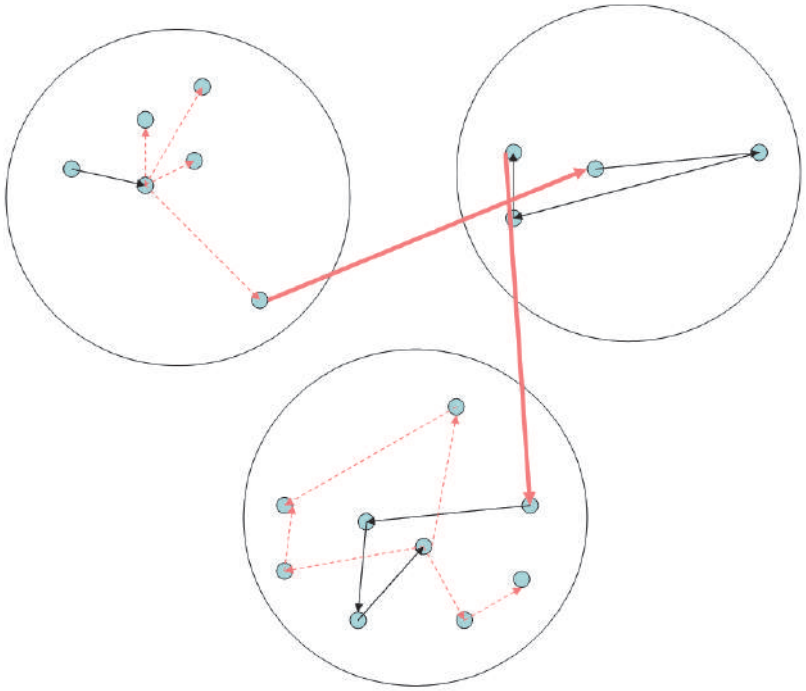


Рисунок 4 – Отображение наиболее оптимального маршрута пользователю

Подход к делению клиентов на группы наиболее оптимален при использовании метода, основанного на принципе просчета ходов в шахматах с заданной глубиной поиска. Именно для максимально эффективного использования данного метода и применяется деление клиентов на группы. Полная блок-схема алгоритма выглядит так (рис. 5).

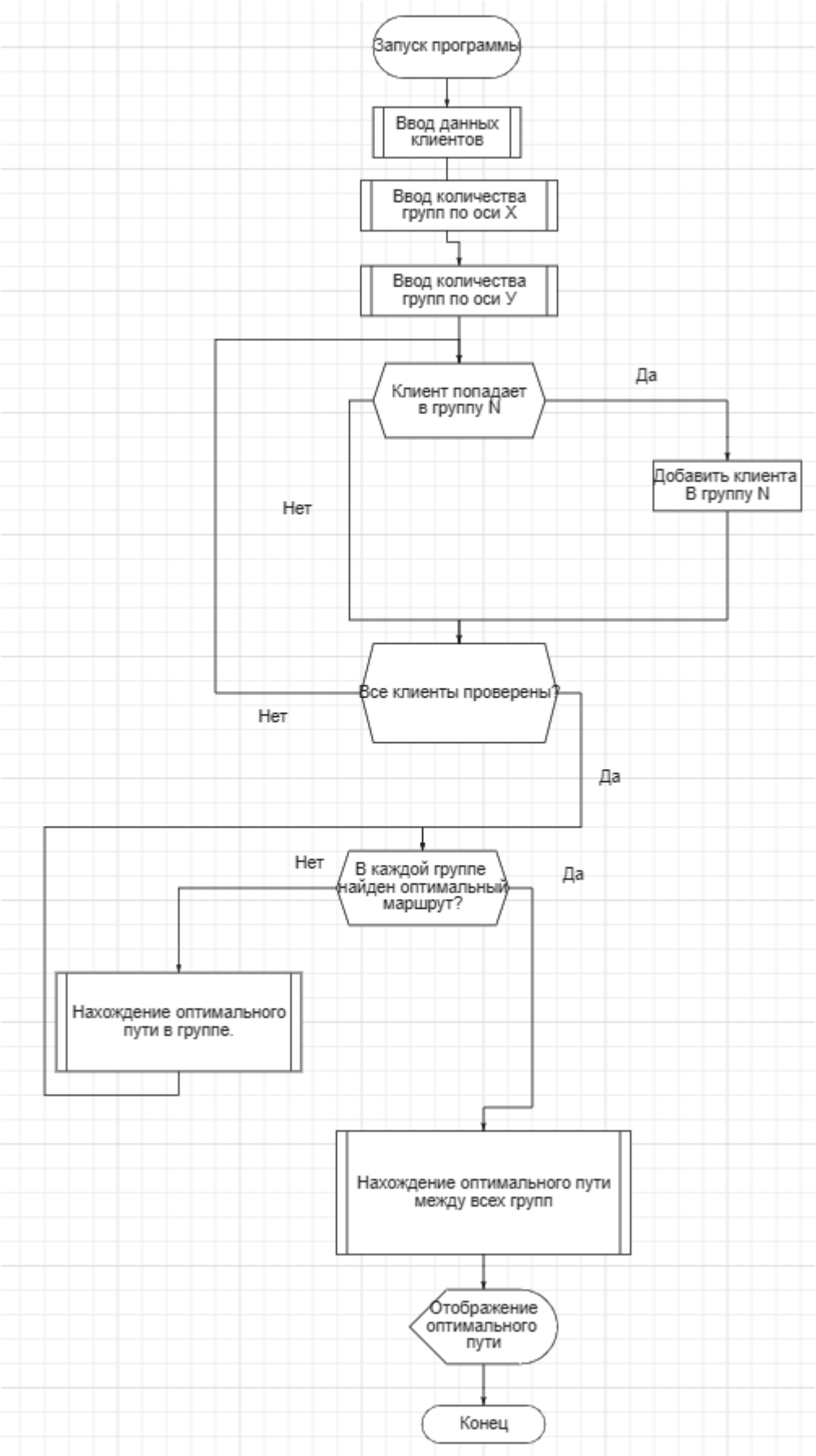


Рисунок 5 — Блок-схема программы

Листинг функции приведены в листинге 1 и 2.

Листинг 1. Функция Otbor.

```
int tempa=0;

	for (int o = 0; o < GroopX; o++) {
	for (int p = 0; p < GroopY; p++) {
	int temp=0;

	for (int j = 0; j < 100; j++)
	{
	if ((myTowns(j).getX() >= (500/GroopX * o) && (myTowns(j).getX() <
(500/GroopX * (o + 1))))
	                                && (myTowns(j).getY() >= (500/GroopY *
p) && myTowns(j).getY() < (500/GroopY * (p + 1))))
	{

	mas[tempa][temp]=j;

	temp++;
	}
	if (j == 99)
	{
	elem[tempa] = temp;
	}
	}
	tempa++;
	}}
```

Листинг 2. Функция Crednya.

```
	for (int z = 0; z < Group; z++) {
	double temp = 0;
	double temp_x = 0;
	double temp_y = 0;
	for (int j = 0; j < elem[z]; j++)
	{
	temp++;
	temp_x = myTowns(mas[z][j]).getX() + temp_x;
	temp_y = myTowns(mas[z][j]).getY() + temp_y;
	if (j == elem[z]-1)
	{
```

```
temp_x = temp_x / temp;
temp_y = temp_y / temp;
crednya_tocka[0][z] = temp_x;
crednya_tocka[1][z] = temp_y;
}
}
double max = 0;
for (int i = 0; i < elem[z]+1; i++)
{
if (sqrt((pow(myTowns(mas[z][i]).getX() - crednya_tocka[0][z],2))  +
pow(myTowns(mas[z][i]).getY() - crednya_tocka[1][z],2))> max)
{
max = sqrt((pow(myTowns(mas[z][i]).getX() - crednya_tocka[0][z],2))  +
pow(myTowns(mas[z][i]).getY() - crednya_tocka[1][z],2));
}
}
radios[z] = max/2;
}
```

Заключение

Программная реализация подобного алгоритмического подхода позволит создать удобное для пользователя программное обеспечение в среде AnyLogic, которое можно использовать при логистике. Достаточная гибкость алгоритма позволяет пользователю оперативно менять количество групп и минимизировать путь в каждом случае.

Предлагаемый алгоритм может быть применен и для построения логистических цепочек в других производственных сферах или в другой деятельности, например, при распределении товаров по пунктам выдачи в крупных интернет-магазинах (например, Ozon).

Литература

1. anylogic.ru [Электронный ресурс]. — Режим доступа: https://www.anylogic.ru/blog/statya-sravnenie-instrumentov-imitatsionnogo-modelirovaniya/ (Дата обращения: 24.04.2022)

2. pandia.ru [Электронный ресурс]. — Режим доступа: https://pandia.ru/text/78/419/41691.php. (Дата обращения: 24.04.2022)

3. science-education.ru [Электронный ресурс]. — Режим доступа: https://science-education.ru/ru/article/view?id=11342 (Дата обращения: 24.04.2022)

4. science-education.ru [Электронный ресурс]. — Режим доступа: https://science-education.ru/ru/article/view?id=12599 (Дата обращения: 24.04.2022)

РЕКОМЕНДАЦИИ ПО ПОВЫШЕНИЮ УРОВНЯ ЗАЩИТЫ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ В СИСТЕМЕ ИБ, КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЙ, ПРИ ПРОВЕДЕНИИ ЦЕЛЕВЫХ ТРАНЗАКЦИИ

Петров Александр Дмитриевич, магистрант 1 курса кафедры информационной безопасности
Научный руководитель: **Сухотерин Александр Иванович**, к.воен.н., доцент кафедры информационной безопасности

С тех самых времен, когда подавляющее количество платежных и банковских операций перешло в сферу информатизации, различные виды мошенничества и мошеннические схемы в данной области начали развиваться активными темпами [6].

К самым известным атакам, совершенным против банковских систем за последние годы, можно отнести атаки, выполненные такими преступными организациями, как Lazarus, Cobalt, Lurk и другими.

Злоумышленники, совершая кибернетические атаки, берут в качестве цели системы межбанковских переводов, а также карточный процессинг и другие составляющие банковской системы переводов и совершения платежей [6].

Антифрод-система, онлайн-банкинг, противодействия банковскому мошенничеству.

RECOMMENDATIONS FOR INCREASING THE LEVEL OF PROTECTION AGAINST THREATS IN THE INFORMATION SECURITY SYSTEM, CREDIT AND FINANCIAL ORGANIZATIONS, WHEN CONDUCTING TARGETED TRANSACTIONS

Petrov Alexander, 1st year graduate student of the Department of Information security
Scientific adviser: **Sukhoterin Alexander**, Candidate of Military sciences, Associate professor of the Department of Information security

Since the days when the overwhelming number of payment and banking transactions moved to the field of informatization, various types of fraud and fraudulent schemes in this area began to develop at an active pace.

The most famous attacks against banking systems in recent years include attacks carried out by criminal organizations such as Lazarus, Cobalt, Lurk and others.

When attacking cyber attacks, cybercriminals target interbank transfer systems, as well as card processing and other components of the banking system for transfers and payments.

Anti-fraud system, online banking, anti-banking fraud.

Согласно данным, предоставленным в отчете Positive Technologies, в большинстве случаев злоумышленники в своей работе и при планировании атак используют 5 этапов, идущих друг за другом в строгой последовательности [6]:

1. Первым делом злоумышленники занимаются разведкой и тратят очень много сил на проведение подготовительных работ.
2. После этого они совершают проникновение во внутреннюю сеть.
3. Следующий этап – закрепление как точки входа, так и самого факта проникновения с последующем развитием планируемой атаки.
4. Сама атака, основанная на компрометации банковской системы.
5. Последний этап – сокрытие совершенного деяния.

Все эти 5 этапов актуальны при таких видах кибератак, как фишинг, заражение ПК или гаджета вирусами, применение кейлокеров, атаки в духе man-in-the-middle и использование уязвимости нулевого дня.

Квалифицированные работники Group-IB отметили семь самых распространенных вариантов хищения денег в случае атак на ДБО (или на систему дистанционного банковского обслуживания):

- социальная инженерия;
- проведение переводов карта-карта;
- переводы, осуществляемые при помощи онлайн-банкинга;
- перехват паролей и вообще всего доступа к банкингу на мобильном телефоне;
- использование поддельного мобильного банкинга;
- покупки, совершаемые при помощи магазинов мобильных приложений;
- похищение с помощью SMS-банкинга [6].

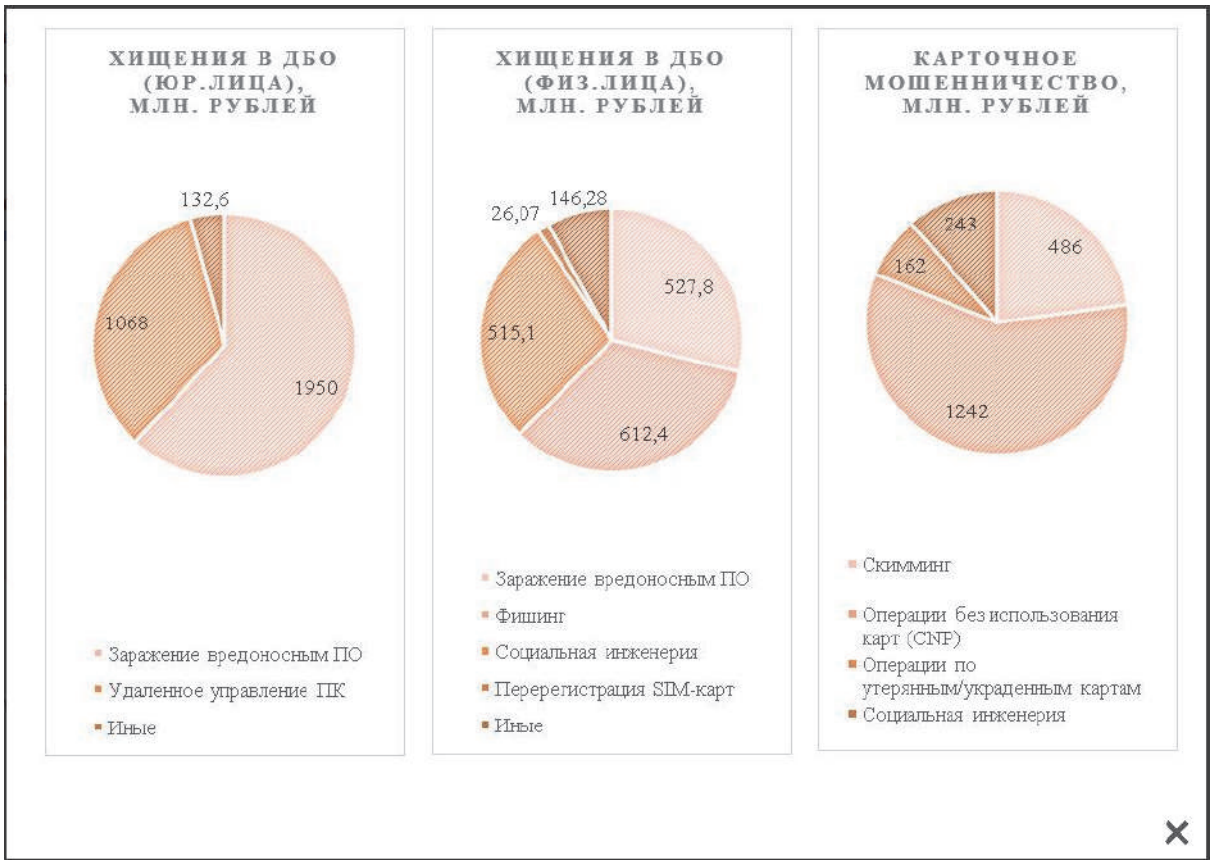


Рисунок 1 – Объем потерь от мошенничества в кредитно-финансовых организациях за 2015 год, по статистике от компании Инфосистемы Джет

Функции систем противодействия банковскому мошенничеству

Процессы, касающиеся как обнаружения, а также предотвращения мошеннических действий, отличаются тем, что у них нет конечных или же начальных стадий. Такие процесс должны выполняться постоянно и на беспрерывной основе, и состоять из таких подпроцессов, как:

- изучение и мониторинг;
- своевременное обнаружение;
- оперативное принятие оптимальных решений;
- обучение [6].

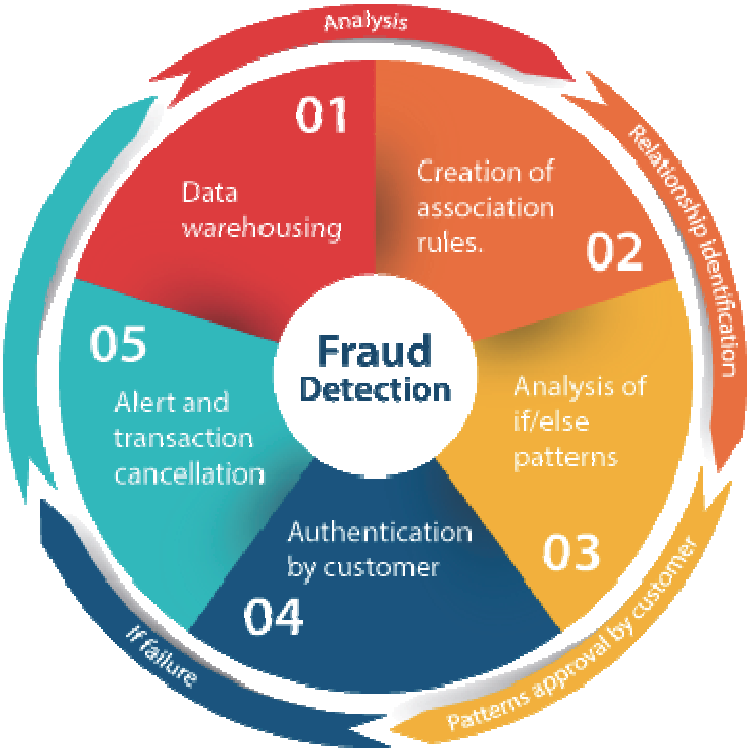


Рисунок 2 – Принцип работы антифрод-систем

Системы, связанные с противодействием мошенническим атакам, могут состоят из следующих возможностей и технологий:

- аналитика текста, выполняемая при помощи поиска, сортировки и извлечения необходимого контента из поступающей информации [6];
- расчет комплекса статистических данных и параметров, используемый для того, чтобы находить и выявляться любые отклонения, прямо или косвенно указывающие на возможность совершения мошеннических действий;
- сетевая аналитика, используемые для того, чтобы идентифицировать соединения и выявлять закономерности;
- Gap-тестирование, в рамках которого должен происходить поиск любых данных или элементов, находящихся в таких местах, где их быть вообще не должно;
- подтверждение времени и точной даты выхода, которое необходимо для более точной оценки подозрительного или же неподходящего времени для размещения информации или для ее ввода;
- машинное контролируемое обучение, создаваемое и управляемое на основании имеющихся исторических данных, позволяющих выявлять некоторые шаблоны, стандартны и уже устоявшиеся методики;
- обучение, совершаемое без помощи учителя, что также говорит об анализе или об оценке данных, не содержащих сведений об обнаруженном мошенничестве;
- выявление новых аномалий [6].

У всех существующих антифрод-систем есть только одна единая функция, и заключается она в выявлении и последующем предотвращении мошеннических действий. Правда, здесь стоит отметить и то, что эти системы способны решать свою задачу совершенно разными, даже кардинально отличающимися друг от друга способами. Также они способны сравнивать особенности и алгоритмы работы других антифрод-систем без каких-либо дополнительных классификаций, что является в корне неверным решением [6].

К примеру, существуют core-системы, являющиеся аналитическими мощными платформами, позволяющими воплощать в жизнь и в работу логику в некоторых отдельно взятых сегментах (ДБО или процессинг банковских карт). Также, одновременно с ними, существуют и специальные системы, отвечающие за контроль параметров устройств, а также рисков с их стороны.

Одновременно с этим создаются отдельно работающие системы, чья рабочая деятельность заточена под распознавание речи, а также видео и фото данных.

Представленные системы не только не конкурируют, но и дополняют друг друга за счет наличия у них уникальных функций. К примеру, определенные решения с узкой специализацией не способны в одиночку закрывать те требования, которые указаны в 167-ФЗ от 27 июня 2018 года «О внесении изменений в законодательные акты в сфере взаимодействия хищению денег». Также такие решения, даже при их реализации, все равно не могут работать как отдельные независимые платформы.

Исходя из этих особенностей можно поделить существующую сегодня систему, направленное на противодействие мошенничеству в банковской сфере, на 3 отдельных класса:

- 1 класс. Решения, направленные на определение, выявление, а также на идентификацию мошеннических следов, а также на поиск и определение аномалий.

- 2 класс. Решения, направленные на то, чтобы идентифицировать элементы, инструменты и способы мошеннических действий, а также на то, чтобы определить причины или возможные риски.

- 3 класс. Решения, позволяющие решать различные задачи узкой специализации (распознавание речи, изображений и т.д.) [6].

Комплексные системы обнаружения банковского мошенничества и выявления аномалий

Компания Group-IB появилась в 2003-ом году в городе Москва. Главные направления этой компании – найти, предотвратить, а также расследовать любые случаи киберпреступной деятельности. Также компания должна заниматься компьютерной криминалистикой, аудитом и консалтингом систем информационной безопасности. Для того, чтобы достичь этих целей, компания, в числе прочих задач, также занимается

созданием систем, позволяющих предупредить потенциальную киберугрозу. [6]

Антифрод-система, разработанная организацией Group-IB, получила название Secure Bank. Система способна не только выявлять и своевременно предотвращать мошеннические действия с невероятно быстрой реакцией, но и обеспечить защиту от мошенничества различных видов, включая CNP, использование P2P-страниц и другие.

Также система способна выявить и защитить банковскую сферу от кроссканальных мошеннических действий (атаки с помощью онлайн-порталы) и от кредитного мошенничества.

Поимо этого, система позволяет идентифицировать устройство клиентов с последующим предоставлением этих устройств и их показателей доверенности банку для улучшения и ускорения оптимизации работы банка по защите от пользовательского опыта [6].

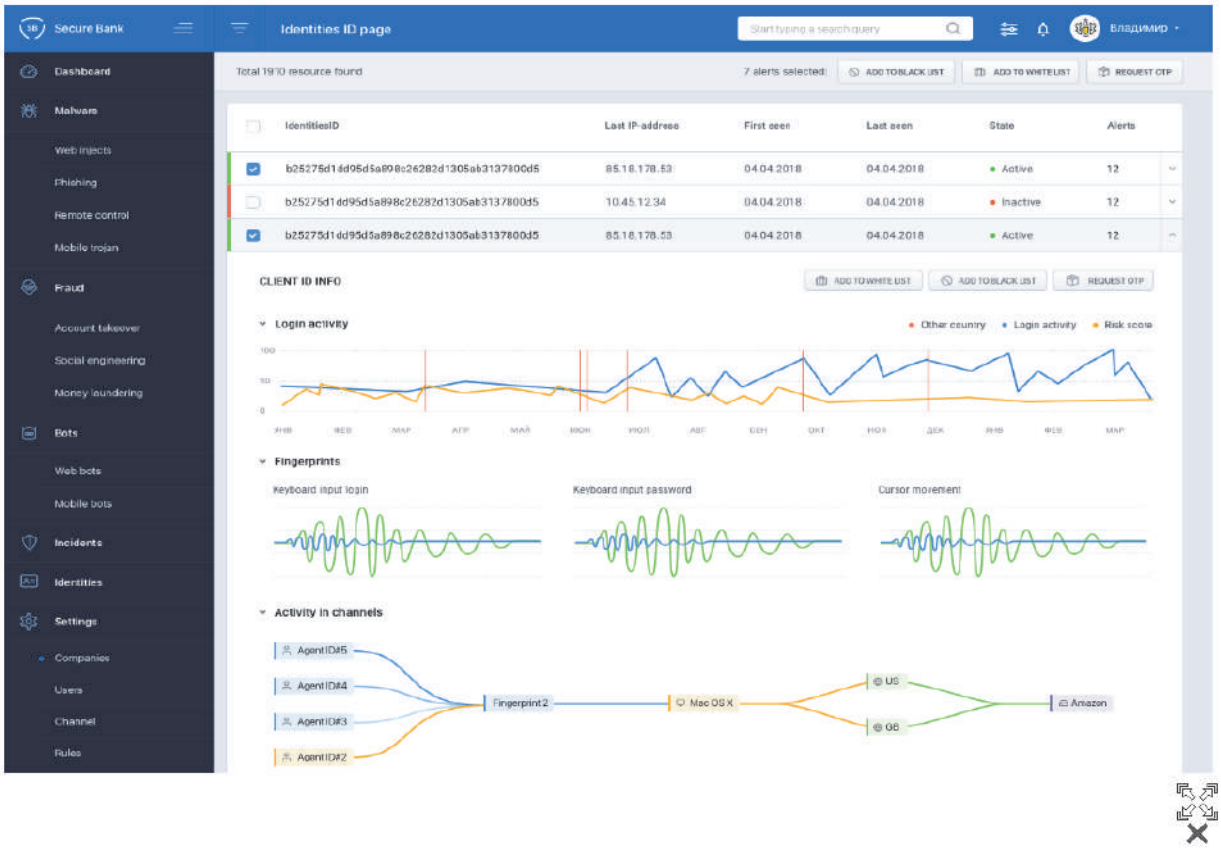


Рисунок 3 – Интерфейс системы Secure Bank

Особенности Secure Bank

Среди основных особенностей Secure Bank можно выделить такие, как:

- применение UEBA, то есть технологий анализа поведения, что поможет в случае захвата учетных записей или при социальной инженерии [6];

- анализ технических параметров того или иного устройства, а также браузера (цифровой отпечаток);

- создание пользовательских профилей, способных отличить мошенника и клиента;

- гибко настраиваемый конструктор правил;

- модуль JavaScript, встраиваемый в исходный код, а также SDR для мобильных приложений, способные защитить от подмены информации и replay-атак;

- готовая интеграция с антифрод-системами вроде RSA, SAS, GBG Predator [6].

Также стоит отметить еще одну компанию, а именно «Лабораторию Касперского», которая появилась еще в 1997 году в том же городе Москва. Компания с самого первого дня работы взяла для себя направление защиты конечных станций, а также создание защиты для коммерческого или же для частного использования [6].

Сейчас компания вовсю занимается развитием таких продуктов защиты, которые ориентированы на обеспечение безопасности как облачных, так и виртуальных сред, различных критических инфраструктур и средств, защищающих от мошенничества.

Одно из распространенных решений Лаборатории – это Fraud prevention. Данное решение необходимо для того, чтобы решить проблемы мошенничества в онлайн банковской составляющей, а также в онлайн играх, государственных веб-сервисах и в иных отраслях, которые используют интернет и сайты (а также приложения) для того, чтобы предоставлять свои услуги [6].

В рамках представленного решения появилось два продукта:

- Automated Fraud Analytics. Данное решение способно определять и обнаруживать похищение учетных записей, находить опасные программы и приложения без каких-либо дополнительных установок [6].
- Advanced Authentication. Это решение может предоставлять результаты проводимой аутентификации на основе изученных, возможных и вероятных рисков. Подобное решение позволяет значительно улучшить уровень безопасности, а также улучшить пользовательский опыт и максимально сократить риски на уже ставшие стандартами подходы к аутентификации [6].

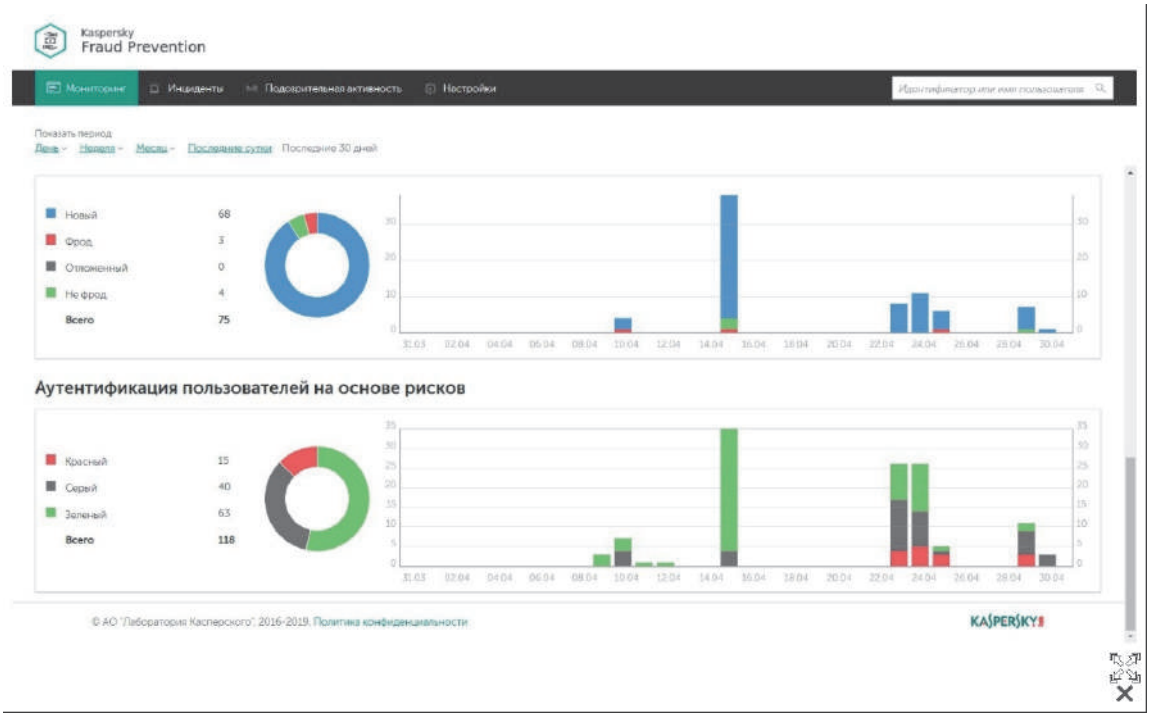


Рисунок 4 – Интерфейс системы Kaspersky Fraud Prevention

Особенности Kaspersky Fraud Prevention:

- проактивное и беспрерывное обнаружение мошеннических схем до того, как были проведены транзакции; [6]
- кроссканальное обнаружение мошенников;
- использование поведенческой, личностной и иной биометрии для сбора данных;
- применение технологий обучения и анализа поведения для обеспечения защиты от программ, способных нанести вред;
- анализ цифровых профилей устройств и их владельцев;
- предотвращение таких мероприятий, которые направлены на отмывание денег [6].

Мошенничество, быстро распространяющееся внутри банковской сферы, продолжает не только распространятся, но и прогрессировать. Именно поэтому, в ответ на повышающееся мошенничество, необходимо улучшать рынок средств, методом и технологий против такого мошенничества, в чем преуспела Америка. Но и для России актуальным стало создание защиты от фрода [6].

При грамотном подборе методик и мер защиты от мошенничества необходимо определить те задачи, которые защита должна выполнять. Чаще всего для того, чтобы обеспечить надежную защиту в банковской сфере, необходимо использовать антифрод-системы различных классов.

При всем этом, в процессе выбора аналитических общих платформ для защиты необходимо грамотно отметить саму сложность внедрения, а также уровень удобства при использовании.

При выборе же систем, относящихся ко второму классу, необходимо обратить внимание на используемые методы, а при выборе продуктов 3 класса учесть то, что они в состоянии дополнить уже существующую систему защиты [6].

Литература

1. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646).

2. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 31.12.2017) "О персональных данных".

3. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ.

4. ГОСТ Р 52069.0-2003 «Защита информации. Система стандартов. Основные положения».

5. ГОСТ Р 51898-2002 «Аспекты безопасности. Правила включения в стандарты».

6. Электронный ресурс. Режим доступа: https://www.anti-malware.ru/analytics/Market_Analysis/anti-fraud-Bank-systems#part4 (дата обращения: 08.10.2020)

ПУТИ РАЗВИТИЯ СИСТЕМ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ И РЫНКА БИОМЕТРИИ В РОССИИ

Пунгин Глеб Александрович, магистрант 1 курса кафедры информационной безопасности
Научный руководитель: **Воронов Александр Николаевич**, к.воен.н., доцент кафедры информационной безопасности

Практическая роль и место информационной безопасности в системе управления организацией повышается в связи с распространением цифровых технологий. Исходя из этого, актуальным выступает применение биометрической аутентификации, как инструмента обеспечения информационной безопасности. В рамках статьи рассмотрены основные тенденции и перспективы развития систем биометрической аутентификации, а также рынка технологий биометрии в Российской Федерации. Определены возможные проблемы и барьеры в распространении систем биометрической аутентификации при совершенствовании информационной безопасности в организациях.

Информационная безопасность организации, система биометрической аутентификации, рынок биометрии, технологии биометрии.

WAYS OF DEVELOPMENT OF BIOMETRIC AUTHENTICATION SYSTEMS AND BIOMETRY MARKET IN RUSSIA

Pungin Gleb, 1st year graduate student of the Department of Information security
Scientific adviser: **Voronov Alexander**, Candidate of Military sciences, Associate professor of the Department of Information security

The practical role and place of information security in the management system of an organization is increasing due to the spread of digital technologies. Based on this, the use of biometric authentication as a tool for ensuring information security is relevant. Within the framework of the article, the main trends and prospects for the development of biometric authentication systems, as well as the biometric technology market in the Russian Federation, are considered. Possible problems and barriers in the dissemination of biometric authentication systems while improving information security in organizations are identified.

Information security of an organization, biometric authentication system, biometrics market, biometrics technologies.

Коммерческая деятельность организации предполагает производственные и управленческие процессы, одним из ресурсов которых

выступает информация. При управлении бизнес-процессами и передачи информации происходит коммуникационная связь, в основе которой лежит необходимость обеспечения информационной безопасности.

На уровне людей информация является также важным инструментом при управлении коммуникациями. Все чаще происходит обмен различными данными через социальные сети и мессенджеры, которые слабо защищены от кражи информации и взлома профилей или паролей.

Кроме того, актуальность формирования эффективной системы информационной безопасности связана с тенденциями, которые наблюдаются вокруг цифровой трансформации бизнес-процессов и бизнес-модели. Все больше количество российских предприятий внедряют различные цифровые технологии и инновации, которые совершенствуют их хозяйственную деятельность. Вместе с преимуществами от автоматизации и цифровизации появляются недостатки в виде негативного влияния новых угроз, связанных, как раз с информационной безопасностью.

Так, на рисунке 1 изображена динамика основных показателей развития сектора ИКТ в экономике Российской Федерации.

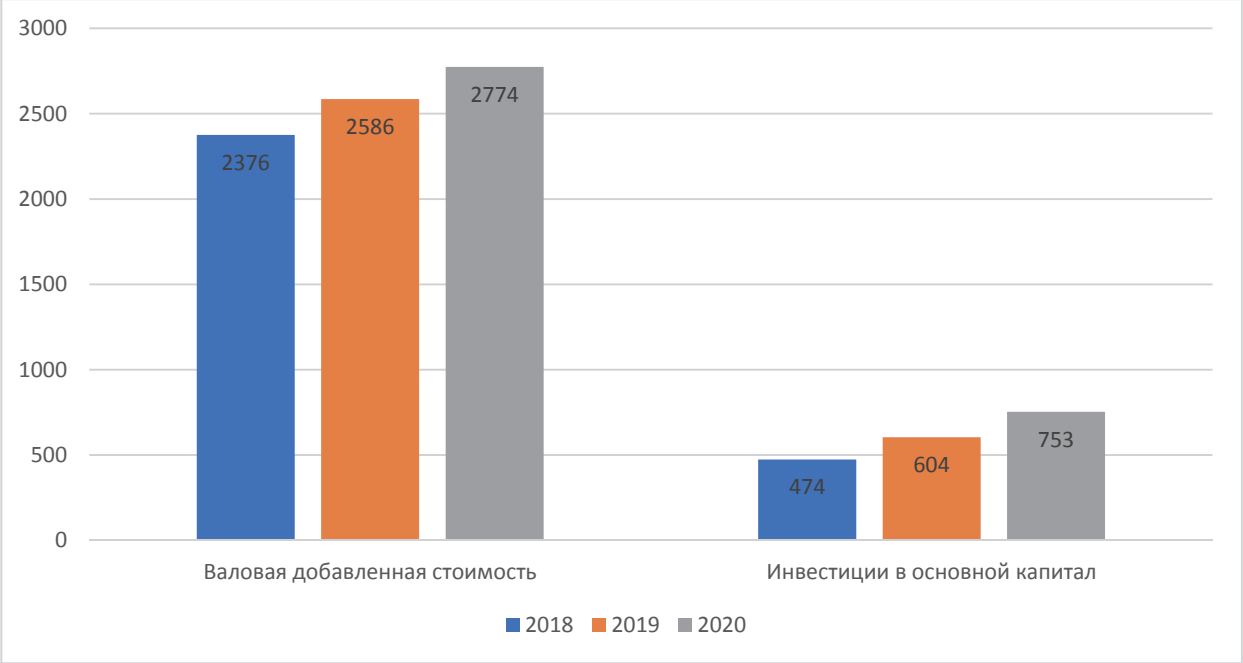


Рисунок 1 – Динамика показателя развития ИКТ в России, в млрд рублей [1]

В периоде с 2018 по 2020 гг. валовая добавленная стоимость, производимая в секторе ИКТ увеличилась с 2,376 трлн руб. до 2,774 руб. Наблюдается и увеличение объема капитальных вложений компаний в создание новых объектов производства высокотехнологической продукции, включая информационных технологий и цифровых систем.

В итоге, современное состояние ИКТ в России демонстрирует в основном тенденцию роста и развития. Увеличивается инновационная активность, повышается объем производства инновационной продукции, стимулируется рост капитальных вложений в инновационные проекты организаций. Таким образом, в дальнейшем инновационное развитие будет стимулировать увеличение перспектив социально-экономического прогресса нашего государства.

Однако внедрение различных инноваций повышает роль информации и механизмов ее защиты, поскольку при использовании различных информационных ресурсов формируются угрозы утечки данных.

Также актуальность обеспечения информационной безопасности связана из-за нечестных методов конкуренции, поскольку есть ряд предприятий, совершающих такие экономические преступления, как:

- промышленный шпионаж;
- кража и незаконное использование объектов интеллектуальной собственности (патентов, изобретение, лицензий);
- кража конфиденциальной информации и ее использование в собственных коммерческих целях.

Кроме того, в 2020 году на 51% увеличилось количество атак злоумышленников на корпоративные информационные системы российских организаций (рисунок 2).

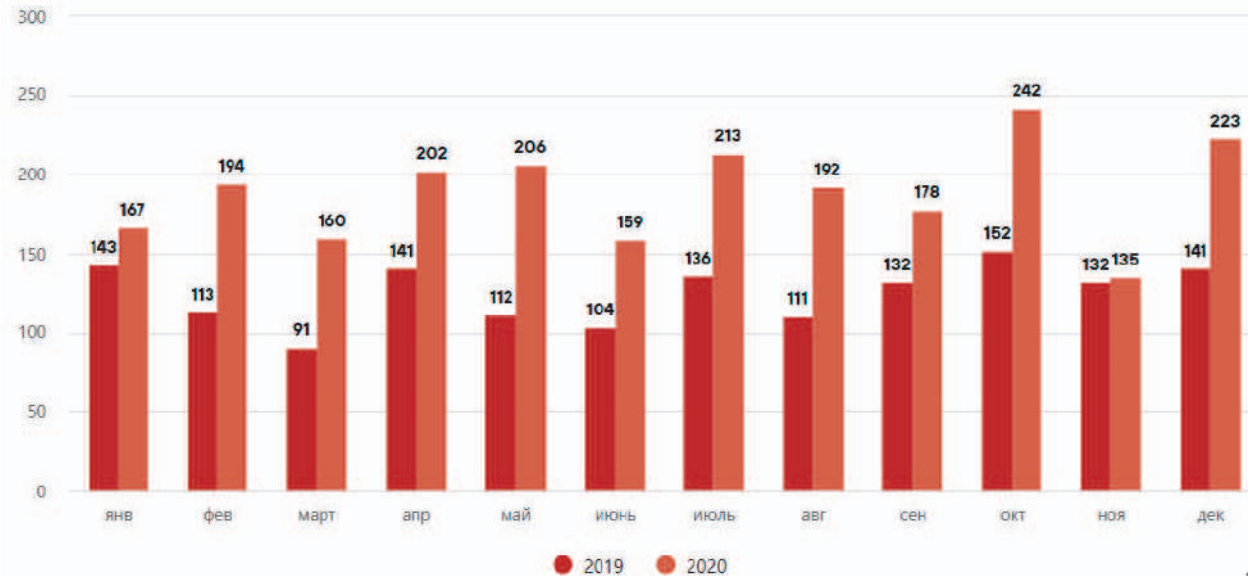


Рисунок 2 – Количество инцидентов с взломом информационных систем организаций [4]

В российской практике все чаще наблюдается такая проблема обеспечения информационной безопасности организаций, как хакерские атаки и утечка информации.

Например, в середине сентября 2021 года стало известно о крупной утечке данных абонентов «ВымпелКома». В свободном доступе оказались персональные данные пользователей услуг домашнего интернета.

С учетом высокой практической роли информационной безопасности необходимо использование таких методов защиты информации, как [2]:

1. Принятие ограничительных мер, направленных на настройку доступа к важным данным и коммерческой информации только тем сотрудникам и управляющим, которые ответственны за выполнение задачи и проведение бизнес-процесса, где данная информация нужна.

2. Совершенствование системы информационной безопасности при помощи внедрения новых цифровых и информационных технологий, повышающих безопасность управления и распределения данными и информацией.

Важнейшим аспектом совершенствования системы информационной безопасности организации является функционирование биометрических систем. Биометрия определяется как система распознавания людей по одной или более физических, или поведенческих черт.

Биометрическая система – это технологическая система, которая использует информацию о человеке для идентификации этого человека. Биометрические системы полагаются на конкретные данные об уникальных биологических признаках, чтобы работать эффективно.

Биометрическая система будет включать обработку данных с помощью алгоритмов для получения определенного результата, обычно связанного с достоверной идентификацией пользователя или другого лица.

На рисунке 3 изображены основные методы биометрической аутентификации.

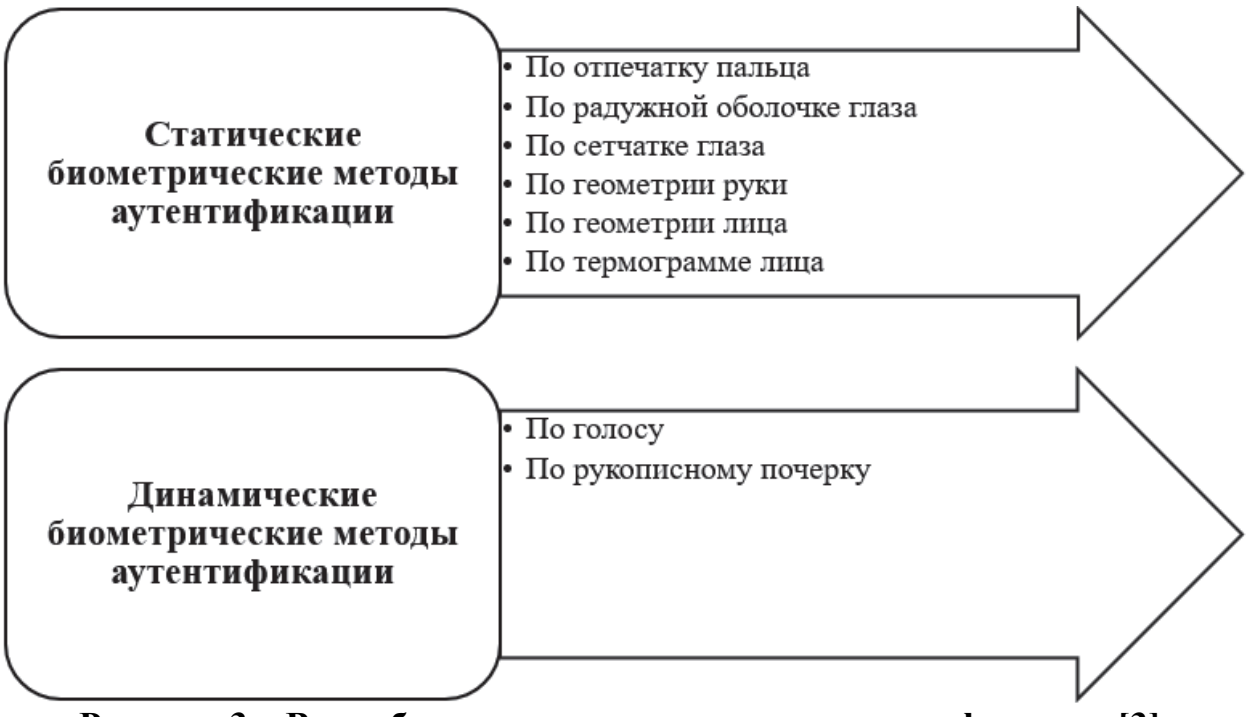


Рисунок 3 – Виды биометрических методов аутентификации [3]

Помимо статистических и динамических методов есть и современные инструменты биометрических систем обеспечения информационной безопасности, как метод LBP и метод k-ближайших соседей.

Причиной применения систем биометрической аутентификации при обеспечении информационной безопасности организации является наличие следующих преимуществ, как:

- отсутствие угрозы потери личных данных;
- легкость в пользовании из-за отсутствия лишних процессов;
- максимальный уровень сложности подделки биометрических данных для взлома системы безопасности.

По прогнозам MarketsandMarkets, размер мирового рынка средств контроля доступа при помощи использования технологий биометрии вырастет с 8,6 млрд долларов США в 2020 году до 12,8 млрд долларов США к 2025 году. При этом среднегодовой темп роста составит 8,2% [5].

Основными драйверами роста рынка биометрии в России будут выступать следующие факторы, как [6]:

- растущая осведомленность граждан о необходимости применения домашней системы информационной безопасности;
- тенденции роста сектора ИКТ, которые постоянно создает новые технологические достижения и инновации, которые совершенствуют систему информационной безопасности;
- увеличение числа пользователей беспроводных СКУД, из-за чего повышается необходимость внедрения систем биометрической аутентификации;
- развитие технологии биометрии не только в корпоративном секторе (поскольку ранее биометрию использовали лишь крупные корпорации), но и в потребительском секторе, где много гаджетов людей оснащены данными технологиями;
- развитие технологии искусственного интеллекта и машинного обучения;
- создание на территории России технологических компаний, которые разрабатывают качественные алгоритмы идентификации по лицу.

Согласно данным по прогнозу Банка России в 2022 году российский рынок биометрии будет составлять около 240 млн долларов США. В 2018 году объем рынка составлял лишь 90 млн долларов США. Глобальный рынок технологии систем биометрической аутентификации в 2022 году может увеличиться до 43 млрд долларов США [7].

На рисунке 4 изобразим структуры рынка биометрии в России, которая должна быть к концу 2022 года.

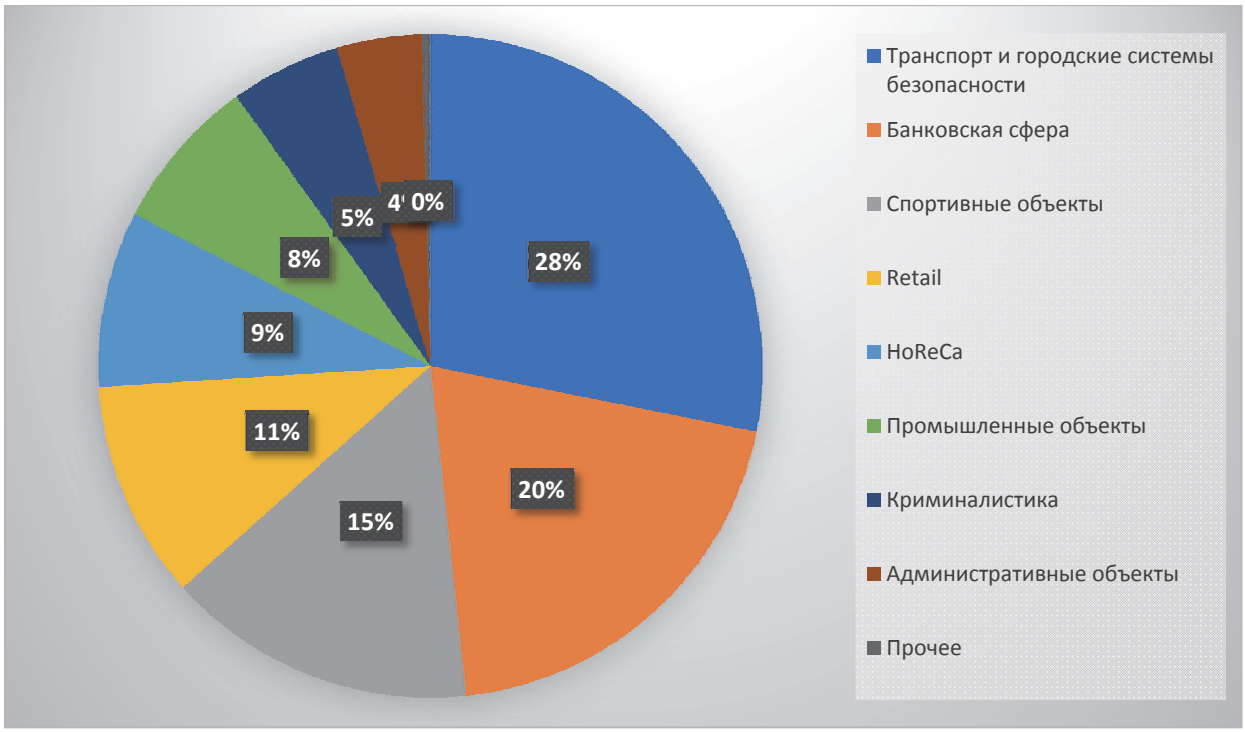


Рисунок 4 – Структура рынка биометрии в России по отраслям применения систем биометрической аутентификации [7]

Таким образом, основной сферой применения биометрии в российской практике является транспорт и городские системы безопасности. Далее идут коммерческие банки, спортивные объекты и сектор Retail.

Среди основных проблем развития рынка биометрии в России стоит перечислить:

- высокие затраты организации на сбор данных, которые необходимы для работы систем биометрической аутентификации;
- недоверие общества и граждан к данному способу аутентификации;
- клиенты, которые проходят проверку при помощи системы биометрической аутентификации становятся публичными и их более сложно удерживать организациям или банкам;
- активное участие Правительства РФ с 2020 года при регулировании рынка биометрии, что создает дополнительные административные и нормативно-правовые барьеры развития технологий и компаний, создающих системы биометрической аутентификации.

Таким образом, можно заключить следующее: что системы биометрической аутентификации для российских организаций являются перспективным инструментом и методом в совершенствовании информационной безопасности. Их практическое распространение будет с каждым годом больше. Тем самым, предприятия смогут обезопасить свои личные данные и коммерчески важную информацию от взлома при промышленном шпионаже или кражи конфиденциальной информации.

Литература

1. Цифровая экономика: 2021: краткий статистический сборник / Г.И. Абдрахманова, К.О. Вишневский, Л.М. Гохберг и др.; Нац. исслед. ун-т «Высшая школа экономики». – М.: НИУ ВШЭ, 2021. – 124 с.

2. Гребенникова В.А., Помогаева К.Г. Обзор биометрических технологий и их применение в банке ВТБ // Международный журнал прикладных наук и технологий «Integral». 2019. №3.

3. Бутов А.В., Карякин А.М. Проблемы развития биометрии как основы цифровизации отечественной экономики и пути их решения // Известия ВУЗов ЭФиУП. 2020. №1 (43).

4. Актуальные киберугрозы: итоги 2020 года. Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/ (дата обращения: 09.04.2022).

5. Мировой и российский рынки биометрии. Режим доступа: http://www.techportal.ru/security/biometrics/mirovoy-i-rossiyskiy-rynki-biometrii/#mirovoy-rynok (дата обращения: 09.04.2022).

6. Российский биометрический рынок в 2019–2022 годах. Режим доступа: https://www.tbforum.ru/blog/rossijskij-biometricheskij-rynok-v-2019-2022-godah.-rezultaty-masshtabnogo-issledovaniya-json-partners-consulting (дата обращения: 09.04.2022).

7. Прогнозы развития рынка биометрии в России. Режим доступа: https://bio.rt.ru/upload/iblock/9ee/Prezentatsiya-Edinoy-biometricheskiy-sistemy-_Versiya-ot-21.05.2021_.pdf (дата обращения: 09.04.2022).

ПРИМЕНЕНИЕ МЕТОДОВ РАЗГРАНИЧЕНИЯ ДОСТУПА В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Пушкарев Павел Вячеславович, Солодухин Илья Валентинович,
магистранты 1 курса кафедры информационных технологий и управляющих систем
Научный руководитель: **Исаева Галина Николаевна,** к.т.н., доцент кафедры информационных технологий и управляющих систем

В статье рассматриваются и сравниваются различные методы разграничения доступа в информационных системах. Приводится описание каждого метода и обсуждаются их преимущества и недостатки. Разграничение доступа — это система определения полномочий субъекта в информационной системе и обеспечения их действий строго в рамках, установленных для них полномочий. Система, которая, с одной стороны, определяет, кому из субъектов разрешён допуск к тем или иным объектам, и с другой стороны, не позволяет им превышать собственные полномочия.

Разграничение доступа, информационная система, обмен сообщениями.

MODERNIZATION OF THE SYSTEM FOR GRANTING ACCESS RIGHTS IN MESSAGE MESSAGES

Pushkarev Pavel, Solodukhin Ilya, 1st year graduate student of the Department of Information technology and system management
Scientific adviser: **Isaeva Galina,** Candidate of Technical sciences, Associate professor of the Department of Information technology and system management

The article discusses and compares various methods of access control to information technology. Each method is given and their description is examined. Access control is a system of definitions established for consideration within the framework and requiring their strict observance in the framework of drawing up protocols for them. A system that, on the one hand, determines which of the subjects is allowed access to those other objects, and on the other hand, does not allow them to impose authority on themselves.

Access control, information system, messaging.

В наши дни люди очень часто ведут общение друг с другом через интернет. Сейчас люди все чаще выбирают дистанционный формат общения вместо того, чтобы встречаться лично. Поэтому существует множество различных способов общения в интернете, самым популярным из которых

является мессенджер. В нем люди могут вести диалог с каким-нибудь другим пользователем, либо с несколькими одновременно.

Выбранная для исследования система обмена сообщениями имеет функциональность разделения полномочий пользователей, однако данная система, хоть и имеет гибкую систему разделения прав использования, недостаточно удобна для пользователя из-за того, что пользователям будет сложно адаптироваться к правилам поведения в групповых чатах.

Разграничение доступа реализуется для решения следующих задач:

- обеспечение конфиденциальности информации;
- обеспечения целостности и информации;
- обеспечения доступности информации.

Обеспечение конфиденциальности достигается за счет того, что субъекту, не входящему в круг легальных пользователей той или иной конфиденциальной информации, не будет предоставлен доступ к этой информации. Пользователям, которые могут нанести вред целостности или доступности информации, доступ к ней не предоставляется.

Разграничение доступа позволяет обеспечивать контроль действий пользователя. Это происходит за счёт того, что каждый пользователь действует строго в рамках своих полномочий в системе и не может их превысить. Разграничение доступа служит реализацией принципов минимизации полномочий и разделения обязанностей, то есть каждый из субъектов в системе обладает только тем набором прав, который соответствует его должностным обязанностям. Необходимо, чтобы ни к каким дополнительным ресурсам системы пользователь не имел бы доступа, так как это является уязвимостью, которой может воспользоваться злоумышленник, обойдя систему аутентификации и представившись легальным пользователем.

Системы разграничения доступа могут оцениваться по следующим параметрам:

- трудоёмкость первоначальной настройки;
- возможность настройки полномочий в нетипичных случаях;
- удобство добавления нового субъекта или объекта.

Трудоёмкость первоначальной настройки заключается в оформлении прав всех пользователей для того, чтобы система могла начать функционировать и корректно предоставлять пользователям права в информационной системе (ИС).

Возможность настройки полномочий в нетипичных ситуациях также характеризует качество системы разграничения доступа. Например, должны ли руководители разных отделов иметь доступ к информации, относящейся к ведению другого отдела? Должен ли бухгалтер иметь доступ к файлу паролей, который, относится к ведению службы безопасности? И наоборот, должен ли администратор безопасности ИС иметь доступ к файлу с ведомостью на получение заработной платы сотрудников? Должен ли

пользователь быть допущен к информации или нет, зависит от решения того, кто имеет полномочия на разделение прав доступа. Возможность реализации на практике прав доступа зависит от того, какая система разграничения доступа была выбрана. Некоторые модели позволяют более тонкие настройки прав пользователей, а некоторые — нет.

Ещё одно важное качество, которое влияет на удобство системы разграничения доступа — это удобство добавления нового субъекта или объекта. Под субъектом здесь подразумевается пользователь информационной системы, а под объектом — файл или иной информационный ресурс.

После того, как субъект благополучно пройдёт процедуру авторизации, то есть получит доступ к тем полномочиям, которые предоставлены ему в системе, контроль его подлинности не осуществляется. Как правило, такая процедура проходится единожды. Но, иногда, может потребоваться дополнительное подтверждение подлинности субъекта, и это является хорошим решением.

Система разграничения доступа без использования других средств защиты информации, не ограничивает действия привилегированных пользователей, например, администраторов безопасности и тех сотрудников, службы безопасности, которые производят настройку системы разграничения доступа и имеют полномочия предоставлять права другим пользователям.

Разграничение доступа, как правило, строится на одной из трёх следующих моделях: дискреционное разграничение доступа, мандатное разграничение доступа и ролевое разграничение доступа.

Дискреционная модель основывается на разграничении доступа с использованием поименованных субъектов и объектов на основе установленных прав доступа для каждой пары. В основе работы модели лежит формирование так называемой матрицы прав доступа. Строки и столбцы данной матрицы соответствуют субъектам и объектам, а на их пересечении находятся права, которые субъекты имеют по отношению к объектам. Например, субъект может обладать только правом чтения или правами на чтение и запись, либо может иметь какие-то другие наборы прав. В большинстве случаев субъекту выдается признак наличия или отсутствия права доступа, например, ноль или единица.

Каждый из пользователей обращается к системе разграничения доступа через сервер авторизации для того, чтобы осуществить попытку доступа к какому-либо объекту в информационной системе. Сервис авторизации, который, принимает решение о том, обладает ли пользователь правами на получение запрашиваемого объекта, обращается к базе данных, в которой хранится матрица доступа. Матрица содержит строку, в которой записан идентификатор пользователя, и в одном из столбцов — название того объекта, к которому пользователь желает обратиться. Если на пересечении строки и столбца находится информация о том, что данный пользователь

действительно имеет право для реализации такого доступа, то доступ предоставляется, в противном случае в доступе будет отказано.

Данная модель имеет следующие достоинства:

- Индивидуальная настройка прав для каждого пользователя;
- Для каждого объекта можно настроить права доступа, то есть ту группу субъектов, которая будет иметь к ним доступ.

Индивидуальная настройка прав для каждого пользователя доступна за счет того, что заполняется полная матрица соответствия субъектов и объектов. Например, в модели с двумя начальниками двух отделов можно настроить для каждого из них нужный уровень доступа к тем или иным файлам, относящимся к ведению их отделов, и не предоставлять им прав на доступ к файлам других отделов. При настройке для каждого объекта прав доступа не будет образовываться зависимость между сходством в уровне секретности объектов или в должностном уровне субъектов. Например, два системных администратора, могут иметь совершенно разный набор прав доступа к объектам, например, на основе их опыта, или на основе их должностных обязанностей.

Недостатком модели является то, что для реализации модели требуется полностью заполнить матрицу субъектов и объектов в каждой ее ячейке - на пересечении каждого столбца и каждой строки установить конкретные права доступа данного субъекта к данному объекту. Из этого следует, что для добавления нового субъекта или объекта требуется заполнить все элементы соответствующей строки или столбца матрицы доступа. При добавлении нового субъекта, появляется строка, в которой нужно прописать права его доступа ко всем существующим объектам. А, при добавлении нового объекта, для всех субъектов, которые описаны в системе, требуется установить их права доступа к новому объекту.

Мандатная модель разделения доступа. Данная модель использует определенные значения, называемые метками конфиденциальности и уровнями допуска субъектов. Меткой конфиденциальности является уровень конфиденциальности, который назначается субъекту информационной системой. Рассмотрим, для примера, некоторую организацию, в которой существуют следующие метки конфиденциальности: информация общего пользования, специальная информация, секретная и абсолютно секретная информация. Таким образом, можно сказать, что все ресурсы системы занимают одну из четырех позиций в вертикали уровней доступности. Из этого видно, что метка конфиденциальности – отношение какого-либо объекта к определенному уровню доступа. Отсюда можно обозначить определение уровня доступа – это степень конфиденциальности, выше которой субъект с данной ему меткой конфиденциальности не сможет получить. Допустим, если субъект имеет уровень доступа «специальный» сто означает то, что ему доступны все объекты с меткой конфиденциальности «не секретно» и «специальная информация». Однако, в таком случае, субъект

не сможет иметь доступ к объектам с уровнем доступа с другими метками конфиденциальности. Если в организации работают сотрудники, имеющие одну и туже должность, то все они будут обладать одним и тем же уровнем доступа. Получается, что все те объекты, к которым они будут иметь доступ будет полностью одинаковым.

Уровень доступа сопоставляется и сравнивается с меткой конфиденциальности объекта с той целью, чтобы понять имеет ли пользователь права на получение объекта. Доступ к объекту может быть получен, если уровень доступа не ниже метки конфиденциальности. Если рассмотреть такую ситуацию, в которой есть пользователь с уровнем доступа «секретно» будет запрашивать объект с меткой конфиденциальности «специальная информация», то этот пользователь сможет получить запрашиваемую информацию. Но, если пользователь будет иметь уровень доступа слабее, чем «служебная информация», то он не сможет получить нужный для него объект.

Преимуществом такого подхода является то, что для того, чтобы его воплотить, нужно всего лишь присвоить каждому субъекту уровень доступа, а каждому объекту предоставить метку конфиденциальности. При таком подходе, при появлении в ИС нового субъекта или нового объекта, не будет необходимости в изменении полномочий других объектов и субъектов. Назначение прав будет намного удобнее, чем полное редактирование матрицы для каждой связи между объектом и субъектом. Когда в информационную систему будет добавлен новый объект, ему автоматически будет присвоена метка конфиденциальности, а когда в системе зарегистрируется новый субъект, то ему будет назначен уровень доступа. Больше системе не нужно будет производить никаких действий.

В качестве минуса можно выделить то, что для объектов с одной и той же степенью доступности доступ будет выдан или не выдан для них совместно. Нельзя разложить все объекты, имеющие уровень доступа «для корпоративного использования» на часть, которой сможет пользоваться глава отдела и на часть, которой он воспользоваться не сможет.

Ролевая модель разделения доступа. Ролевая модель, как следует из ее названия, основывается на так называемых ролях субъектов информационной системы. Под ролью в данной модели подразумевается совокупность прав доступа субъекта к объектам информационной системы. То есть существует определенное фиксированное значение этих прав доступа субъекта, которое единожды сохраняется и именуется каким-то названием. Например, может быть роль «системный администратор». В этом случае существует некий набор прав, который является стандартным для системного администратора. Так же в системе может присутствовать роль начальника отдела, роль оператора, роль бухгалтера. Каждой роли, по аналогии с дискреционной системой разграничения доступа, присваивается набор прав доступа к различным объектам системы.

Такой подход имеет ряд достоинств:

- Добавление нового субъекта не требует заполнения строки матрицы при наличии подходящей роли;
- Количество ролей ничем не ограничено;
- Роль не предполагает полного нисходящего предоставления доступа к объектам информационной системы.

Для того, чтобы добавить нового пользователя в информационную систему, по сравнению с дискреционной моделью разграничения доступа уже не требуется полностью заполнять всю строчку его прав доступа ко всем объектам в информационной системе, которых может быть очень большое количество. Неограниченное количество ролей дает возможность создавать специальные роли, например, начальника конкретного отдела или помощника начальника конкретного отдела. В отличие от мандатной модели разделения доступа, ролевая модель не предполагает полного нисходящего предоставления доступа к объектам информационной системы. Например, администратору можно предоставить доступ к файлу с уровнем секретности, который в мандатной модели имел бы метку конфиденциальности «секретно», но при этом относится, допустим, к вопросам администрирования информационной системы. И при этом не предоставить ему права доступа к тем объектам, которые в мандатной модели имели бы более низкие метки конфиденциальности. Роль вполне это допускает. Полное нисходящее предоставление доступа к объектам не предполагается.

Недостатком является то, что если для каждого субъекта требуется отдельная роль, то разграничение доступа станет аналогичным дискреционной модели, и необходимость в ролях может отпасть. Если доступ предоставляется к отдельным объектам, а не группам объектов, то добавление нового объекта аналогично дискреционной модели. В классической ролевой модели о группировании объектов речи не идет. Создаются роли для субъектов, а объекты, описываются независимо отдельными строками в этой матрице. По сути, речь идет о формировании такой матрицы, где каждой строкой является не субъект, а роль. Ролевая модель имеет смысл, если под одну роль подходит более одного субъекта.

Выводы:

В ходе исследования был проведён обзор методов разграничения доступа в информационных системах. Рассмотрены основные модели разделения доступа: дискреционная, мандатная и ролевая. Были выявлены их достоинства и недостатки.

Данные подходы и методы целесообразно применять и в образовательных информационных системах, реализуемых как на базе кафедры информационных технологий и управляющих систем, так и в ИС, развёртываемых в ГБОУ ВО МО «Технологический университет».

Литература

1. Бопп В. А. Типы моделей разграничения доступа/ Статья 2020, - С.233-235, Режим доступа: https://cyberleninka.ru/article/n/tipy-modeley-razgranicheniya-dostupa (Дата обращения 15.04.2022)

2. Васильков А.В. Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков.— Москва : ФОРУМ: ИНФРА-М, 2013.— 368с.

3. Зегжда Д. П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко.— Москва : Горячая линяя — Телеком, 2000.— 452с.

4. Малюк А.А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В. Пазизин, Н.С. Погожин.— Москва : Горячая линия — Телеком, 2001.— 148с.

5. Мельников В.В. Безопасность информации в автоматизированных системах / В.В. Мельников— Москва : Финансы и статистика, 2003.— 368с

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ

Рыжов Павел Егорович, магистрант 2 курса кафедры математики и естественно научных дисциплин
Научный руководитель: **Вилисов Валерий Яковлевич**, д.э.н., к.т.н., профессор кафедры математики и естественнонаучных дисциплин

Статья посвящена проблемам безопасности в Интернете вещей. В материале рассматриваются основные виды проблем безопасности Интернета вещей, способы и практики защиты Интернета вещей. Автором были изучены успешные и актуальные практики защиты Интернета вещей и причины возникновения необходимости этих практик.

Интернет вещей, проблемы безопасности, контроль доступа.

SECURITY ISSUES IN THE INTERNET OF THINGS

Ryzhov Pavel, 2nd year graduate student of the Department of Mathematics and natural sciences
Scientific adviser: **Vilisov Valery**, Doctor of Economic sciences, Candidate of Technical sciences, Professor of the Department of Mathematics and natural sciences

The article is devoted to the problems of security on the Internet. In the material of the study of the main types of security problems of the Internet of things, practices and protection of the Internet of things. The author conducted successful and effective defense practices.

Internet of things, securuty issues, access control.

ВВЕДЕНИЕ

Интернет вещей - глобальная сеть компьютеров, датчиков и исполнительных устройств, связывающихся между собой с использованием интернет-протокола [1].

Широкое распространение систем под управлением Интернета вещей и характер передаваемых с его помощью данных сделали безопасность в данном вопросе важной проблемой.

Обеспечение безопасности в системах с использованием Интернета вещей на данный момент актуальный вопрос среди разработчиков. Последние убеждены в необходимости создания инструментальных средств разработки, снижающих стоимость внедрения компонентов безопасности в "умные" системы ещё на этапе разработки и проектирования.

Эксперты в области информационной безопасности высказывают мнение о том, что Интернет вещей должен отвечать требованиям безопасности систем критической инфраструктуры. Так, границы между устройствами для промышленных и домашних систем очень условные: одно и то же "умное" устройство (элементы освещения, различные датчики, электроприводы, аудиосистемы) может быть использовано как в домашних, так и в производственных условиях [2].

Согласно данному утверждению, рассмотрим основные виды безопасности в системах промышленного интернета вещей, т.е. системах, состоящих из производственных автоматизированных объектов и городских информационных инфраструктур.

1. Промышленный интернет вещей

Чтобы перейти к рассмотрению проблем безопасности Интернета вещей, обозначим системы, в рамках которых будет проводиться анализ.

Промышленный интернет вещей (англ. IIoT) является частью так называемой четвёртой промышленной революции, наряду с большими данными, виртуальной и дополненной реальностью, блокчейном и т.д.[2]

Промышленный интернет вещей является объединением передовых технологий автоматизации в единые системы. Если рассмотреть составляющие компоненты промышленного Интернета вещей, они будут схожи с аналогичными бытовыми системами. В IIoT на самом высоком уровне будут входить приложения и операционные системы, с помощью которых будет производиться взаимодействие с результатами работы системы и её мониторинг. Приложения и данные, собираемые с различных датчиков, будут являться частью "Облака" - цифровой частью Интернета вещей (рис.1) [2].

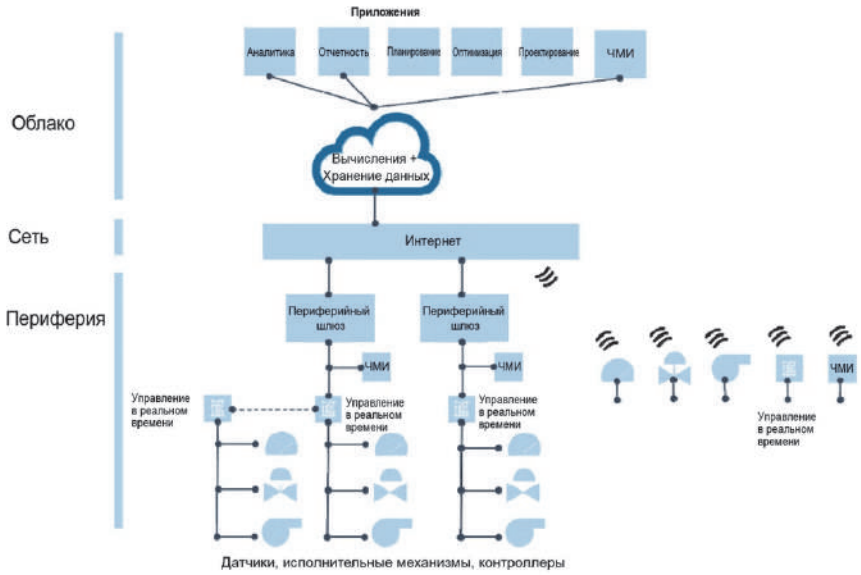


Рисунок 1 – Схематичное изображения промышленного Интернета вещей

На уровень ниже в системе находятся шлюзы, объединяющие отдельные узлы, состоящие из конечных устройств, человеко-машинного интерфейса (рабочие места операторов в случае, если речь идёт о производственном оборудовании). Каждый шлюз управляется в реальном времени, передавая данные в сеть по проводной и беспроводной связи

На самом нижнем уровне находятся узлы Интернета Вещей - исполнительные механизмы, датчики и контроллеры.

2. Виды проблем безопасности в интернете вещей

Далее рассмотрим основные виды проблем безопасности в контексте Интернета вещей.

Самая первая проблема в вопросе безопасности системы происходит на этапе *аутентификации*. В Интернете вещей этот процесс позволяет интегрировать различные устройства в систему. На данном этапе исполнительные устройства системы "регистрируются" в сети, проходят проверку безопасности и совместимости.

Одним из способов безопасной аутентификации является использования так называемых ключей - определённой байтовой последовательности, которая проходит проверку в системе для подключения устройства. Сложность заключается, в первую очередь, в том, что генерация и обмен ключами неизбежно приводит к увеличенному расходу ресурсов системы, что, в свою очередь, может сказаться на производительности и задержках в передачи данных. Если перед разработчиком стоит задача не увеличивать стоимость конечной системы, т.е. не увеличивать её вычислительные и передающие ресурсы, важно будет максимально оптимизировать процесс аутентификации [3].

Следующая проблема безопасности возникает в результате необходимости предоставления пользователя или узлам сети прав на выполнение определённых действий, то есть, *авторизации*. Механизмы контроля доступа в данном случае должны гарантировать право доступа в систему только авторизованным узлам.

Некоторые промышленные исполнительные устройства собирают личные данные. Например, если мы говорим про медицинское оборудование, это могут быть данные о состоянии здоровья. Сюда же могут входить видеозаписи с камер, отпечатки пальцев с идентификационных устройств и т.д.

Узлы Интернета вещей постоянно собирают и накапливают личные данные людей. Существующие механизмы обеспечивают сохранность конфиденциальной информации, хранящейся в системе, однако зачастую данные между узлами системы передаются в незащищённом или плохо защищённом виде, что может привести к утечке информации и несанкционированному доступу к ней третьих лиц.

Логическим завершением описанных выше проблем становится проблема *создания архитектуры безопасности,* которая отвечала бы

необходимым требованиям безопасности [3]. При разработке отдельных компонентов системы нужно учитывать нюансы безопасности всей системы в целом, внедрять элементы защиты, однако не все производители уделяют внимание данному вопросу.

Проблема заключается в том, что любая уязвимость базовых датчиков будет унаследована всей облачной средой системы. Таким образом, обнаружение и профилактика вредоносного трафика, просочившегося в сеть через уязвимые узлы сети - сложная и актуальная задача при проектировании архитектуры Интернета вещей.

3. Способы защиты интернета вещей

Важным принципом информационной безопасности является учёт. Для крупных систем первым и важным шагом к безопасности станет *каталогизация* всех компонентов: обслуживание крупной системы невозможно без подробного понимания её составляющих. При учёте всего "умного" оборудования на предприятии появляется возможность прогнозировать возможные утечки и иметь общее представление об уязвимости системы, что является актуальным для предприятий, где число умных устройств исчисляется тысячами.

Одним из логичных и простых подходов к обеспечению безопасности является *мониторинг трафика* подключаемых устройств. Таким образом, можно сразу выявить несанкционированные попытки доступа в систему извне, однако данный способ требует установки дополнительных накладных устройств в систему, что существенно может повысить стоимость системы и потенциально снизить производительность. Также стоит отметить, что данный способ мониторинга будет затруднителен в случае, если отдельные устройства в системе будут работать не напрямую с облачной сетью, а передавать информацию в отдельный шлюз Интернета вещей (рис.1).

Наконец, вероятной проблемой мониторинга трафика Интернета вещей является *шифрование* передаваемых данных, которое, с другой стороны, вводит дополнительный уровень защиты от утечки. Поскольку в большинстве случаев между "умными" устройствами и цифровой платформой нет промежуточных звеньев, безопасность может обеспечиваться только на уровне протокола передачи данных и усиленной аутентификации и идентификации устройства. Таким образом, безопасность должна обеспечиваться на уровне устройства, включая шифрование всех хранимых и передаваемых данных.

Более продвинутым способом защиты можно назвать *криптографическую идентификацию*. При наличии у каждого устройства уникального криптографического ключа, заложенного на аппаратном уровне в памяти, аутентификация компонентов сети становится более сложной, однако значительно усложняет несанкционированный доступ в систему. Так, например, для проникновения в сеть злоумышленнику будет уже недостаточно подменить MAC или IP адрес.

На *уровне разработчиков* систем Интернета вещей, говоря в общих чертах, необходимо обеспечивать такие меры безопасности, как:

использование только современных и продвинутых надёжных инструментов разработки;

сокращение количества элементов, необходимых для работы оборудования, т.к. снижая количество компонентов системы, мы повышаем её надёжность и безопасность;

обеспечение надёжной аутентификации, шифрования входных и выходных данных и тщательную проверку подлинности пользователей;

активное использование патч-менеджмента, то есть регулярного обновления программных компонентов для поддержания безопасности системы с учётом текущего состояния возможных уязвимостей.

Наконец, стоит отметить, что защита систем Интернета вещей зависит не только от разработчиков, но и от конечного пользователя. Важным способом защиты является защита на *уровне пользователя.* Немаловажно ввести некий процесс обучения пользователя безопасному обращению с информационной системой.

По возможности пользователю рекомендуется не предоставлять системе выход в глобальную сеть, используя её локально, где это возможно (например, пользователю нет нужды подключать в интернет-облаку умное освещение или бытовую технику, ведь они работают только в рамках квартиры или дома). Также немаловажно соблюдать базовые требования информационной безопасности по сохранности личных данных, то есть хранить данные для входа в сеть Интернета вещей в надёжном месте и не передавать их третьим лицам; не использовать незащищённое подключение; использовать надёжные пароли; не пренебрегать регулярным обновлением программных компонентов; не предоставлять доступ в сеть, особенно с полными правами доступа, непроверенным устройствам и пользователям.

4. Практики защиты устройств интернета вещей

Кибератаки систем Интернета вещей стали за последние несколько лет весьма актуальной проблемой. Об этом свидетельствует исследование аналитической компании Gartner, которое показывает кратный рост расходов на киберзащиту Интернета вещей. Так, с 2016 года сумма *увеличилась* более чем *в 3 раза* (рис.2)

	2016	2017	2018	2019	2020	2021
Endpoint Security	240	302	373	459	541	631
Gateway Security	102	138	186	251	327	415
Professional Services	570	734	946	1,221	1,589	2,071
Total	**912**	**1,174**	**1,506**	**1,931**	**2,457**	**3,118**

Рисунок 2 – Расходы на кибербезопасность для систем Интернета вещей (источник: Gartner)

Существующая проблема находит множество решений в лице крупных мировых компаний, среди которых есть весьма удачные практики киберзащиты.

Таким образом, например, существует практика защиты устройств, работающих через сотовые (GSM) сети. Специально для таких нужд были созданы так называемые выделенные беспроводные сети, Private LTE, предназначенные для решения исключительно технологических задач. Такие сети заранее проектируются с учётом всех требований к безопасности. Обычно под нужды производственной компании развёртывается персональная сотовая сеть, т.е. устанавливается отдельная передающая вышка и абонентское оборудование. Одним из производителей подобных сетей является международная компания Ericsson. Среди опыта развёртывания сетей есть успешные проекты, такие как Boliden - дистанционное управление машинами добычи и вентиляциями на одноимённой шахте, завод Mercedes-Benz в г. Зиндельфинген и другие [5].

Среди отечественных разработчиков стоит отметить Лабораторию Касперского. В 2020 году Лаборатория успешно интегрировала продукт "Kaspersky Automotive Adaptive Platform", автомобильную платформу на основе операционной системы KasperskyOS, в блок управления Ajunic. Высокопроизводительный модуль имеет возможность подключения к широкому спектру устройств и датчиков автомобиля, может быть использован для автономного управления и помощи водителю. Вкупе с интегрированной платформой от Лаборатории Касперского данное решение может быть использовано в качестве защищённой платформы для системы "умного" автотранспорта [4].

Из этих двух реальных практик защиты систем Интернета вещей видно, что, в действительности, крупные компании-поставщики компонентов Интернета вещей используют как защиту всех передаваемых данных в целом, используя отдельные хорошо защищённые сети, не имеющие внешний доступ, так и отдельную защиту на уровне компонентов, используя на блоках управления операционные системы, заведомо обладающие возможностями и решениями для поддержания безопасности. Таким образом, оба случая полностью вписываются в концепцию основных способов защиты Интернета вещей, описанных выше.

Заключение

При разработке и внедрении систем следует подходить к защите комплексно. Отдельно стоит отметить немаловажные шаги, такие как подход к устройствам системы с точки зрения их жизненного цикла (то есть от начала ввода в эксплуатацию, заканчивая снятием с поддержки), выделение устройств Интернета вещей в отдельный сегмент сети, а также внедрение сведений о моделях угроз в политику безопасности компании.

Безопасности стоит внедрять по принципу "снизу-вверх", то есть, учитывая отраслевую специфику, в том числе специфику используемых устройств и их жизненного цикла, а также требования к безопасности потребителей.

Литература

1. Росляков А.В., Ваняшин С.В., Гребешков А.Ю., Интернет вещей: Учебное пособие. - Самара: Приволжский Государственный Университет Телекоммуникаций и Информатики, 2015. - 136 с.

2. Андреев Ю.С., Третьяков С.Д. Промышленный интернет вещей: Учебное пособие. - Санкт-Петербург: Университет ИТМО, 2019. - 54 с.

3. Serpanos D., Wolf M. Internet of Things (IoT) Systems. Architectures, Algorithms, Methodologies. Springer International Publishing. 2018. pp. 37–54.

4. Gartner.com: веб-сайт, Электронный ресурс. Режим доступа: https://www.gartner.com/en/newsroom/press-releases/ (дата обращения: 20.01.2022).

5. Kaspersky Automotive Adaptive Platform: веб-сайт, Электронный ресурс. Режим доступа: https://os.kaspersky.ru/solutions/kaspersky-automotive-adaptive-platform/ (дата обращения: 24.01.2022).

6. Выделенные сети Ericsson: веб-сайт, Электронный ресурс. Режим доступа: https://www.ericsson.com/ru/about-us/company-facts/ericsson-worldwide/russia/private-lte (дата обращения: 21.01.2022).

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ХРАНИЛИЩ ДАННЫХ ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ НА ПЛАТФОРМЕ ANDROID

Рыков Алексей Юрьевич, магистрант 1 курса кафедры информационной безопасности
Научный руководитель: **Сухотерин Александр Иванович**, к.воен.н., доцент, доцент кафедры информационной безопасности

Вопрос информационной безопасности имеет ключевое значение в вопросе разработки программного обеспечения. Основной целью данной статьи является изучение вопроса информационной безопасности облачных хранилищ данных для устройств на платформе Android. Автором используются научные материалы зарубежного и отечественного авторства, а также применяются теоретические методы исследования. Преимущественная часть работы посвящена именно вопросу защиты информации в облачных хранилищах данных устройств на базе Android.

Информационная безопасность, информация, Android.

INFORMATION SECURITY OF CLOUD DATA STORAGE FOR MOBILE DEVICES ON THE ANDROID PLATFORM

Rykov Alexey, 1st year graduate student of the Department of Information security
Scientific adviser: **Sukhoterin Alexander**, Candidate of Military sciences, Associate professor of the Department of Information security

The issue of information security is of key importance in the issue of software development. The main purpose of this article is to study the issue of information security of cloud data storage for Android devices. The author uses scientific materials of foreign and domestic authorship, as well as applies theoretical research methods. The predominant part of the work is devoted specifically to the issue of information protection in the cloud data storage of Android devices.

Information security, information, Android.

Сегодня можно с уверенностью утверждать, что информационные технологии (ИТ) прочно вошли в жизнь человека. Основная цель информационных технологий заключается в повышении качества взаимодействия людей с информационной средой и в усовершенствовании автоматизированных производственных процессов на современных

предприятиях. Указанные выше технологии осуществляют свою работу на базе средств и методов сбора и обработки информации, а также передачи данных о состоянии процесса или исследуемого объекта. Процесс внедрения новых информационных технологий повсеместный и необратимый. На предприятиях происходит постоянное совершенствование ИТ и внедрение новых цифровых технологий. Эти процессы во многом определяют развитие экономики и общественной жизни государства в целом [1].

Свое широкое применение информационные технологии находят на производственных предприятиях и позволяют перевести деятельность человека в цифровой формат. Все это позволяет перейти от механического труда в любой сфере деятельности к использованию информационных технологий. Ряд преимуществ, присущих ИТ, обуславливает важность и целесообразность использования их на предприятии в деятельности технолога.

Следует отметить, что классифицировать информационные технологии на сегодняшний день можно с разных точек зрения. Сам термин «информация» имеет огромное количество значений и остается одним из самых обсуждаемых и изучаемых исследователями, несмотря на распространенность в современной деятельности человека.

Одним из основных направлений становления сегмента ИТ является мобильная разработка. На сегодняшний день существует множество платформ, программного обеспечения и иных инструментов, посредством которых разрабатываются и активно интегрируются в жизнь современного человека инновационные гаджеты. Так, к примеру, одной из наиболее популярных платформ, на базе которой разрабатываются мобильные устройства, является Android. В дополнение необходимо отметить, что в связи с непрерывно растущим потоком информации, факторы чего были указаны ранее в статье, формируется проблема хранения большого объема данных. Для решения данной проблемы в современных мобильных устройствах активно интегрируются различные облачные хранилища, позволяющие значительно экономить занимаемый объем памяти на физическом носителе [2].

Почти все процессы деятельности человека связаны с использованием информационных процессов и информации в том числе. С помощью информации осуществляется передача, хранение и обработка данных, выполняются транзакции и т.д. Исходя из проблемы обработки конфиденциальной информации и повсеместного доступа к ИТ, возникает необходимость защиты информации и информационных ресурсов в целом (рис. 1). Информация, представляющая собой ценность, может быть подвержена атакам хакеров и противозаконным действиям со стороны мошенников. Все это ведет к постоянному возрастанию опасности рисков в сфере мобильных разработок. В связи с этим информационная безопасность

становится ключевым направлением развития на сегодняшний день, что ведет к разработке новых способов и методов защиты информации?

В современном мире складывается тенденция роста количества попыток совершения преступлений на мобильных устройствах с помощью использования различных информационно-коммуникационных технологий. Множественные удачные попытки подобного рода преступлений свидетельствуют о том, что можно действительно нанести колоссальный как физический, так и информационный ущерб для современных устройств, имеющих недостаточный уровень защиты [3-4].

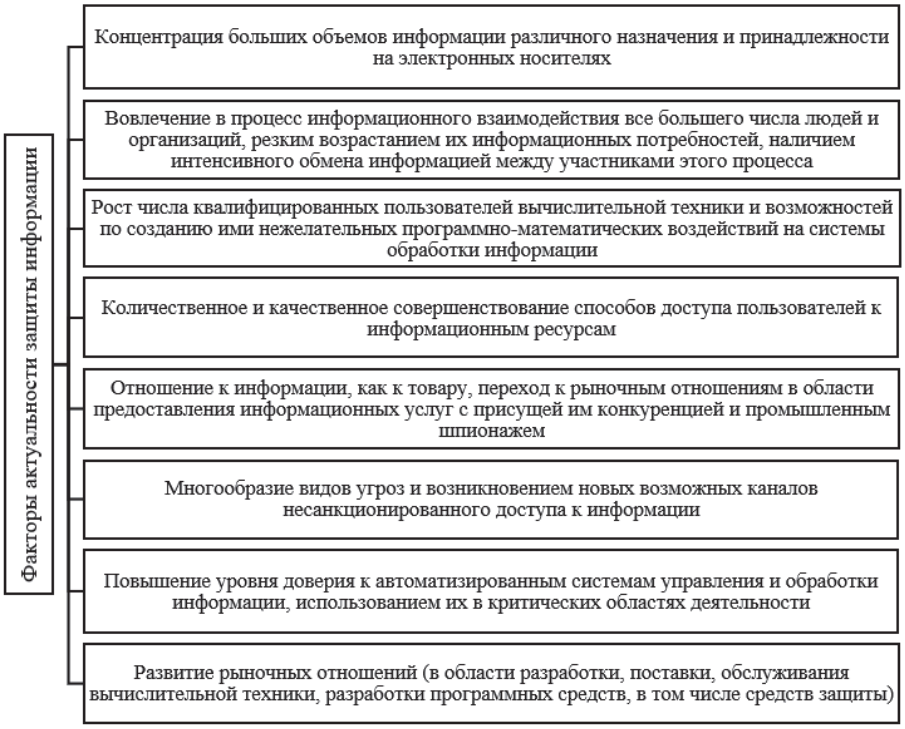


Рисунок 1 – Факторы, актуализирующие роль ИБ

Сейчас у злоумышленников широкое распространение находят вредоносное программное обеспечение, совместимое с операционной системой Android, и позволяющее получать конфиденциальную информацию с устройств и производить снятие денег с личных счетов пользователей. Эти вредоносные программы позволяют получать беспрепятственный доступ к любой информации, хранящейся в памяти мобильного телефона. Отсюда можно сделать вывод, что обеспечение информационной безопасности устройств, работающих на системе Android, является одной из наиболее важных задач на сегодняшний день. К основным требованиям обеспечения защиты устройства можно отнести использование современных методов защиты информации, быструю адаптацию к возникающим угрозам и опасностям в области безопасности и своевременное определение угрозы «нулевого дня» [5].

Среди способов проведения статического анализа можно выделить два основных способа. Первый – использование программного обеспечения ApkTool, с помощью которого становится возможным дизассемблирование программы, предположительно считающейся вредоносной или несущей угрозу безопасности устройства. Второй способ характеризуется использованием программы JD-GUI, позволяющим проводить анализ исходного кода. Произведя проверку на основе динамического и статического анализа, можно получить результат, указывающий на вредоносность программы. Кроме того, обеспечение и уровень информационной безопасности характеризуется также уровнем защищенности каналов передачи данных, через которые информация попадает в облачное хранилище. Снизить риск утечек и перекрыть канал передачи данных можно посредством специальных программных средств, таких как DLP-системы, способных защитить от хищения данных.

Решение задачи обеспечения безопасности информационных данных облачных хранилищ выходит на первый план и требует поиска и внедрения инновационных методов защиты, так как постоянно растет уровень угроз ИБ этих хранилищ. Однако, обеспечение ИБ требует больших финансовых вложений на свою реализацию. Проводя сравнение и соизмерение требуемых затрат на внедрение ИТ и обеспечение информационной безопасности с возможным ущербом от утечки конфиденциальной информации с предприятия, становится видна необходимость обеспечения максимального уровня защиты данных со стороны государства.

При обеспечении защиты информации на устройствах, осуществляющих работу на базе Android, важно использовать шифрование носителей этой информации. Всестороннюю защиту данных облачного хранилища в случае потри, конфискации устройства и др. может обеспечить полное шифрование диска. Доступ к данным, находящимся на зашифрованном устройстве для сотрудников специальных служб не так прост и сопряжен с рядом условий. К осложнению доступа к данным может привести простое разряжение батареи устройства или его отключение [6].

Одним из наиболее перспективных и актуальных инструментов обеспечения безопасности облачных хранилищ данных для мобильных устройств на базе Android является технология искусственного интеллекта (ИИ). Посредством интеллектуальных средств представляется возможность производить анализ большого объема данных с быстрой скоростью. Именно это и позволяет обнаруживать угрозы информационной безопасности и прогнозировать их в дальнейшем посредством самообучения модели ИИ и моделирования рисков в целом. На сегодняшний день существует ряд интеллектуальных решений применительно к безопасности облачных хранилищ. Также на сегодняшний день происходят активные разработки интеллектуальных решений из области ИБ, позволяющих в автоматическом режиме реагировать на атаки и управлять защитой.

Одним из решений создания эффективного модуля безопасности для защиты данных для мобильных устройств на базе Android является применение технологии искусственных нейронных сетей на основе программного комплекса Snort. Данный программный комплекс является перспективным сервисом, имеющим открытый код и распространяющийся под лицензией GPL. Snort предоставляет возможность настройки препроцессора и правил, направленных на повышение скорости работы системы. В результате чего детектор производит анализ поступивших данных, производя в пакетах поиск определенных правил или сигнатур, находящихся в базе.

Тип пакета можно определить путем использования специальной системы правил. Правила в свою очередь содержат определенный пакет параметров, через которые возможно определение текущей ситуации. Модуль безопасности для обнаружения атак с помощью данных инструментов характеризуется тем6 что модули определения отклонений в работе системы не расходуют слишком большого объема ресурсов и позволяют системе работать быстро (рис. 2). В случае возникновения подозрения на атаку, в работу вступает модуль определения типа атаки.

Рисунок 2 – Структура встраиваемой в «Snort» системы обнаружения и классификации сетевых атак

Для решения задачи обнаружения атак необходима разработка модуля, выполняющего посредством нейронных сетей анализа основных характеристик трафика. Посредством него представляется возможным достижение безопасного функционирования облачных хранилищ данных путем мониторинга и анализа на аномальность ключевых характеристик поступающего трафика. Схема системы обнаружения атак и аномалий с использованием нейронной сети на основе программного комплекса Snort имеет интегрированный в нее адаптивный нейронный модуль, работа которого выполняется в параллельном режиме общего функционирования системы. Посредством данной архитектуры можно обеспечить автоматизированный процесс обучения с учителем и обеспечить достаточно высокий уровень защиты информации в облачных хранилищах данных для мобильных устройств [7].

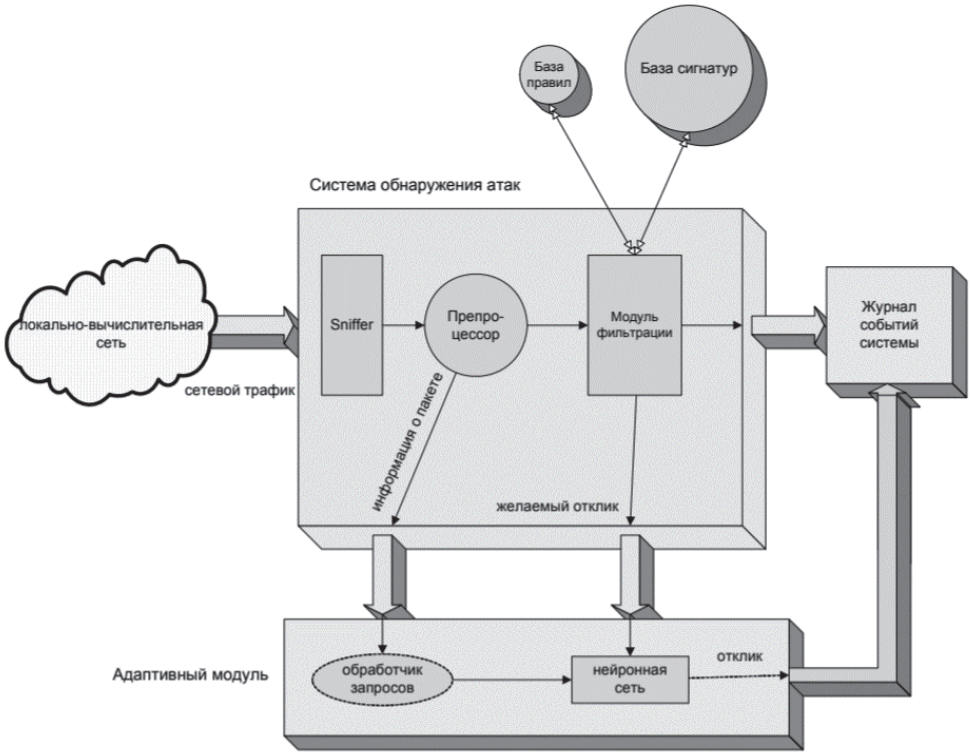


Рисунок 2 – Функциональная схема системы обнаружения атак с учетом работы интегрированного адаптивного модуля

Для получения требуемого отклика в результате анализа трафика выходной слой нейронной сети сформирован таким образом, что информация одновременно поступает на вход системы и линейной сервис-ориентированной архитектуры. Результат работы системы будет более эффективным, если она будет функционировать в двух режимах: раздельном, который используется при штатной работе адаптивного модуля отдельно от общей системы и совмещенном.

Он используется вначале запуска весов, которая обеспечивает проверку сходимости и работоспособности в период обучения. Параллельный режим работы обеспечивает одновременную корректировку весов и работу сервис-ориентированной архитектуры. Обучение завершается при превышении установленного порогового значения коэффициента ошибки.

Необходимо отметить, что при нахождении киберпреступником уязвимости в одном из компонентов мобильного устройства на платформе Android, представляется возможным осуществление целенаправленных нападений на другие объекты по всей стране или миру. Исходя из этого, особую актуальность приобретают задачи, решение которых направлено на своевременное обновление базовых компонентов систем управления и обеспечение должного уровня защиты информации в облачных сервисах хранения данных.

Также стоит отметить, что на сегодняшний день не только со стороны производителей, но и со стороны самих потребителей не всегда уделяется

необходимый уровень внимания вопросу информационной безопасности. Примерами являются пренебрежение создания сложного пароля, передача конфиденциальных данных в сообщениях и многое другое. Совокупность данных факторов приводит к развитию новых методов и угроз нарушения информационной безопасности, что особенно актуализирует проблематику представленного исследования [8-9].

Таким образом, основной целью данной работы являлось изучение вопроса информационной безопасности облачных хранилищ данных для мобильных устройств на платформе Android. В рамках представленной статьи были рассмотрены такие аспекты, как: взаимосвязь актуализации вопроса обеспечения информационной безопасности с повсеместным развитием информационных технологий; актуальность обеспечения информационной безопасности мобильных устройств на базе Android; возможные и инновационные пути решения проблемы защиты информации в мобильных облачных сервисах.

Можно сделать вывод, что одним из основных направлений совершенствования системы Android на данный момент можно выделить обеспечение безопасности. Сейчас, постоянно в технологиях идет борьба между разработчиками и злоумышленниками, в которой также важную роль играет и пользователь платформы Android. Можно в значительной степени обезопасить свое мобильное устройство, если не использовать сторонние сети выхода в Интернет, не устанавливать стороннее и подозрительное программное обеспечение, обновлять операционную систему своего телефона, а также настроить его на использование VPN [10].

В заключение необходимо отметить, что текущий уровень развития вопроса информационной безопасности облачных хранилищ данных для мобильных устройств на платформе Android является недостаточно разработанным. Исходя из этого, мобильные устройства могут быть подвержены множественным атакам со стороны киберпреступников и нанести колоссальный ущерб в экономическом аспекте. Таким образом, со стороны государства и разработчиков должно быть уделено намного большее внимание в сторону развития вопроса обеспечения информационной безопасности облачных хранилищ данных для мобильных устройств не только на базе Android, но и других.

Литература

1. Branding D.V. Cloud storage gateways for data protection in the organization // Actual problems of aviation and cosmonautics. 2018.
2. Kuleshova A.V., Kuzmin E.V. Influence of shadow cloud applications on organization security // ANI: Economics and Management. 2017.
3. Nesterenko V.R., Maslova M.A. Modern challenges and threats to information security of public cloud solutions and ways of working with them // Scientific result. Information technology. 2021.

4. Александров Я.А., Сафин Л.К., Трошина К.Н., Чернов А.В. Статический бинарный анализ мобильных приложений для платформы Android по требованиям информационной безопасности // Вестник Московского университета. 2016.

5. Баркалов Ю.М., Нестеров А.Д. Особенности обеспечения информационной безопасности в мобильных устройствах под управлением операционной системы Android // Вестник ДГТУ. Технические науки. 2019.

6. Гатиятуллин Т.Р. Меры безопасности для устройств под управлением Android os // Научный журнал. 2016.

7. Гришко И.С. Безопасность мобильных устройств на платформе Android // Вестник магистратуры. 2016.

8. Кучин И.Ю., Иксанов Ш.Ш., Белов С.В., Нургалиев М.М. Усовершенствование дискреционной модели доступа мобильных приложений к сервисам операционной системы Android // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. 2016.

9. Подколзина Л.А., Коваленко Д.К. Обеспечение безопасности мобильных облачных хранилищ на основе методов классификации данных // Молодой исследователь Дона. 2016.

10. Романов А.А., Панченко Е.А., Винокуров И.В. Разработка мобильного приложения для управления документами из облачных хранилищ // Символ науки. 2016.

АВТОМАТИЗАЦИЯ ПРОЦЕССА ОТСЛЕЖИВАНИЯ ЭТАПА ВЫПУСКА ПРИБОРА

Скворцов Владимир Сергеевич, Гусятинер Леонид Борисович,
магистранты 2 курса кафедры математики и естественнонаучных дисциплин
Научный руководитель: **Вилисов Валерий Яковлевич**, д.э.н., к.т.н.,
профессор кафедры математики и естественнонаучных дисциплин

В статье описана программа по отслеживанию этапа выпуска прибора. Представлены цель создания программы, описание процесса выпуска прибора до и после внедрения разработанной программы. Также приведены структура и описание рабочих окон программы, представлены варианты улучшения программы. Данная разработка планируется к применению на АО «НПО ИТ» для оптимизации процесса выпуска приборов, разрабатываемых отделом 211.

Автоматизация, программа, структура.

AUTOMATION OF THE PROCESS OF TRACKING THE RELEASE STAGE OF THE DEVICE

Skvortsov Vladimir, Gusyatiner Leonid, 2nd year graduate students of the Department of Mathematics and natural sciences
Scientific adviser: **Vilisov Valery**, Doctor of Economic sciences, Candidate of Technical sciences, Professor of the Department of Mathematics and natural sciences

The article describes a program for tracking the release stage of the device. The purpose of the program creation, description of the device release process before and after the implementation of the developed program are presented. The structure and description of the working windows of the program are also given, options for improving the program are presented. This development is planned to be used at NPO IT JSC to optimize the process of producing devices developed by the department 211.

Automation, program, structure.

1. Цель создания программы

В настоящее время на АО «НПО ИТ» при разработке конкретного прибора создается технологический паспорт, в который подшиваются:

1) список операций, проведенных над прибором во время его разработки;

2) документы задействованных комплектующих (датчики, блок питания, блок информационной обработки, корпус и разъемы);

3) отчет о проведённых предъявительских и приемосдаточных испытаниях;

В процессе разработки прибор перемещается между разными отделами:

– отдел, разработавший прибор (отдел 211, далее отдел разработки), где проводится его проверка функционирования и настройка;

– монтажный цех, где проводятся монтажные работы и упаковка готовых приборов; цех гальваники, где проводятся покрасочные работы.

При этом в разработке всегда находится более одного прибора. В связи с вышеуказанным повышается важность отслеживания и оперативного перемещения разрабатываемого прибора между отделами для проведения определённых этапов разработки, чтобы не допустить срыва сроков разработки прибора. Ранее указанный технологический паспорт не может решить данную проблему, так как неотрывно сопровождает прибор, поэтому и было разработано заявленное приложение.

2. Описание оптимизируемого процесса до и после внедрения программы

Для иллюстрации процесса выпуска прибора (от стадии закупки комплектующих деталей до стадии упаковки готового прибора) до внедрения программы представлена диаграмма AS-IS (рисунок 1).

На данной диаграмме представлены все три задействованных отдела и выполняемые ими операции в упрощенном виде. Синими стрелками обозначен процесс передачи результата выполнения операции. Красными стрелками обозначен процесс возврата испытуемого образца после проверки на функционирование в случае обнаружения дефекта в работе.

На диаграмме представлены следующие процессы [1]:

1) отдел разработки проводит закупку комплектующих деталей прибора – датчиков, платы для блоков питания и обработки информации. Данные комплектующие передаются в монтажный цех;

2) инженер монтажного цеха подготавливает к работе полученные комплектующие детали и соединяет их согласно схемам подключения без монтажа в корпус. Данная сборка передаётся в отдел разработки для проверки функционирования. Если проверка показала, что сборка неисправна, то сборка возвращается обратно инженеру для поиска и устранения неисправности;

3) инженер-испытатель отдела разработки проверяет функционирование полученной сборки в разных температурных условиях. Если проверка показала, что сборка функционирует исправно, то она отправляется обратно в монтажный цех для установки в корпус прибора. В случае выявления неисправности сборка возвращается в цех с целью устранения дефекта;

4) в случае успешной проверки сборки на функционирование инженер монтажного цеха осуществляет установку комплектующих деталей в корпус прибора, затем передаёт собранный прибор обратно в отдел разработки для проверки его функционирования. Если во время данной проверки выяснится, что прибор неисправен, его вернут для поиска и устранения дефекта;

5) инженер-испытатель отдела разработки проверяет функционирование полученного прибора в разных температурных условиях. Если проверка показала, что собранный прибор функционирует исправно, то далее он отправляется в цех гальваники для проведения работ по окрашиванию прибора. В случае, если проверка функционирования выявила наличие дефектов в работе прибор возвращают в монтажный цех;

6) маляр проводит покрасочные работы. затем окрашенный прибор передаётся в отдел разработки для проведения настройки работы прибора;

7) инженер-испытатель проводит настройку работы прибора, далее проводит, совместно с отделом технического контроля (далее – ОТК) и Представителем Заказчика предъявительские и приёмосдаточные испытания. В случае их успешного прохождения прибор отправляется на упаковку;

8) инженер монтажного цеха проводит подготовку к упаковке прибора (маркировка и пломбирование прибора), затем упаковщик упаковывает прибор в подготовленный кейс. После данной операции прибор готов к поставке.

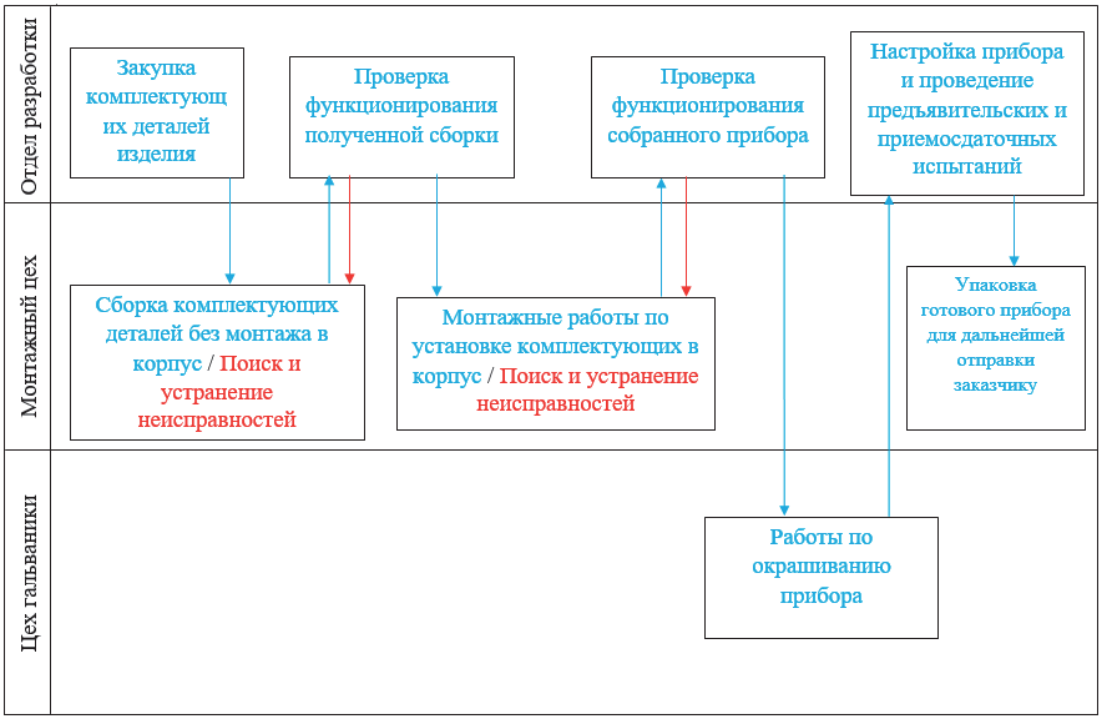


Рисунок 1 – Диаграмма AS-IS процесса выпуска прибора

Процесс выпуска прибора достаточно эффективен, поэтому достаточно оптимизировать контролирующий элемент, так как нельзя исключать

воздействие человеческого фактора, что может привести к срыву установленных сроков выпуска прибора.

Разработанная программа позволяет:

- начальнику отдела разработки в режиме реального времени отслеживать:

1) на каком этапе разработки находится конкретный прибор;

2) весь список операций, проведённых с прибором, с указанием точного времени и даты завершения операции и исполнителя;

- в случае отправки прибора на ремонт осуществить возврат к требуемой операции.

Процесс выпуска прибора после внедрения программы представлен на диаграмме TO-BE (рисунок 2).

На представленной диаграмме TO-BE зелёными стрелками обозначен удалённый контроль начальником отдела разработки через разработанное приложение. Остальные процессы остаются без изменений.

3. Описание программы

Программа представляет собой многооконное приложение с двумя режимами работы: инженер, начальник. Программа является многофайловым проектом (Рисунок 3), с графическим интерфейсом, где применяются библиотеки [2]:

1. PyQT 5 – фреймворк графической оболочки программы).
2. docx – работа с Word файлами.
3. sqlite3 – работа с базой данных SQLite.

Программа напрямую взаимодействует с базой данных, получая и вписывая всю требуемую информацию. Интерфейс позволяет с удобством производить требуемые операции с базой данных.

Приведём описание некоторых окон программы:

1. «Список завершённых операций» — окно вывода всех операций по прибору (рисунок 4.1);
2. «Окно создания нового прибора» — окно для регистрации нового прибора в базе данных (рисунок 4.2);

4. Предложения по улучшению

Для повышения функциональности проекта целесообразно добавить персонализированные аккаунты, возможность печати отчета в утверждённом формате, возможность отката операции.

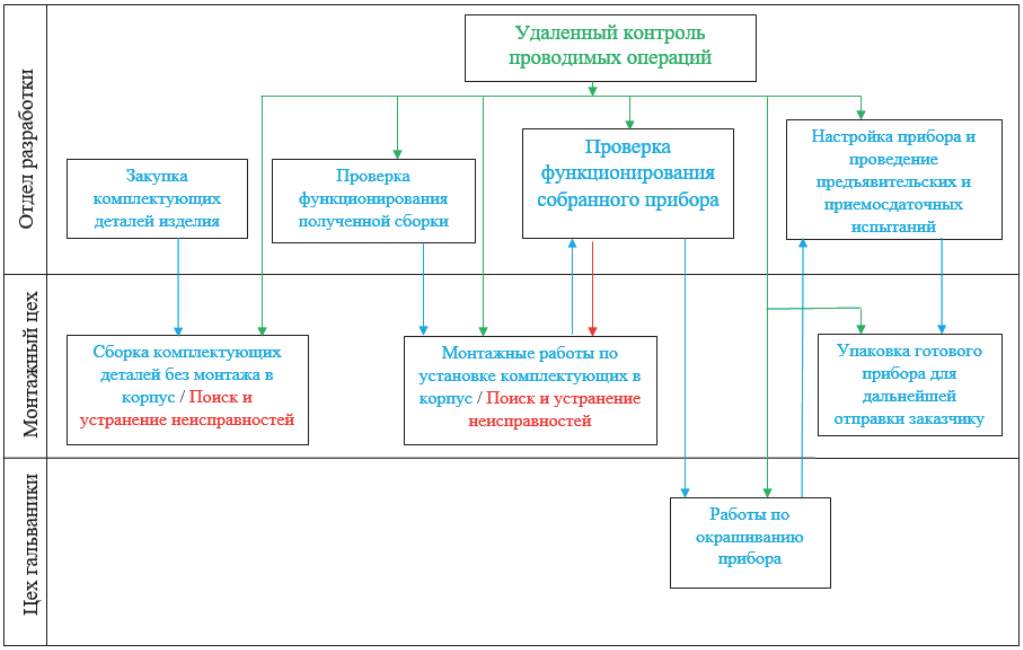


Рисунок 2 – Диаграмма TO-BE процесса выпуска прибора

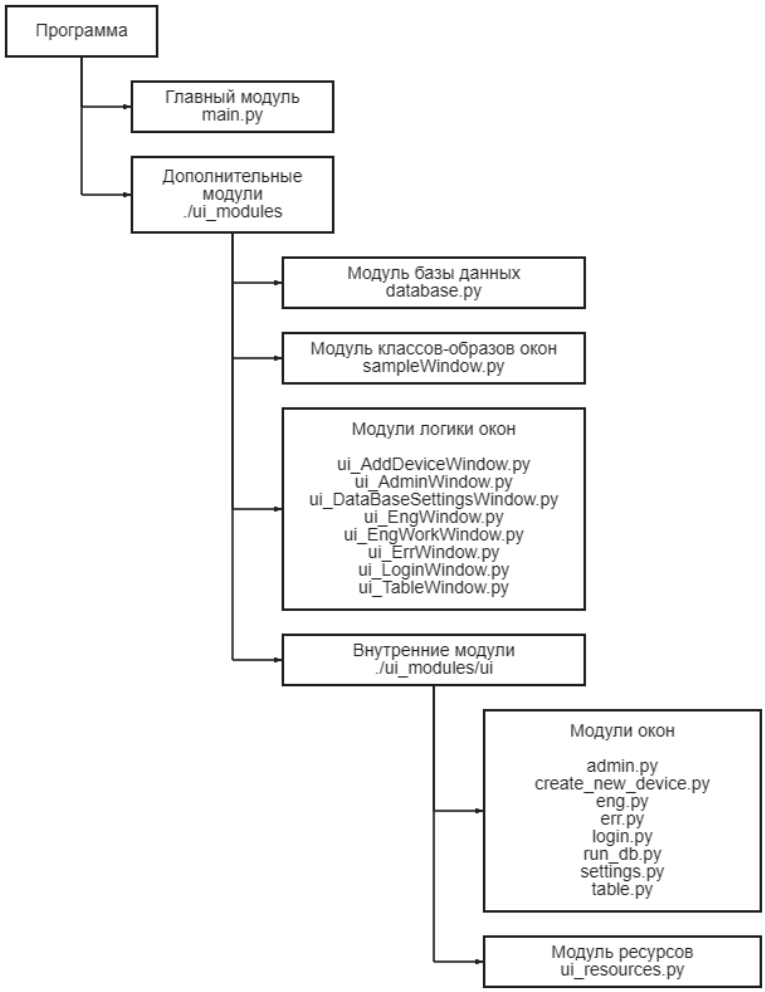


Рисунок 3 – Структура программы

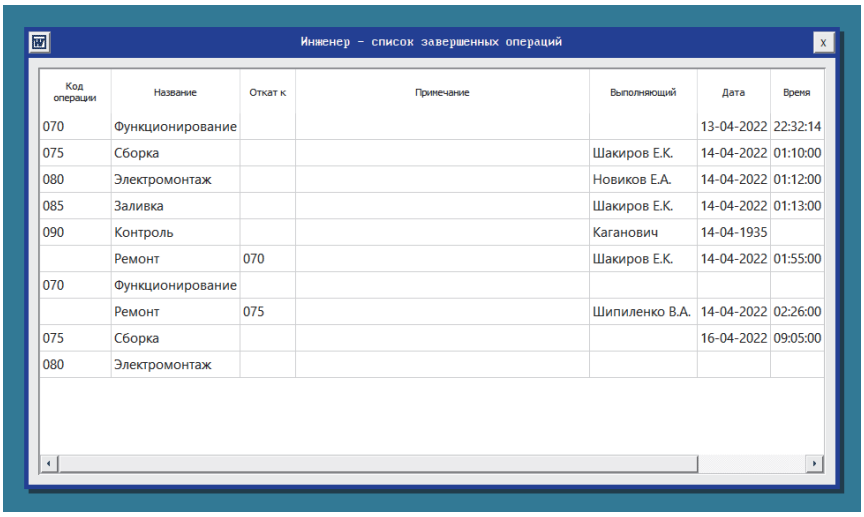


Рисунок 4.1 – Список завершенных операций

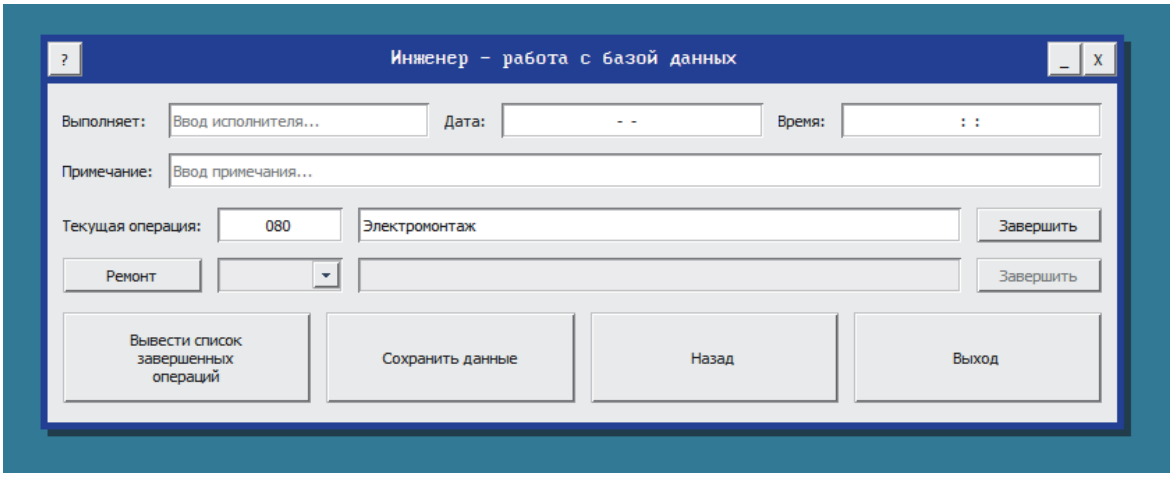


Рисунок 4.2 – Карточка операции

Литература

1. Инструкция на определительные испытания БЧЭ БЫ2.529.012 И18. Введ. с 01.01.2015. Королёв, 2015, 50с.

2. Шакиров Е. К. Проект «devices» [Электронный ресурс] Режим доступа: https://github.com/ego-rick/device.git (дата обращения 28.04.2022).

АКТУАЛЬНОСТЬ ВНЕДРЕНИЯ CRM-СИСТЕМ

Смирнов Роман Сергеевич, магистрант 2 курса кафедры информационных технологий и управляющих систем
Научный руководитель: **Логачева Надежда Вадимовна**, к.т.н., доцент кафедры информационных технологий и управляющих систем

CRM существенно влияет на эффективность процесса продаж. Это позволяет систематизировать контакты и базы данных для более слаженной работы с клиентами. Благодаря этому работа многих отделов в компании станет более эффективной, как было сказано ранее, но и более адекватной, простой и менее трудоемкой, а значит, и более дешевой.

CRM-система, IT индустрия, организация рабочего процесса, компания, клиенты.

RELEVANCE OF CRM-SYSTEMS IMPLEMENTATION

Smirnov Roman, Master, 2nd year graduate student of the Department of Information technologies and control systems
Scientific adviser: **Logacheva Nadezhda**, Candidate of Technical sciences, Associate professor of the Department of Information technologies and control systems

CRM significantly affects the efficiency of the sales process. This allows you to systematize contacts and databases for a more coordinated work with clients. Thanks to this, the work of many departments in the company will become more efficient, as mentioned earlier, but also more adequate, simpler and less labor-intensive, and therefore cheaper.

CRM-system, IT industry, workflow organization, company, clients.

Испокон веков люди путешествовали по миру. С самыми разными целями: командировки, поездки в гости или просто посмотреть мир. И, само собой, хотели, даже вдали от дома, иметь крышу над головой для безопасного ночлега и комфортного отдыха. Требования к месту ночлега у всех были различные и для каждого нужно было подобрать комфортные условия. Если одному достаточно было обычной крыши над головой, чтобы спрятаться от дождя, то другому, даже находясь на другом конце света от своего родного дома, не хочется отказываться от всего благо общества, которые были для него привычным делом. Столетия назад гостиничный бизнес уже зарождался в мире и, хоть ему еще не дали такое название, уже выполнял свою главную функцию, которая остается актуальна и по сей день.

Бум на строительство гостиниц в России начался в 20 веке, но даже век спустя эта сфера обслуживания остается одной из самых перспективных и прибыльных отраслей.

Сегодня для мирских задач предпочтение отдается технологиям, а не человеческому взаимодействию. Например, автоматическая регистрация в отелях происходит намного быстрее, чем в очереди на регистрацию сотрудниками стойки регистрации.

Мы живем в мире, где технологии стали неотъемлемой частью всей профессиональной и личной деятельности. Ожидания потребителей растут благодаря технологиям. В индустрии гостеприимства, где ожидания клиентов особенно высоки, технологии могут дать возможность для удовлетворения потребностей на высшем уровне. По этой причине решения, обеспечивающие персонализированное, эффективное и уникальное обслуживание клиентов, стало ключом к привлечению и удержанию гостей.

Отели внедряют автоматизацию, чтобы улучшить свою деятельность и революционизировать гостевой опыт. Технологии играют ключевую роль в обеспечении бесперебойного обслуживания клиентов: от бронирования номеров и работы стойки регистрации до обслуживания номеров, и выставления счетов. Автоматизация может преобразовывать неэффективные, независимые и отключенные процессы в интегрированные, автоматизированные и упрощенные рабочие процессы. Автоматизация повышает эффективность за счет оптимизации задач и повышения общего качества и надежности. Это также обеспечивает бесперебойное и эффективное комплексное пребывание клиентов.

Сегодня для мирских задач предпочтение отдается технологиям, а не человеческому взаимодействию. Например, автоматическая регистрация в отелях происходит намного быстрее, чем в очереди на регистрацию сотрудниками стойки регистрации. Поэтому отели все чаще вкладывают средства в необходимые технологии, чтобы гости могли удаленно регистрироваться и выезжать по своему усмотрению. Управление онлайн-бронированием – это функция автоматизации, которая позволяет клиентам бронировать номера по своему усмотрению в рамках дозволенной системы. Автоматизация устраняет необходимость в любом интерфейсе пользователя, а бронирование и отмена могут быть выполнены в любое время. Гости также могут пройти регистрацию заезда или выезда из отеля с помощью своих мобильных устройств или киоска на территории, что позволяет им не тратить время в очереди на стойке регистрации.

1.1 Определение CRM-системы

CRM– система, которая представляет собой веб или мобильный интерфейс, который дает конечному клиенту лично работать с ПО компании и самостоятельно выбирать услуги, тарифы и дополнительные сервисы, которые будут оказаны. Также отправлять и получать информацию. С помощью системы самообслуживания можно автоматизировать и улучшать

бизнес-процессы, в сферах продаж, маркетинга, обслуживание и поддержка клиентов. При помощи системы самообслуживания можно управлять взаимодействием разных отделов компании, которые взаимодействуют с клиентом. Также, система может передавать информацию о клиенте различным отделам внутри компании, для обеспечения наилучшего удовлетворения его.

Определение удовлетворенности и приверженности потребителей с помощью технологии самообслуживания и использования персональных услуг

Технология самообслуживания сегодня очень популярна в любой отрасли. Тем не менее, по-прежнему существует определенное неизвестное о SST и использовании персональных услуг в отношении его удовлетворенности потребителей и приверженности потребителей.

Система должна выполнять функции регистрации клиента, выбора номера, учет услуг, выбранных клиентом, и оплата в режиме самообслуживания. Также система должна обладать микросервисной архитектурой и возможностью расширения функционала. К примеру, такими возможностями, как - умная гостиница, бесключевой доступ к номеру и другие.

Система всегда находится под наблюдением администратора ИС на случай каких-либо неполадок в работе или вопросов от клиента, требующие вмешательства сотрудника.

В настоящее время на рынке появляется все больше компаний, предлагающих программы управления взаимоотношениями с клиентами, но не все из них обладают обширными функциями, таким образом, имея лишь ограниченные возможности работы.

Далее рассмотрим некоторые примеры существующих CRM-систем с описанным функционалом.

1.2 Готовые решения, представленные на рынке CRM-систем

1.2.1 Clock Hotel

Первая для рассмотрения система самообслуживания в отелях от компании Clock Software. Компания предлагает самостоятельную регистрацию клиента в гостинице с использованием web в три шага.

- Безопасная оплата.

Клиент переходит по ссылке, которая указывается в письме. Далее совершает защищенный перевод денежных средств через модуль оплаты. Тем самым автоматизированная электронная почта гарантирует клиенту бронирование номера.

- Выбор или назначение комнаты.

Клиент делает запрос на выбор понравившемуся ему номера или, по необходимым настройкам, комната назначается автоматически. Также клиент может выбрать дополнительные требования к своему заказу.

- Заполнение регистрационной карты и электронной подписи.

Карточки регистрации заполняются гостями еще до приезда, поэтому, когда они приезжают в гостиницу, остается только проверить правильность заполненных данных и подписать их на стойке регистрации. После чего гость получает ключ от номера. Либо гость может пройти этот процесс в киоске отеля.

Также система предлагает такие дополнительные возможности, как

- Запрос изменения периода, комнаты или гостей;
- Указание дополнительных пожеланий;
- Отмена бронирования;
- Организация трансфера;
- Возможность предупредить о скором визите.

1.2.2 Clock Terminal

Вторая система от той же компании Clock Software. Компания предлагает самостоятельную регистрацию клиента в гостинице через терминал самообслуживания, которая также является частью программы по взаимодействию с клиентами. Система подразумевает следующие шаги:

- Идентификация гостя

Для регистрации и заселения, клиенту нужно выбрать язык и пройти процесс аутентификации, путем подтверждения бронирования и PIN-кода, из сообщения, которое отправляется на устройство.

- Повышение категории номеров / специальные предложения

Отображение у гостя персонализированных предложений по повышению категории доступных номеров. Предложения автоматически синхронизуются с информацией о заполненности номеров и параметрами бронирования.

- Карточки электронной регистрации, политики и подпись

С помощью терминала самообслуживания клиент может изучить правила заезда и проживания в гостинице, внести свои персональные данные в карточке электронной регистрации и оставить на сенсорном экране терминала отпечаток своего пальца в качестве подписи.

- Работа с кредитными картами и выставление счетов

В терминале для самостоятельной регистрации клиент может совершать авансовые платежи, которые требуют предварительную авторизацию при оплате кредитной картой. Также клиенты, которые находятся в командировке, могут ввести информацию о компаниях, в которых они работают. Счета по оплате будут перенаправлены в них

- Получение магнитной карты

После заезду клиенту необходимо пройти процесс шифрования магнитной карты. Для этого ему нужно взять карту из коробки с картами рядом с терминалом и поднести ее к устройству для кодирования карт. После успешного шифрования клиент услышит звуковой сигнал от устройства.

1.2.3 POSitive CRM

Третья для рассмотрения система самообслуживания в отелях от

компании LSI Software, чья обширная система POSitive CRM значительно выделяется среди других решений. Помимо стандартных опций, т.е. получение и анализ всей информации о клиентах, как индивидуальных, так и групповых, возможность просмотра истории контактов с клиентами, их счетов и заказанных услуг, CRM, предлагаемая LSI Software, также предоставляет современные функции, значительно улучшающие продажи. и маркетинговой деятельности.

Благодаря интеграции с программным обеспечением для управления отелем, CRM-система автоматически загружает данные о доступных ресурсах отеля, ресторана или СПА, что позволяет быстро подготовить предложение для выбранных групп клиентов. В результате процесс продаж и предложений значительно сокращается, а благодаря анализу предпочтений клиентов предложения точно подстраиваются под конкретных гостей. Также значительно улучшен процесс бронирования номеров, конференц-залов, столиков в ресторане отеля и других гостиничных ресурсов, и услуг.

На основе собранных данных о гостях отеля, истории их пребывания в данном отеле, их предпочтениях, еде или услугах CRM также готовит программу лояльности, специально предназначенную для конкретных клиентов или организованных групп. Это позволяет обеспечить высокую персонализацию обслуживания для каждого клиента или группы при организации конференций, тренингов, банкетов или специальных мероприятий.

Программное обеспечение LSI, принимая во внимание, что большую часть доходов отелей составляет организация конференций, обучающие курсы имеют специально разработанные функции CRM, позволяющие, среди прочего, планировать и бронировать сервировку столов во время конференций, полное бронирование и учет кофе-брейков и мультимедийные средства, необходимые для обслуживания конференций. Среди прочего, благодаря таким удобствам отдел маркетинга отеля получает возможность предлагать клиентам услуги, более соответствующие их потребностям. Еще одним инновационным решением LSI Software является предварительный просмотр поставленных задач и степени их выполнения.

Руководитель данного отдела может наблюдать за процессом выполнения поставленных перед ним задач сотрудниками и степенью их выполнения. Таким образом, комплексная система POSitive CRM, разработанная LSI Software специально для гостиничной индустрии, является связующим звеном, соединяющим все отделы отеля - приемную, ресторан, СПА, маркетинг, продажи - она анализирует и координирует все действия, чтобы предоставить гостям услуги высочайшего качества.

Каковы преимущества POSitive CRM?

Благодаря накопленным знаниям о потребностях гостей, отдел маркетинга отеля, предлагая новые продукты и услуги, может значительно опередить конкурентов, которые, не имея ключевой информации от своих

клиентов, узнают о возможности предложения новых услуг, которые действительно интересуют гостей, только когда они появляются на рынке. Поэтому, благодаря быстрому и правильному анализу потребностей клиентов, гостиница будет восприниматься как выдающийся первопроходец на рынке новых услуг и продуктов, приобретая тем самым дополнительных клиентов. Кроме того, хорошая CRM-система, обеспечивающая укрепление долгосрочных отношений между отелем и его гостями, позволяет лучше понять актуальные потребности клиентов и их наилучшую реализацию. Благодаря этому заказчик, довольный надлежащим сервисом, не будет заинтересован в переходе на конкурентов и использовании их услуг, которые не будут располагать информацией о его потребностях. Здесь стоит упомянуть о значительном снижении затрат, которое обеспечивает правильно подобранная CRM-система, ведь ее эксплуатация в долгосрочной перспективе позволяет снизить затраты, направляемые на маркетинговые мероприятия, направленные на привлечение новых клиентов. Тем более что затраты на привлечение нового клиента даже в шесть раз выше, чем на поддержание существующего довольного клиента.

Суммируя бесчисленные возможности и преимущества, которые предоставляет современная и правильно настроенная CRM-система, а также наблюдая за мировыми тенденциями, кажется, что в ближайшие годы именно Управление взаимоотношениями с клиентами станет залогом успеха в гостиничном бизнесе. Внедрение CRM-систем очень актуально для эффективного развития бизнеса.

Литература

1. А. Кудинов, М. Сорокин, Е. Голышева. CRM. Практика эффективного бизнеса. Издательство 1С-Паблишинг 2021.

2. Боковой Ю. В. Особенности методологии проектирования информационных систем для малого и среднего бизнеса //Прикладная информатика. – 2006. – №. 5.

3. Е. Золина, И. Попова. Идеальный сервис. Как получить лояльность Клиентов. Год издания 2020.

4. Казакова А.Н., Файзуллина А.Г. Концепция CRM и CRM системы на предприятиях // Символ науки. 2019.

5. Калмакова Н.А., Подповетная Ю.В. Системные свойства динамического и экономического развития организации // Управление в современных системах. 2019.

6. Коцюба И. Ю., Чунаев А. В., Шиков А. Н. Основы проектирования информационных систем //Санкт-Петербург: Университет ИТМО. – 2015.

7. Кузнецов С. Д. Проектирование и разработка корпоративных информационных систем //М: Центр Информационных Технологий. – 1998.

8. Макаров Р. И., Мазанова В. И. Методические указания к

практическим занятиям по дисциплине «Проектирование информационных систем». – 2008.

9. Маклаков С.В. AllFusion и ERWin. CASE – средства разработки информационных систем. – М.: ДИАЛОГ – МИФИ, 2010. – 256с.

10. Рогозов Ю.И., Стукотий Л.Н., Свиридов А. С. Моделирование систем, ТРТУ, 2011. – 34с.

11. С. Ю. Золотов. Проектирование информационных систем: Учебное методическое пособие. – Томск: ТМЦДО, 2012 – 34с.

12. Яковлев В. П. Корпоративные информационные системы: конспект лекций //СПб.: СПбГТУРП. – 2015.

ПОСТРОЕНИЕ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ НА БАЗЕ ОРГАНИЗАЦИИ ОАО "РОССИЙСКИЕ ЖЕЛЕЗНЫЕ ДОРОГИ"

Соловьев Артём Сергеевич, магистрант 1 курса кафедры информационной безопасности
Научный руководитель: **Сухотерин Александр Иванович**, к.воен.н., доцент, доцент кафедры информационной безопасности

В России более 45% национальных грузовых перевозок и более 25% пассажирских перевозок приходится на железную дорогу, что делает ее основным видом транспорта в стране. Система управления информационной безопасностью (СУИБ) - это структурированный подход, используемый для лучшего управления наиболее важными данными и информацией вашей компании. Это может быть достигнуто путем принятия стандарта СУИБ, такого как ISO 27001 или российского стандарта ГОСТ, и посредством процесса сертификации. Но интеграция системы управления информационной безопасностью в вашей организации может быть сопряжена с проблемами и сложностями. Ниже мы описали пять проблем, которых вам следует избегать при создании своих СУИБ.

Железные дороги, инновационные технологии, информационная безопасность, управление информационной безопасностью.

BUILDING AN INFORMATION SECURITY MANAGEMENT SYSTEM BASED ON THE ORGANIZATION OF "RUSSIAN RAILWAYS"

Soloviev Artem, 1st year graduate student of the of the Department of Information security
Scientific adviser: **Sukhoterin Alexander**, Candidate of Military sciences, Associate professor of the Department of Information security

In Russia, more than 45% of national freight traffic and more than 25% of passenger traffic falls on the railway, which makes it the main mode of transport in the country. An Information Security Management System (ISMS) is a structured approach used to better manage your company's most important data and information. This can be achieved by adopting an ISMS standard, such as ISO 27001 or the Russian GOST standard, and through a certification process. But the integration of an information security management system in your organization can be fraught with problems and difficulties. Below we have described five problems that you should avoid when creating your ISMS.

Railways, innovative technologies, information security.

Введение

Термины "информационная безопасность", "компьютерная безопасность" и "информация", безусловно, ошибочно применяются как взаимозаменяемые. Хотя эти темы взаимосвязаны, и все они имеют общие цели защиты конфиденциальности информации, интеграции информации и доступности, но между ними есть тонкие различия.

В первую очередь, эти различия заключаются в подходе и темах, на которых сосредоточено внимание. По сути, информационная безопасность относится к конфиденциальности, целостности и доступности данных, независимо от формы информации, включая электронные, печатные их формы.

Компьютерная безопасность фокусируется на обеспечении доступности и надлежащего функционирования компьютерной системы, не заботясь об информации, которая сохраняется или обрабатывается компьютерной системой, правительство, военные ведомства, корпорации, финансовые учреждения, больницы и частные предприятия собирают большое количество конфиденциальной информации о клиентах сотрудников, продуктах, исследованиях и финансовом состоянии.

Большая часть этой информации уже находится на электронных компьютерах, собранных, обработанных, сохраненных и переданных по сети на другие компьютеры. Если конфиденциальная информация о клиентах и / или финансовых проблемах или финансовом продукте нового института будет получена по прибытии, утечка этой информации может привести к финансовым потерям для бизнеса, судебному преследованию и / или даже банкротству.

Защита конфиденциальной информации - это бизнес-потребность, а во многих случаях также моральная и юридическая необходимость. Для людей информационная безопасность оказывает значительное влияние на конфиденциальность. В последние годы информационная безопасность значительно повзрослела и эволюционировала. Есть много способов сделать карьеру в этой области.

Решения для повышения защиты

Существуют различные специализированные темы, такие как защита сетей и инфраструктур, защита практических приложений и баз данных, тестирование безопасности, аудит и проверка информационных систем, планирование продолжения бизнеса и проверка электронных штрафов и т.д. фактически информационная безопасность заключается в обеспечении безопасности информации и минимизации несанкционированного доступа к ней, а также в изучении методов защиты данных в компьютерной и коммуникационной системе от несанкционированного изменения. Информационная безопасность - это защита информации с точки зрения конфиденциальности, целостности и доступности.

Кроме того, другие функции, такие как подлинность, оперативность, достоверность (достоверность), неопровержимость, надежность информации, также могут включать этот вид защиты.

Организация безопасности, включающая в себя три основные функции, такие как:

- разработка политики информационной безопасности;
- разработка системы защищенного обмена информацией внутри организации;
- утверждение систем защиты от несанкционированного доступа, выбор средств криптографической защиты данных.

Вопрос о том, как организации может внедрить технически информационную безопасность:

1. Внедрить систему управления путем обучения сотрудников, повышения осведомленности, применения правильных мер безопасности и применения системного подхода к управлению информационной безопасностью. Риск, связанный с потерей информации или несанкционированным доступом, сводится к минимуму.
2. Повысить осведомленности и компетентности людей, назначенных на должности в области информационной безопасности. Повысить доверие клиентов, продемонстрировав, что компания сертифицирована по стандарту ГОСТ 34.602 и руководящим документам ФСТЭК России.
3. Организация соответствует нормативным требованиям, в том числе указанным в Регламенте по защите персональных данных (ГОСТ 34.602), ГОСТ Р 51583 и ГОСТ Р 51624.

Компании, как правило, трудно определить, какие данные являются наиболее важными и почему, потому что для этого требуются огромные усилия из многих различных областей внутри компании.

Например, не все важные данные хранятся внутри компании, поэтому вы должны выяснить, у кого есть к ним доступ. Более того, как только эта важная информация будет идентифицирована, компания должна определить, как создать надлежащие средства контроля, которые снизят или устранят риск того, что эти данные попадут в чужие руки.

Для того, чтобы система управления информационной безопасностью работала должным образом нужно создать культуру кибербезопасности сверху вниз. Руководители высшего звена должны посылать правильные сообщения об информационной безопасности, чтобы другие сотрудники относились к ней серьезно, и внутренние процессы обучения должны идти рука об руку с этим.

Наличие инструментов поведенческой аналитики может помочь вам определить, когда сотрудники используют данные вне рамок своей обычной деятельности, что может указывать либо на то, что сотрудник делает что-то сомнительное, либо на то, что его учетные данные были скомпрометированы.

Для ваших третьих лиц важно иметь доступ к вашим данным, который им необходим для выполнения своей работы. Но контроль за объемом конфиденциальных данных и доступом к сети, которые имеют ваши третьи стороны, имеет решающее значение для создания функциональной системы управления информационной безопасностью.

Набор стандартов для автоматизированных систем. Справочные условия создания автоматизированной системы"(далее - ГОСТ 34.602), ГОСТ Р 51583 и ГОСТ Р 51624. Класс безопасности информационной системы может быть пересмотрен, если объем информационной системы или важность информации в ней обрабатываются изменения.

Было проанализировано несколько информационных систем на российских железных дорогах, чтобы определить их класс безопасности.

В частности, были проанализированы следующие системы:

- Управление безопасности дорожного движения;
- Департамент цифровой технологической радиосвязи DMR;
- Система аудиосвязи и система видеоконференций.

На основании анализа информационных систем, существующих на Российских железных дорогах, и определения их класса безопасности можно сделать вывод, что основными элементами являются: рабочие станции, сервер, сетевое оборудование, оборудование для формирования каналов, параметры конфигурации системного и прикладного программного обеспечения, данные аутентификации пользователей и системных администраторов, диагностическая информация о состоянии отслеживаемых устройств.

Следующие параметры информационной безопасности были разработаны для обнаружения различных атак из сети. Было предложено использовать систему обнаружения вторжений Honeypot Manager 2.0. Эта система анализирует трафик как на компьютерах, так и на серверах и сертифицирована ФСТЭК. Для обнаружения локальных угроз рекомендуется использовать зонды во всех сегментах сети.

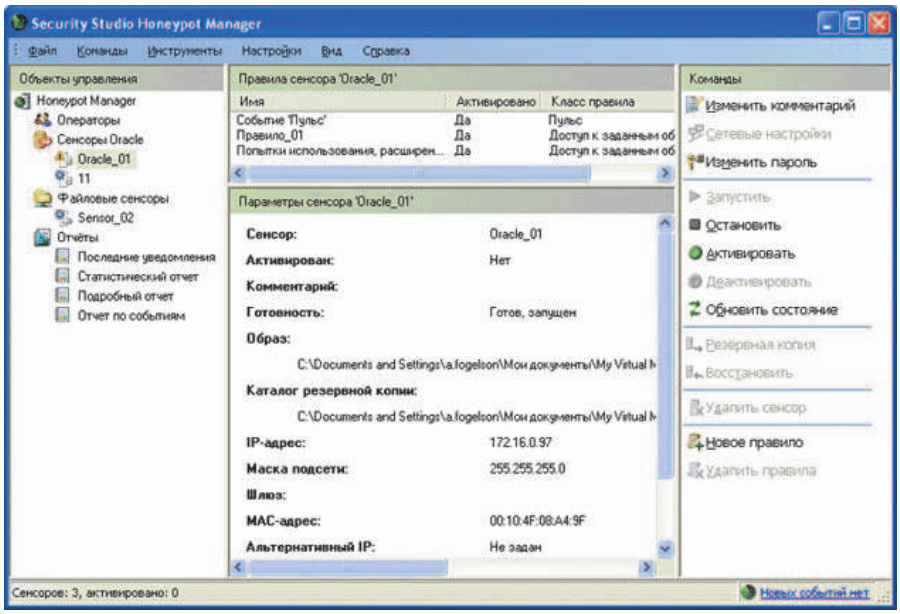


Рисунок 1 – Консоль Honeypot Manager

Для обмена с отличными компаниями и организациями предлагается использовать ViPNet Client 4.5, персональный дисплей и криптографический

провайдер для шифрования. Он также сертифицирован Федеральной службой безопасности. Для защиты компьютеров от вирусных атак необходимо установить антивирусное программное обеспечение. ESET NOD32 был выбран как лучший среди своих антивирусов, потому что он сертифицирован FSTEC, обнаруживает угрозы быстрее и эффективнее, чем другие, и относительно недорог, чтобы контролировать доступ к критическим ресурсам, необходимо использовать устройство безопасности, например, «МДЗ-Эшелон», АПМДЗ «КРИПТОН-ЗАМОК», Аккорд-АМДЗ или ПАК «СОБОЛЬ".

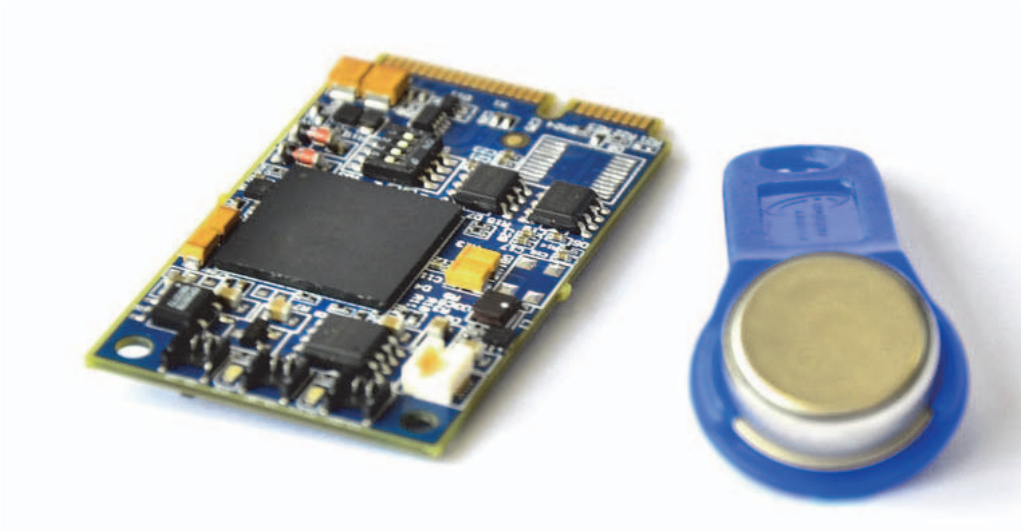


Рисунок 2 – Аккорд-АМДЗ

Эти меры безопасности необходимы для предотвращения несанкционированной загрузки компьютера пользователя, доступа к конфиденциальной информации и загрузки операционной системы.

МДЗ-Эшелон будет выбран в качестве аппаратной и программной защиты, так как вместе со своими коллегами он практически совместим с любой операционной системой и файловой системой, но является самым дешевым инструментом безопасности.

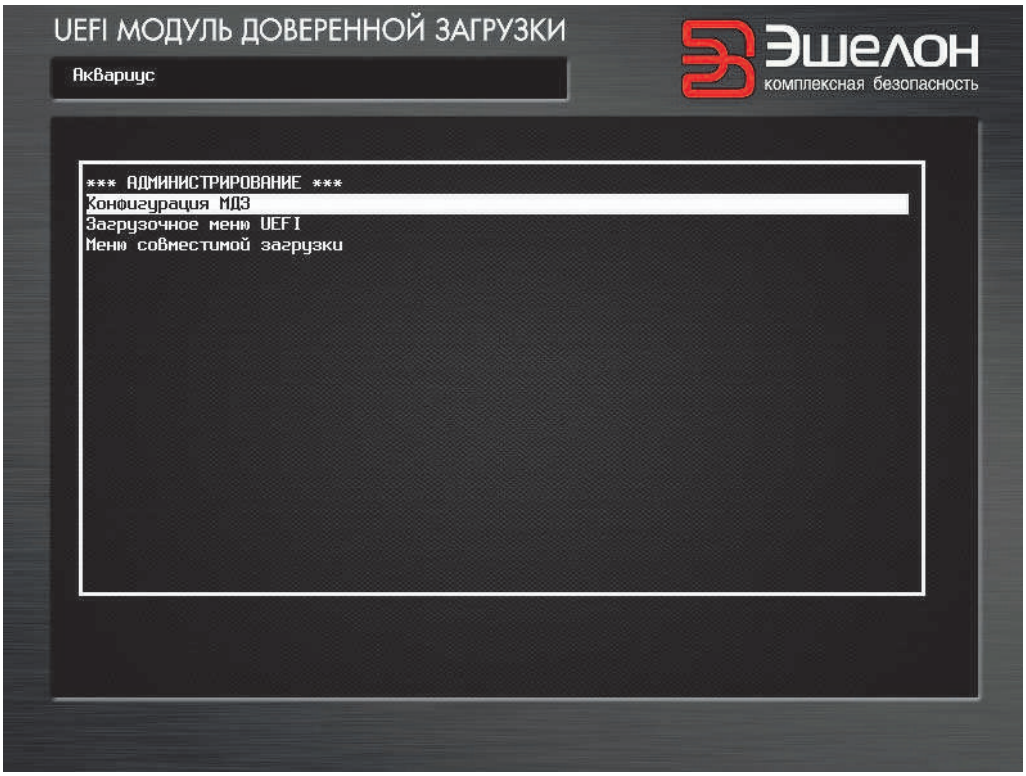


Рисунок 3 – МДЗ-Эшелон

В зависимости от принимаемого сетевого устройства, программного обеспечения и различных мер безопасности должна быть установлена базовая политика безопасности предприятия для всех пользователей и сетевых администраторов. Одной из основных предпосылок успешного процесса управления безопасностью информационной системы является использование определенной классификации угроз безопасности.

Таким образом, поскольку таким способом можно определить, от чего мы защищаем информационную систему, можно более эффективно использовать ограниченные ресурсы (например, время, деньги, сотрудников), инвестируя в эти средства защиты. которые имеют дело с самыми обычными угрозами и это в целом повысит уровень безопасности информационной системы, и, устраняя наиболее распространенные угрозы безопасности, будет доступно больше ресурсов для использования в других областях безопасности информационных систем.

Литература

1. R. Filipek. (2017). Information security becomes a business priority, Internal Auditor, Vol. 64 No. 1, p. 18.

2. H. Currangi. (2018). Managing Information Security Systems, Fifth Seminar on Academic Network of Western Asia, Faculty of Electrical Engineering Computer , Shahid Beheshti University

3. C. Shu-The. (2018). A study into the internationalization of national standards. Bureau of Standards, Metrology and Inspection, Ministry of Economic Affairs.

4. F B. Solms, R. Solms. (2011). Incremental information security certification, Computers and Security 20 (4), pp. 308 – 310.

5. A. Asadi Shali. (2015). Management of Information Security Systems, E- Journal of Information and Documentation Center of Iran, No. 4, Period 4

6. Information security operations planning and control program | NIST, (n.d.). Режим доступа: https://www.nist.gov/programs-projects/smart-manufacturingoperationsplanning-and-control-program

ТЕНДЕНЦИИ РАЗВИТИЯ СОВРЕМЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ АНАЛИЗА ТЕЛЕМЕТРИИ

Такташов Егор Дмитриевич, магистрант 1 курса кафедры информационных технологий и управляющих систем
Научный руководитель: **Исаева Галина Николаевна**, к.т.н., доцент кафедры информационных технологий и управляющих систем

В статье описаны системы первичного и вторичного анализа телеметрии космических аппаратов и ракет-носителей. Показаны возможные варианты улучшения систем анализа телеметрии с учетом их специфики на фоне быстрого развития современных систем и алгоритмов анализа данных.

Вычислительные системы, телеметрия, системы анализа, космический аппарат.

TRENDS IN THE DEVELOPMENT OF MODERN COMPUTING SYSTEMS FOR TELEMETRY ANALYSIS

Taktashov Egor, 1st year graduate student of the Department of Information technologies and control systems
Scientific adviser: **Isaeva Galina,** Candidate of Technical sciences, Associate professor of the Department of Information technologies and control systems

The article describes the systems of primary and secondary telemetry analysis of spacecraft and launch-vehicles. Possible options for improving telemetry analysis systems are shown, taking into account their specifics against the background of the rapid development of modern systems and data analysis algorithms.

Computing systems, telemetry, analysis systems, spacecraft.

Телеметрия, принимаемая с космического аппарата, является основным, а зачастую единственным источником информации о состоянии аппарата, его полезной нагрузки и, в случае пилотируемых аппаратов, состоянии экипажа. Таким образом, оперативный анализ телеметрии позволяет вести мониторинг сложных и требовательных к безопасности систем и, в частности, помочь избежать аварий на борту космических аппаратов.

В современных телеметрических системах передача данных осуществляется в цифровом виде. Выбор цифровой формы данных обусловлен сразу несколькими особенностями такой формы:

- Высокая помехоустойчивость передаваемого сигнала, обеспечиваемая использованием помехозащищенных кодов.
- Простота дальнейшей обработки и анализа телеметрической информации посредством ЭВМ.
- Возможность использования систем с адресным разделением каналов, вместо систем с временным или частотным разделением каналов.

В цифровых телеметрических системах данные с различных датчиков после прохождения АЦП (в случае если датчик является аналоговым), передаются на сумматор, где формируется телеметрический кадр для последующей передачи. В нем содержатся данные со всех датчиков, а также служебная информация, необходимая для декодирования кадра.

Также в современных телеметрических системах анализ информации принято разделять на два этапа [4]:

- Первичный анализ
- Вторичный анализ

На рисунке 1 представлена схема работы телеметрической системы при проведении первичного и вторичного анализов информации.

Первичный анализ

На этапе первичного анализа телеметрической информации основной задачей является приведение принятого сигнала в его изначальную форму. Для этого, прежде всего, необходимо выделить сигнал, что осуществляется автоматически посредством приемной аппаратуры.

После этого, с телеметрического кадра снимается помехоустойчивое кодирование, после чего проверяется его целостность. В случае, если телеметрический кадр поврежден и его восстановление невозможно, данные, закодированные в нем, пропускаются.

Если кадр цел или его удалось восстановить, начинается следующий этап первичного анализа, заключающийся в разбиении кадра на показания отдельных датчиков и их временной синхронизацией (в случае отечественных телеметрических систем, временная синхронизация осуществляется всегда с московским временем).

Все эти этапы осуществляются на приемной станции, что позволяет передавать для дальнейшего анализа сразу готовую к обработке информацию.

Помимо этого, во время первичного анализа также проводят восстановление утерянных данных и приводят данные в формат, удобный для дальнейшего анализа.

Для восстановления данных, используется множество алгоритмов: от самых простых – заполнение пропусков математическим ожиданием до более сложных. Применение того или иного метода восстановления зависит как от восстанавливаемого массива данных, так и от аппарата и стадии его эксплуатации. Однако, все эти методы можно разделить не две группы:

- Первая - подразумевает использование в качестве исходных данных для восстановления лишь параметров, принятых с борта аппарата до этого.
- Вторая группа, помимо использования ранее принятых данных в качестве исходных, при восстановлении пропусков использует так же данные, полученные при эксплуатации аналогичных аппаратов на аналогичных этапах эксплуатации при сходных условиях.

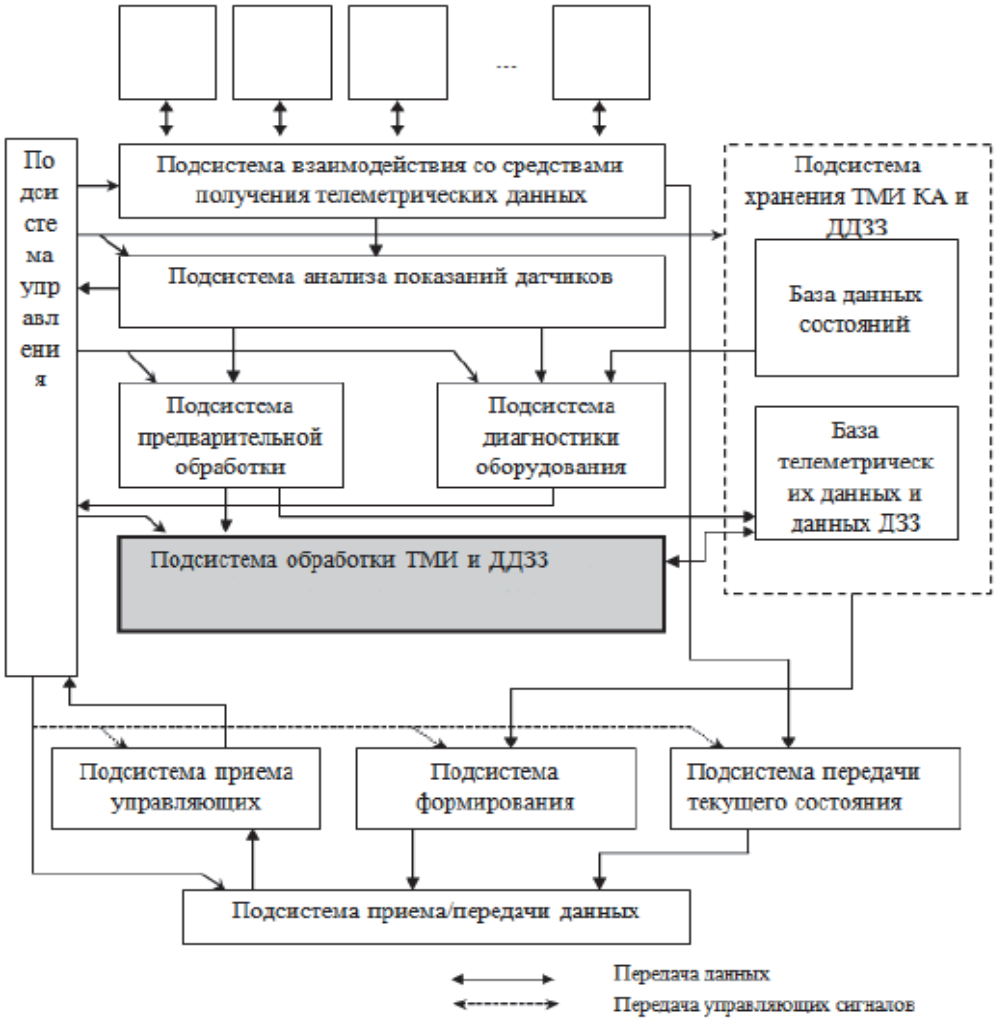


Рисунок 1 – Схема системы обработки телеметрической информации

Первая группа методов обладает меньшей точностью восстановления пропущенных данных, однако, при отсутствии данных, получаемых при эксплуатации аналогичных аппаратов в сходных условиях, методы этой группы являются единственными, способными восстановить утерянные в ходе передачи данные, пусть и не так точно. Методы этой группы, как правило, применяются при первичном анализе телеметрии аппаратов запускаемых впервые или, в случае, если запуск или эксплуатация аппарата происходят в новых условиях.

Вторая группа методов обладает значительно большей точностью восстановления данных, благодаря использованию в качестве исходных данных для анализа не только ранее принятой от аппарата телеметрии, но и архивов телеметрии аналогичных аппаратов, эксплуатируемых в схожих условиях. Методы этой группы, как правило, применяются при первичном анализе телеметрии серийных аппаратов, таких как ракеты-носители (при условии, что запуски производятся с одного и того же космодрома и в схожих погодных условиях) или телекоммуникационных спутников.

В последнее время все чаще при первичном анализе телеметрии применяются искусственные нейронные сети. Нейросеть можно отнести ко второй группе методов восстановления, ввиду необходимости настройки и обучения нейронной сети. Настройка нейронной сети в таком случае будет производиться на схожих исходных данных, наиболее правдоподобными из которых будут являться данные, полученные в ходе эксплуатации аналогичных аппаратов. Однако, в отличие от алгоритмов, относящихся ко второй группе методов восстановления, нейронные сети будут использовать данные предыдущих полетов только в период обучения и настройки, что способно повысить скорость восстановления данных в ходе первичной обработки телеметрии за счёт исключения обращений к базе данных с телеизмерениями предыдущих полетов.

Последним этапом первичного анализа является распределение поступившей телеметрии по потокам потребителей. Целью данного этапа является предоставление для дальнейшего вторичного анализа необходимых данных. Поэтому данные переводятся в наиболее удобный для дальнейшего анализа вид, и отправляются в соответствующие каналы связи.

Вторичный анализ

В отличие от первичного анализа, представляющего из себя определенную последовательность действий, производимых с данными телеизмерений, вторичный анализ является набором процедур, часть из которых выполняется параллельно друг другу в ходе эксплуатации аппарата, а часть из которых выполняется лишь при возникновении определённых условий. Под определенными условиями, как правило, понимаются нештатные ситуации, например, неисправность на борту аппарата или редкое астрономическое явление, требующее корректировки программы полёта орбитальной обсерватории. В целом, процедуры, входящие во вторичный анализ телеметрических данных, являются менее автоматическими, многие из них выполняются людьми, но с использованием различных программных средств, как для ускорения обработки информации, так и для выработки рекомендаций. Однако, существуют и полностью автоматизированные процедуры.

Процедуры вторичного анализа можно разделить по выполняемым ими задачам на:

- Процедуры прогнозирования

- Процедуры диагностирования
- Процедуры управления
- Процедуры архивации

Процедуры прогнозирования предназначены для построения моделей будущего состояния системы или ее частей с целью обнаружения возможных проблем до возникновения критических неисправностей, а также с целью выработки исходных данных для управляющих воздействий.

Процедуры диагностирования предназначены для сравнения текущего состояния космического аппарата с его моделью. Сравнение состояния аппарата и его модели производится с учетом предыдущих измерений, полученных в ходе полета. Основной целью процедур диагностирования является выявление неисправностей путем сравнения исправной модели системы с состоянием рабочий модели.

Процедуры архивации необходимы для сохранения телеметрической информации, полученной в процессе полета. Данная информация необходима как для расчетов, производимых непосредственно в процессе полета аппарата, так и в случае расследования аварии.

Основной задачей процедур управления является выработка реакции, как на внутренние изменения системы космического аппарата, так и на изменения внешних условий. К внутренним изменениям можно, например, отнести динамику расхода топлива ступенью ракеты-носителя, что в свою очередь влияет на ее баллистические характеристики [1, 2]. При рассмотрении в качестве телеметрируемого объекта ракеты носителя, внешними факторами, влияющими на объект, будут погодные условия: например, сила и направление движения воздушных масс в низких слоях атмосферы. В таком случае процедура управления по данным акселерометров и гироскопов, а также по данным метеослужбы космодрома, будет вырабатывать управляющее воздействие для противодействия потоку воздуха, что в случае ракеты-носителя будет проявляться как включение или изменение мощности газовых рулей.

Методы вторичного анализа можно разделить на две группы по их математической реализации [3]:

- Детерминированные
- Статистические

К детерминированным методам относят методы, в которых есть однозначная связь между измеряемым параметром и определяемой характеристикой или параметром состояния. Основным преимуществом детерминированных методов является их простота и, как следствие, малое время необходимое на обработку. Главными недостатками детерминированных методов являются невозможность повышения точности измерений, а также необходимость построения полностью нового алгоритма, при изменении набора анализируемых параметров, что снижает степень унификации.

Статистические методы подразумевают избыточность измерений. На основе статистических методов возможно построение как рекуррентных алгоритмов, то есть алгоритмов, обрабатывающих информацию по мере ее поступления, так и разовых, то есть алгоритмов, работающих с определенным объемом данных, накапливаемым в определённые промежутки времени. Главным достоинством статистических методов является их точность, значительно превышающая точность детерминированных методов, а также отсутствие необходимости полного изменения алгоритма анализа в случае изменения набора анализируемых параметров. Главным недостатком статистических методов является значительно больший объем вычислений.

Выводы: В настоящее время, с ростом вычислительных мощностей становится возможным массовое применение искусственных нейронных сетей, как при первичном, так и при вторичном анализе телеметрии. При первичном анализе использование нейронных сетей уже сейчас позволяет значительно повысить точность восстанавливаемых данных при несколько большем, затрачиваемом на анализ времени.

Использование нейронных сетей при вторичном анализе обладает всеми преимуществами статистических методов анализа и при этом лишено их главного недостатка - сравнительно большого объема вычислений [4].

Особую значимость системы телеметрии имеют для критичных к безопасности сложных систем, таких как космические аппараты.

Литература

1. Лысенко Л.Н., Соловьев В.А., Любинский В.Е. Управление космическими полетами. МГТУ им. Н.Э. Баумана, 2009.

2. Майорова В. И., Гришко Д. А., Ремень Б. А., Амбарцумов А. А., Калдаров И. С. Автоматизация приема и обработки резервной телеметрической информации с космических аппаратов// Научная электронная библиотека «Киберленинка» [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/avtomatizatsiya-priema-i-obrabotki-rezervnoy-telemetricheskoy-informatsii-s-kosmicheskih-apparatov (дата обращения: 29.04.2022).

3. Назаров А.В., Козырев Г.И., Шитов И.В. Современная телеметрия в теории и на практике: Наука и техника, 2007.

4. Сатыбалдиев А. А, Таштай Е. Т. Анализ практического применения нейросжатия для телеметрических задач космического назначения// Научная электронная библиотека «Киберленинка» [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/analiz-prakticheskogo-primeneniya-neyroszhatiya-dlya-telemetricheskih-zadach-kosmicheskogo-naznacheniya (дата обращения: 29.04.2022).

ОЦЕНКА ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ ОБОРОТНОГО КАПИТАЛА, ЛИКВИДНОСТИ И ПЛАТЕЖЕСПОСОБНОСТИ ООО «ПОЛИКОМ»

Хаярова Виктория Эльдаровна, магистрант 2 курса кафедры управления качеством и стандартизации
Научный руководитель: **Овсийчук Вадим Ярославович,** д.э.н., профессор кафедры финансов и бухгалтерского учета

В статье проведена оценка эффективности оборотных средств на примере предприятия ООО «Поликом», а также анализ ликвидности и платежеспособности компании. Анализ проводился с помощью финансовых коэффициентов и использованием числовых данных бухгалтерской отчетности исследуемого предприятия. По результатам проведенных расчетов были сформулированы соответствующие выводы.

Оборотные активы, ликвидность, платежеспособность, оборачиваемость, финансовые коэффициенты.

EVALUATION OF THE EFFICIENCY OF WORKING CAPITAL, LIQUIDITY AND SOLVENCY OF LLC «POLIKOM»

Khayarova Victoria, 2nd year graduate student of the Department of Quality management and standardization
Scientific adviser: **Ovsiychuk Vadim**, Doctor of Economic sciences, Professor of the Department of Finance and accounting

The article evaluates the efficiency of working capital on the example of the company LLC "Polycom", as well as the analysis of the liquidity and solvency of the company. The analysis was carried out using financial coefficients and using numerical data of the accounting statements of the investigated enterprise. According to the results of the calculations, the relevant conclusions were formulated.

Current assets, liquidity, solvency, turnover, financial ratios.

Для характеристики деятельности предприятия, эффективности ее работы, составлении планов и прогнозов, бюджетов, важно оценивать финансовое положение предприятия, а также не менее важные показатели, такие как рентабельность и ликвидность предприятия. При расчете данных показателей зачастую используются величины составных элементов оборотного капитала.

Оборотные средства занимают значительную часть всего капитала организации, поэтому от их состояния, грамотной организации управления оборотным капиталом, в который входят запасы, дебиторская задолженность и денежные средства, зависит эффективность их использования и финансовое состояние предприятия в целом. Благодаря такой эффективности есть возможность высвобождения средств из оборота и начать инвестировать в финансово-хозяйственную деятельность без привлечения сторонних финансовых ресурсов, например, займов или кредитов.

Целью данной статьи является проведение оценки эффективности использования оборотного капитала исследуемого предприятия с помощью финансовых коэффициентов, анализ его финансового состояния.

Анализ оборотного капитала предприятия можно проводить как в целом, так и по конкретным его составляющим или группам. Для данного процесса применяют различные финансовые показатели, в том числе характеризующие оборачиваемость оборотных средств и его отдельных элементов.

Оборотные средства за определенный промежуток времени совершают некоторое количество оборотов, такой процесс характеризует коэффициент оборачиваемости, который показывает, на сколько интенсивно используются оборотные средства в организации и как тем самым увеличивается их доходность. Увеличение данного показателя означает положительную тенденцию эффективности использования оборотного капитала, т.е. для ведения операционной деятельности предприятия понадобится меньше средств.

Коэффициент загрузки или показатель закрепления оборотных средств показывает, сколько оборотных средств приходится на 1 руб. реализованной продукции. И чем он меньше, тем эффективнее используются оборотные средства. [4, с.252]

Оборачиваемость можно определить не только количеством оборотов, но и периодом, за которые эти обороты совершаются. Для этого существует показатель длительности одного оборота оборотных средств. Он определяется средним сроком, в который вложенные денежные средства в финансово-хозяйственные операции компании возвращаются обратно в организацию.

Проведем анализ эффективности использования оборотного капитала ООО «Поликом» за 2020-2021 годы на основании исходных данных, представленных в бухгалтерской отчетности анализируемого предприятия (таблица 1).

Таблица 1 – Исходные данные для анализа оборачиваемости оборотных средств ООО «Поликом» за 2020-2021 гг., тыс. руб.

№ п/п	Наименование показателя	2020	2021
1	Выручка	1297303	2360667
2	Себестоимость продаж	1 142 060	2 106 408
3	Оборотные активы	548300	596003
4	Запасы	293210	345390
5	Дебиторская задолженность	182403	222134

В таблице 2 отображены результаты анализа оборачиваемости оборотных средств, а также динамика их показателей.

Таблица 2 – Анализ оборачиваемости оборотных средств ООО «ПОЛИКОМ» за 2020-2021 годы

№ п/п	Показатель	Методика расчета	2020	2021	Изменение (+,-)
1	Коэффициент оборачиваемости оборотных средств	$Коб = \frac{Вп}{Со}$	2,351	4,126	1,775
2	Коэффициент закрепления оборотных средств	$Кз = \frac{Со}{Вп}$	0,103	0,24	0,137
3	Продолжительность одного оборота, дни	$Од = \frac{Со*Д}{Вп}$	153,1	87,25	-65,85
4	Коэффициент оборачиваемости дебиторской задолженности	$Кодз = \frac{Вп}{ДЗср}$	6,81	11,67	4,86
5	Период оборота дебиторской задолженности, дни	$Одз = \frac{Д}{Кодз}$	53,6	31,28	-22,32
6	Коэффициент оборачиваемости запасов	$Коз = \frac{СРП}{Зср}$	4,54	6,6	2,06
7	Период оборота запасов, дни	$Оз = \frac{Д}{Коз}$	80,4	55,3	-25,1

Анализ оборачиваемости показал, что на предприятии выросла эффективность использования оборотного капитала за счет следующих моментов:

1) в 2021 году увеличился коэффициент оборачиваемости, что говорит о быстрой оборачиваемости капитала и то, что каждый рубль актива приносит больше прибыли;

2) снижение длительности одного оборота оборотных средств характеризуется интенсивностью использования оборотного капитала. В 2021 году показатель сократился на 66 дней.

3) наблюдается увеличение коэффициента оборачиваемости

дебиторской задолженности, при этом период оборачиваемости сокращается, это говорит о выборе эффективной стратегии развития и экономической стабильности предприятия;

4) увеличение коэффициента оборачиваемости запасов вызвано ростом объема продаж организации. Сокращение периода одного оборота запасов говорит об эффективном контроле процесса формирования и использования запасов.

В то же время коэффициент загрузки показали, что в 2021 году на 1 руб. реализованной продукции затрачено 24 копейки оборотных средств, а в 2020 году – 10 копеек. В 2021 году оборотные средства компании использовались менее эффективно по сравнению с 2020 годом. Это говорит об увеличении трат оборотных средств для получения 1 руб. реализованной продукции.

Для оценки успешной деятельности компании также необходимо проанализировать показатели рентабельности, в данном случае рентабельность оборотного капитала. При его расчете используются данные полученной прибыли от реализации продукции и среднегодовой стоимости оборотных средств. С помощью показателя можно понять, сколько приходится прибыли до налогообложения на вложенный в оборотные активы один рубль денежных средств. Эффективность использования оборотных средств будет характеризоваться повышением этого коэффициента. [2, с.108]

Формула расчета рентабельности оборотного капитала имеет вид:

$$\mathbf{Р} = \frac{\text{Пп}}{\text{Со}}, \quad \textbf{(1)}$$

где Р – рентабельность оборотного капитала, Пп – прибыль от продаж продукции.

Проанализируем рентабельность оборотного капитала за 2020 и 2021 годы.

2021: Р = 84203/572151,5 = 0,15

2020: Р = 58017/551734 = 0,11

Анализ рентабельности оборотного капитала показал, что в 2021 году на 1 рубль средств, затраченных в оборотные активы, приходилось 15 копеек прибыли, что на 4 копейки больше по сравнению с 2020 годом.

Высвобождение средств из оборота происходит в результате ускорения оборачиваемости, и наоборот, при ее замедлении необходимо вложение дополнительных средств в хозяйственную деятельность.

Высвобождение оборотных средств определяется по формуле:

$$\mathbf{Эо} = \frac{\text{Врп} * (\text{Об} - \text{Оп})}{360}, \quad \textbf{(2)}$$

где Эо — экономия оборотных средств; Оп — длительность одного оборота в плановом периоде; Об — длительность одного оборота в базисном периоде; Врп — выручка от реализации в плановом периоде. [2, с.108]

Получим следующие значения показателя:

2021: Эо = 2360667 * (87,25-153,1)/360 = -431805,33

2020: Эо = 1297303*(153,1 – 147,5)/360 = 20180,27

Исходя из полученных результатов видно, что в 2021 году произошло высвобождение оборотных средств на 431805,33 руб., об этом свидетельствует полученное значение со знаком «-». В 2020 году были задействованы дополнительные средства на сумму 20180,27 руб. Таким образом, в 2021 году высвобождение оборотных средств характеризует ускорение оборачиваемости, т.е. эффективности деятельности предприятия.

Для обеспечения непрерывности своей производственной и финансовой деятельности организации необходим достаточный объем капитала, но в то же время компания должна вовремя и полностью погашать свои обязательства перед кредиторами, бюджетом, персоналом, поставщиками и прочими третьими лицами, чтобы считать свое финансовое состояние устойчивым. [1, с. 207]

Сможет ли предприятие покрыть свои финансовые обязательства за счет текущих активов или нет, можно определить с помощью расчета коэффициентов ликвидности.

Анализ ликвидности проведем с помощью следующих показателей: коэффициентов абсолютной ликвидности, текущей ликвидности и быстрой ликвидности (таблица 3).

В ходе анализа установлено, что результаты коэффициентов находятся в пределах нормативных значений. Во многих источниках значение коэффициента абсолютной ликвидности, равному 0.1, находится в пределах нормы данного показателя. Таким образом полученные данные свидетельствуют о том, что компания ООО «Поликом» имеет достаточно ликвидных оборотных средств для своевременного расчета по своим обязательствам. Динамику изменения показателей можно наглядно увидеть на рисунке 1.

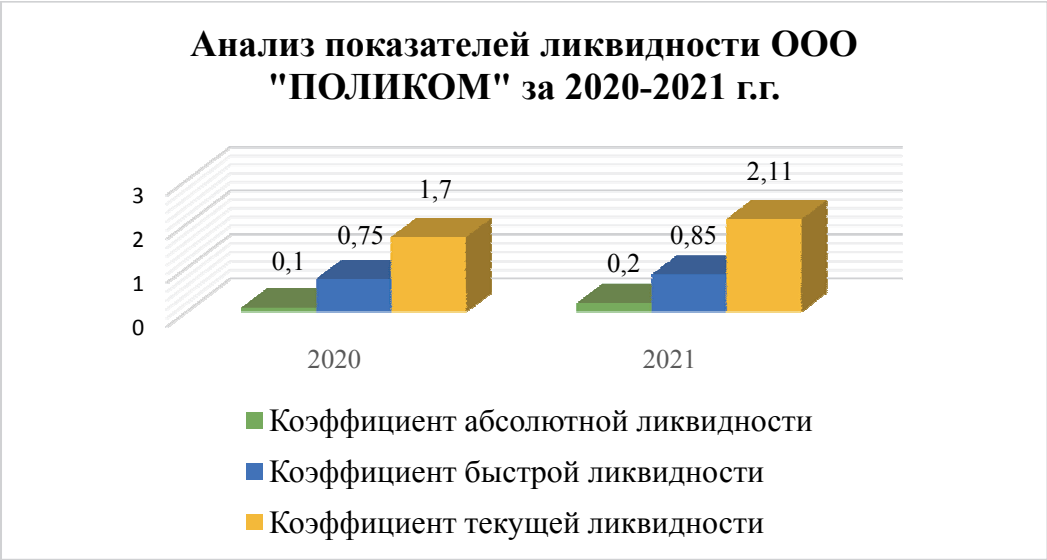


Рисунок 1 – Анализ показателей ликвидности ООО «Поликом» за 2020-2021 гг.

Одним из основных признаков устойчивости финансового положения организации является ее платежеспособность. Ее условием считается погашение в полном объем и в срок своих краткосрочных обязательств. Проведенные расчеты показателей платежеспособности представлены в таблице 3.

Анализ показателей платежеспособности показал, что увеличение денежных средств компании в 2021 году привело к увеличению доли денежных средств в чистом оборотном капитале на 0,5%, которая составила 0,6%. Об этом свидетельствует коэффициент соотношения денежных средств и чистого оборотного капитала организации.

Таблица 3 – Анализ показателей ликвидности и платежеспособности ООО «Поликом»

Наименование показателя	**Формула расчета**	**На начало года**	**На конец года**	**Отклонения (+,-)**	**Нормативное значение**
Коэффициенты ликвидности					
1.Коэффициент абсолютной ликвидности	Кал = ДС+КФВ/КФО	0,1	0,2	0,1	0,2-0,3
2. Коэффициент быстрой ликвидности	Кбл = ДС+КФВ+ДЗ/КО	0,75	0,85	0,1	0,7-0,8
3. Коэффициент текущей ликвидности	Ктл = ОА/КО	1,7	2,11	0,41	1,0-2,0
Показатели платежеспособности					
4. Коэффициент соотношения денежных средств и чистого оборотного капитала	Ксоотн = ДС/ЧОК	0,001	0,006	0,005	0-1,0
5.Коэффициент платежеспособности по текущим обязательствам	Кпл = КрЗС/Вср.мес.	2,99	1,44	-1,55	3 мес. – организация платежеспособна; 3…12 мес. - неплатежеспособность 1 категории; >12 мес. – неплатежеспособность 2 категории
6.Степень платежеспособности общая	Спл.общ. = ЗС/Вср.мес.	4,73	2,55	-2,18	
7.Коэффициент Бивера	BR = (ЧП +А)/(ДО+КО)	0,6	0,7	0,1	0,17 < Кб < 0,45 – предприятие

Наименование показателя	Формула расчета	На начало года	На конец года	Отклонения (+,-)	Нормативное значение
					платежеспособно; Кб>0,45 – предприятие высокоплатежеспособно; Кб<0,17 – предприятие неплатежеспособно.
8. Коэффициент покрытия процентов (защищенности кредиторов)	Кпп = EBIT / Проценты к уплате	1,59	1,83	0,24	⩾1

Коэффициент платежеспособности показал, что в 2021 году компании необходимо 1,4 месяца, чтобы расплатиться по своим текущим обязательствам за счет выручки. Данный показатель сократился на 1,6 месяцев по сравнению с 2020 годом.

Общая ситуация с платежеспособностью организации характеризуется тем, что в 2021 году компании было необходимо почти два с половиной месяца, что она могла рассчитаться по своим обязательствам при помощи выручки.

Коэффициент Бивера показывает степень платежеспособности предприятия, как на текущий момент, так и на перспективу. Таким образом, в 2021 году значение коэффициента показывает, что 0,7 руб. собственных средств приходится на 1 руб. заемного капитала. Рост показателя на 0,1 положительно влияет на финансовую независимость компании.

Полученные значения коэффициента покрытия процентов (защищенности кредиторов) показывает, что компания без проблем может погашать свои кредитные обязательства.

Динамику показателей платежеспособности представим наглядно на рисунке 2.

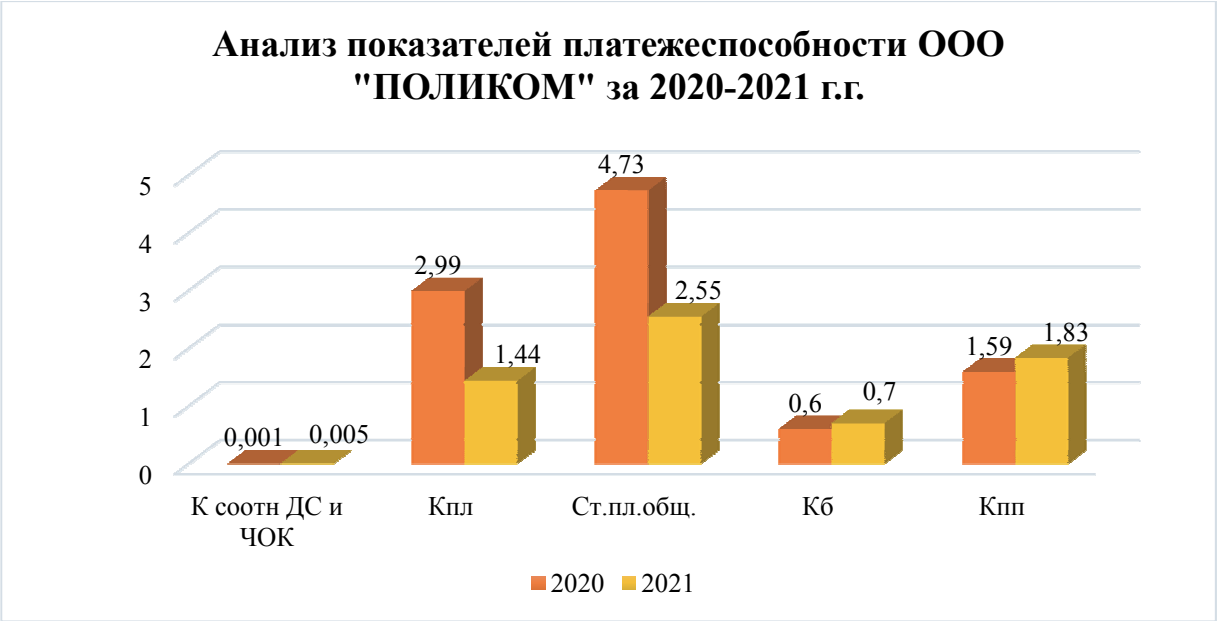


Рисунок 2 – Анализ показателей платежеспособности ООО «ПОЛИКОМ» за 2020-2021 гг.

Таким образом, в статье был проведен анализ эффективности использования оборотного капитала и анализ относительных показателей – коэффициентов ликвидности и платежеспособности.

В 2021 году повысились показатели оборачиваемости и рентабельности оборотных средств. Практически все показатели ликвидности и платежеспособности компании в анализируемом периоде незначительно увеличились. Большинство из них соответствовало пределу или даже превышало уровень рекомендуемых значений. Такое изменение характеризуется ростом объемов производства, что привело к увеличению выручки, оборотных активов и величины чистой прибыли. В то же время на результаты коэффициентов платежеспособности повлияло сокращение краткосрочных обязательств. Полученные выводы свидетельствуют о положительном финансовом состоянии исследуемого предприятия и способности рассчитываться по своим текущим обязательствам.

Литература

1. Герасимова, Е. Б. Экономический анализ: учебник / Е.Б. Герасимова. — Москва: ИНФРА-М, 2022. — 245 с.

2. Карпова, Е. Н. Финансы организаций (предприятий): учебное пособие / Е.Н. Карпова, Е.А. Чумаченко. — Москва: ИНФРА-М, 2020. — 285 с.

3. Краснова, Л. Н. Экономика предприятий: учебное пособие / Л.Н. Краснова, М.Ю. Гинзбург, Р.Р. Садыкова. — Москва: ИНФРА-М, 2022. — 374 с.

4. Мазурина, Т. Ю. Финансы организаций (предприятий): учебник / Т.Ю. Мазурина, Л.Г. Скамай, В.С. Гроссу. — М.: ИНФРА-М, 2018. — 528 с.

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ ОБЕЗЛИЧИВАЯНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ

Щербинина Анна Сергеевна, магистрант 1 курса кафедры информационной безопасности
Научный руководитель: **Сухотерин Александр Иванович**, к.воен.н., доцент, доцент кафедры информационной безопасности

Мир постоянно развивается и задает тенденции в самых разных аспектах жизни человеческого общества, но с давних пор люди осознали, что самым ценным ресурсом является информация. Изначально это касалось военных и государственных дел, но в современном мире в эпоху информационного общества, в котором каждый человек непосредственно связан с цифровым миром – личные данные, виртуальные банковские карты, онлайн образование и многое другое, важность обрели так же персональные данные каждой личности. Применение технологии обезличивания персональных данных в автоматизированной системе может стать одним из ключевых методов для сохранения безопасности данных в современном обществе.

Информационная безопасность, персональные данные, ПДн, обезличивание персональных данных, автоматизированная система.

APPLICATION OF THE TECHNOLOGY OF DEPERSONALIZATION OF PERSONAL DATA IN AN AUTOMATED SYSTEM

Shcherbinina Anna, 1st year graduate student of the Department of Information security
Scientific adviser: **Sukhoterin Alexander**, Candidate of Military sciences, Associate professor of the Department of Information security

The world is constantly evolving and setting trends in various aspects of society, but for a long time people have realized that the most valuable resource is information. Initially, this concerned military and state affairs, but in the modern world, in the era of the information society, in which everyone is directly connected to the digital world – personal data, virtual bank cards, online education and much more, personal data of each individual has also gained importance. The use of the technology of depersonalization of personal data in an automated system can become one of the key methods for maintaining data security in modern society.

Information security, personal data, depersonalization of personal data, automated system.

Тенденции в сфере информационной безопасности продиктованы в первую очередь актуальными угрозами сохранности данных, сейчас невозможно оспорить ценность персональных данных и заинтересованность ими злоумышленниками. Одним из ярких примеров масштабных утечек персональных данных (далее — ПДн) стала кража клиентской базы сервиса «Яндекс. Еда» - в сеть Интернет утекли тысячи учетных записей пользователей этой платформы: номера телефонов, логины аккаунтов, суммы заказов, адреса доставки и эта лишь толика информации, которую нам, обычным пользователям, было позволено увидеть. Но никто не знает насколько глубока кроличья нора и не получили ли злоумышленники более ценную информацию о пользователях.

Большой массив ПДн так же обрабатывается в государственных информационных системах, аккаунт в которых имеет почти каждый достигший совершеннолетия гражданин, а виду последних событий и накалённых отношений между государствами, самыми защищаемыми ресурсами являются государственные и коммерческие системы.

Законодательство всех крупных держав, предъявляет серьезные требования к защите ПДн, и новым веянием в сфере защиты данных является их обезличивание, поэтому это тема очень остро стоит перед специалистами по информационной безопасности [1].

Часто возникает вопрос, насколько данный способ регламентирован законодательством РФ и является ли правомерным его использование для обработки данных? В соответствии с законом «О персональных данных», при использовании обезличивания данных нет возможности определить их принадлежность физическому лицу без использования дополнительной информации. Конечно данный метод обработки данных не является панацеей и требует использования современных средств защиты систем обработки данных, систематическое обучение и контроль операторов, обрабатывающих их.

Таким образом применение технологии обезличивания ПДн в автоматизированных системах является актуальной задачей в сфере информационной безопасности, и носит практическую значимость как для государственных информационных систем, так и для коммерческих.

Роскомнадзор – госструктура, которая контролирует и координирует работу операторов, которые обрабатывают ПДн. Основополагающим нормативным документом, который регламентирует основные методы по обезличиванию ПДн, является - Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. № 996 "Об утверждении требований и методов

по обезличиванию персональных данных", ратифицированный Роскомнадзором в 2013 г. [4].

В зависимости от метода обезличивания, который используется, возможно получить данные с кардинально разными свойствами, которые подходят для определенного класса задач и условий на предприятии.

Как мы отметили ранее при обезличивании ПДн в автоматизированной системе на выходе можно получить информацию разных видов и свойств, обусловленную определенным методом.

Свойства, которыми обладают данные после обезличивания:

- Релевантность, то есть проведение действий с запросами и сбор ответов в единообразной семантической форме.
- Семантическая целостность, то есть сохранение семантики обезличенных данных семантике соответствующих ПДн при их обезличивании.
- Полнота, то есть сохранение полной информации о субъектах, которая имелась до проведения операции обезличивания;
- Применимость, то есть возможность последующего достижением результатов.
- Структурированность, то есть сохранение всех взаимосвязей между обезличенными данными субъекта, которые имелись до проведения операции обезличивания;
- Анонимность, то есть невозможность идентификации ПДн, после процедуры обезличивания, без применения дополнительной информации [4].

Сохранение вышеперечисленных свойств зависит от использованного метода обезличивания. На данный момент на уровне законодательства регламентированы следующие методы:

Метод 1. Введение идентификаторов.

Метод заключается в замене части ПДн, которые позволяют однозначно определить субъект ПДн, с помощью вводимых идентификаторов и составлением таблиц соответствия идентификаторов для субъекта.

При использовании рассматриваемого способа обезличивания мы можем получить данные со свойствами:

- структурированность
- полнота
- семантическая целостность

Рассматриваемый метод целесообразно использовать, когда в обработке участвуют малые массивы данных, так как объем базы данных после проведения обезличивания напрямую зависит от объема дополнительных данных, которые вводятся для идентификаторов, ввиду чего возникает возможность снижения мощности вычислений и затруднениеется внесение изменений в существующие базы;

Метод 2. Модернизация состава или семантики.

Принцип метода - обобщение, изменении значения ПДн или исключения какой-либо части информации, благодаря которой можно точно определить субъект, которому принадлежит эта информация.

Свойства, которыми обладают данные после обработки данным методом:

- структурированность
- анонимность

Метод модернизации состава и семантики стоит применять, когда возможно модернизировать состав и семантику данных, так, чтобы поставленные задачи не требовали дополнительных действий в виде предварительного деобезличивания, так как при использовании рассматриваемого метода невозможно вернуть базу в первозданный вид.

Метод 3. Декомпозиция.

Метод заключается в разделении массива ПДн на несколько частей с последующим раздельным хранением подмножеств.

При обработке данных этим методом, мы получим данные, которым будут характерны свойства:

- семантическая целостность (при использовании удостоверяющих таблиц можно получить исчерпывающий объем данных);
- полнота (атрибуты не меняют свое значение);
- структурированность (деление происходит на таблицы);

Метод декомпозиции используется при большом количестве атрибутов для массива ПДн, недостаток этого способа обезличивания заключается в том, что вычислительная мощность будет понижена при частом внесении изменений в исходный массив данных.

Метод 4. Перемешивание.

Название метода говорит само за себя, он подразумевает перемешивание отдельных значений атрибутов, принадлежащих ПДн между собой.

При применении данные будут обладать свойствами:

- семантическая целостность
- анонимность
- полнота
- структурированность

Данный метод является наиболее эффективным при необходимости обработки большого массива ПДн и соответствующим им атрибутов, так как он является наиболее стойким к атакам злоумышленников за счет возможности регулировки сложности обезличенного массива данных, с помощью увеличения состава атрибутов. Метод перемешивания эффективен при много ранговой обработке ПДн и определенной периодичности внесения изменений в значения данных.

Таким образом, мы провели анализ методов обезличивания ПДн и свойств, которыми обладает информация после обработки данными методами. В таблице 1 графически можно проследить связь между методом обезличивания ПДн и сохранением необходимых свойств для решения задач обработки данных.

Таблица 1 – Корреляция метода обезличивания с свойствами данных

Метод обезличивания / Свойства обезличенных данных	Метод введения идентификаторов	Метод изменения состава или семантики	Метод декомпозиции	Метод перемешивания
Полнота	+	+/-	+	+
Структурированность	+	+	+	+
Релевантность	+/-	+	+	+
Семантическая целостность	+	+/-	+	+
Применимость	+	+	+	+
Анонимность	+/-	+	+/-	+
+ безусловное наличие свойства +/- условное наличие свойства, см. описание метода				

Конечно же выбор метода для обработки массива ПДн будет напрямую определяться задачами, для которых собственно и необходимо проводить обезличивание ПДн. В таблице 2 рассмотрены методы обезличивания в зависимости от класса задач, которые необходимо решить. Указанные методы ранжированы в порядке убывания эффективности их применения.

Таблица 2 – Отношение метода обезличивания к классу задач обработки ПДн

Класс задач	Задачи обработки	Метод обезличивания
Статистическая обработка и статистические исследования ПД	- осуществление выборки по заявленным параметрам; - проведение исследований по заданным параметрам субъектов.	- метод перемешивания; - метод декомпозиции; - метод изменения состава или семантики.
Сбор и хранение ПД	- внесение персональных данных субъектов в информационную систему на основе анкет, заявлений и прочих документов.	- метод декомпозиции; - метод перемешивания; - метод введения идентификаторов.
Обработка поисковых запросов (поиск данных о субъектах и поиск субъектов по известным данным)	- поиск информации о субъектах; - печать и выдача субъектам документов в установленной форме, содержащих персональные данные; - выдача справок, выписок, уведомлений по запросам субъектов или уполномоченных органов.	- метод перемешивания; - метод декомпозиции; - метод введения идентификаторов.
Актуализация ПД	- внесение изменений в существующие записи о субъектах на основе обращений субъектов, решений судов и других уполномоченных органов; - внесение изменений в существующие записи о субъектах на основе исследований, выполнения органом своих функций или требований законодательства РФ.	- метод перемешивания; - метод декомпозиции; - метод введения идентификаторов.
Интеграция данных различных Операторов	- поиск информации о субъектах; - передача данных смежным органам.	- метод перемешивания; - метод декомпозиции; - метод введения идентификаторов.
Ведение учета субъектов ПД	- прием анкет, заявлений; - ведение учета персональных данных в соответствии с функциями органа.	- метод декомпозиции; - метод перемешивания; - метод введения идентификаторов.

Таким образом, был проведен анализ методов, свойств и процессов обработки обезличенных данных, оценка возможности применения полученных массивов информации для решения задач, поставленных в организации или учреждении. Из таблицы 2 видно, что самыми оптимальными методами для обработки данных в автоматизированной системе являются: метод декомпозиции; метод перемешивания; метод введения идентификаторов.

Напомним, что ПДн является любая информация, которая прямо или косвенно относится к определенному или определяемому физическому лицу (ч. 1 ст. 3 Федерального закона от 27 июля 2006 № 152-ФЗ "О персональных данных", далее – Закон № 152-ФЗ). Одним из методов решения проблемы защиты данных на нынешнем этапе развития общества и технологий соответствующий классам задач государственных и коммерческих предприятий может стать процедура их обезличивания. Использование технологии обезличивания персональных данных является своевременным и прогрессивным решением проблем в сфере информационной безопасности при работе с ПДн.

Литература

1. Доктрина информационной безопасности Российской Федерации утверждена Указом Президента Российской Федерации от 5 декабря 2016г № 646;
2. Федеральный закон № 149 от 27.07.2006г (ред. от 18.03.2019г) "Об информации, информационных технологиях и о защите информации";
3. Федеральный закон "О персональных данных" от 27.07.2006г № 152-ФЗ;
4. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. N 996 "Об утверждении требований и методов по обезличиванию персональных данных"
5. ФСТЭК России от 21.12.2017г № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;
6. Домарева В.В. "Безопасность информационных технологий. Системный подход" - К.: ООО ТИД «Диасофт», 2004.-992 с.

ИССЛЕДОВАНИЕ ПРОГРАММНЫХ СПОСОБОВ ЗАЩИТЫ ДАННЫХ В ФИНАНСОВЫХ УЧРЕЖДЕНИЯХ

Ярных Евгений Валерьевич, магистрант 1 курса кафедры информационных технологий и управляющих систем
Научный руководитель: **Исаева Галина Николаевна**, к.т.н., доцент кафедры информационных технологий и управляющих систем

Одной из основных задач организаций является обеспечение высокой степени безопасности информационных ресурсов, в состав которых входит и экономическая информация. Существует большое количество потенциальных угроз для информационных сетей финансовых учреждений. Это является причиной высоких рисков, как экономических, так и информационных. В данной статье проведен анализ развития современных средств защиты информации, показана степень соответствия их текущему уровню развития информационных технологий (ИТ).

Система защиты информации, персональные данные, программные системы.

A STUDY OF SOFTWARE-BASED DATA PROTECTION IN FINANCIAL INSTITUTIONS

Yarnykh Evgeny, 1st year graduate student of the Department of Information technology and system management
Scientific adviser: **Isaeva Galina**, Candidate of Technical sciences, Associate professor of the Department of Information technology and system management

One of the main tasks of organizations is to ensure a high degree of security of information resources, which include economic information. There are a large number of potential threats to the information networks of financial institutions. This is the reason for high risks, both economic and informational. This article analyzes the development of modern information security tools, shows the degree of compliance with their current level of information technology (IT) development.

Information security system, personal data, software systems.

Характерной чертой сегодняшнего времени является широкое использование автоматизированных систем управления(АИС) в различных сферах человеческой деятельности. Основу любой АИС составляет, в том числе, и БД (база данных). Такой способ организации и управления информацией - в виде СУБД (системы управления БД) - наиболее приемлем и требует защиты информации, как внутри самой АИС, так и при доступе из

вне. Особенно важным является организация средств защиты экономической информации финансового сектора.

Существует несколько различных методик формирования требуемого уровня защиты баз данных финансовой информации. Среди этих методик наиболее распространенными и востребованными являются:

- методики, основанные на использовании организационных и технических средствах защиты информации;
- методики, основанные на использовании экономических средств защиты информации;
- методики, основанные на использовании правовых средств защиты информации.

Основой методик защиты, основанных на организационных и технических средствах, являются:

– комплекс различных программных и аппаратных систем защиты информационных ресурсов;
- комплекс мероприятий, которые направлены на профилактику случаев утечки информации (инструкции, регламент работы и обмена информационными ресурсами);
– комплекс мероприятий, направленных на модернизацию применяемых в настоящее время систем обеспечения информационной безопасности;
– комплекс мероприятий, направленных на контроль соблюдения всех норм и правил при работе и обмене информационными ресурсами.

Как показывает практика, без осуществления постоянного контроля за исполнением требований информационной безопасности очень сложно иметь адекватную картину текущего состояния системы безопасности информационных ресурсов.

Процесс совершенствования системы безопасности информации основывается на правовых способах обеспечения информационной безопасности. Основой методик защиты, основанных на правовых средствах, являются:

– комплекс мероприятий, направленных на определение уровня квалификации организаций, которые оказывают услуги по обеспечению безопасности информационных ресурсов;
– комплекс мероприятий, направленных на внедрение систем защиты данных, имеющих соответствующие сертификаты соответствия.

Основой методик защиты, основанных на экономических средствах, являются:

– комплекс мероприятий, направленных на финансирование и развитие комплексных средств обеспечения безопасности информационных ресурсов;
– комплекс мероприятий, направленных на привлечение инвестиций и других средств на развитие информационной безопасности;

– комплекс мероприятий, направленных на планирование и рациональное распределение экономических ресурсов;

– комплекс мероприятий, направленных на формирование страхового обеспечения безопасности информации.

Под термином информационной безопасности подразумевается комплекс мероприятий, основной целью которых является профилактика несанкционированного доступа к базам данных со стороны злоумышленников. При обеспечении всех требований информационной безопасности соблюдаются все нормы и правила работы с информационными ресурсами, которые предусмотрены в соответствующих правовых документах. При применении в системе защиты информации эффективных технических средств, обеспечивается высокий уровень безопасности данных. Также обеспечивается постоянный контроль за активностью средств хищения информационных ресурсов.

В настоящее время в нашей стране действует несколько нормативно-правовых документов, которые осуществляют регулирование работы с базами данных:

- закон «Обеспечение безопасности информационных ресурсов»;
- закон «Обеспечение безопасности конфиденциальных данных»;
- закон «О коммерческой тайне» [5].

Также существует еще один, не менее важный документ, который называется «Сертификация технических средств обеспечения информационной безопасности». Все организации, оказывающие услуги по защите информационных ресурсов должны проходить обязательную процедуру лицензирования. Согласно разработанной программе ФСБ РФ, постоянно ведутся работы по созданию шифровальных (криптографических) средств защиты информации [7].

Согласно основному принципу экономической составляющей системы информационной безопасности, величина затрат на создание безопасных условий для баз данных не должна больше стоимости объекта защиты. Для обеспечения высокой экономической эффективности средств защиты необходимо обеспечивать защиту именно тех информационных ресурсов, которые являются наиболее важными и ценными.

Исходными данными при создании средств защиты информации являются объекты защиты, к которым относятся: информация, передаваемая с помощью различных технических средств, а также информация в виде речи.

Помимо этого, к объектам защиты относятся: комплекс основных технических средств, с помощью которых осуществляется обработка и передача информации, комплекс дополнительных технических средств, с помощью которых осуществляется обработка и передача информации.

Организационная составляющая системы информационной защиты подразумевает формирование комплекса регламентирующих документов, в

основе которых лежат действующие законы по защите информационных ресурсов.

В состав организационной составляющей системы информационной защиты входят следующие элементы:

– формирование служб и организаций, основная задача которых заключается в обеспечении безопасности информационных ресурсов;

– формирование комплекса регламентирующих актов и правил работы с защищаемыми данными и информационными ресурсами;

– формирование комплекса регламентирующих актов и правил обмена информацией, которая является объектом хищения;

– формирование комплекса регламентирующих актов и правил работы с техническими средствами обработки и передачи информации;

– создание подразделений, осуществляющих постоянный контроль текущего состояния безопасности информационных ресурсов.

Основной принцип обеспечения безопасности информационных ресурсов состоит в том, что необходимо контролировать процесс доступа различных сотрудников к тем или иным данным, которые могут быть подвержены атакам со стороны злоумышленников. Организационная составляющая системы информационной защиты не рассматривает технические способы и инструменты, с помощью которых можно обеспечить требуемый уровень безопасности информационных ресурсов.

Техническая составляющая системы информационной защиты подразумевает использование всех имеющихся средств защиты информации: СУБД, ППО, устройства шифрования, DLP и SIEM инструменты и т.д.

Техническая и организационная составляющие системы информационной защиты дополняют друг друга и при комплексном использовании формируют организационно-техническую составляющую. В качестве примера можно привести мероприятия по выявлению технических средств хищения информационных ресурсов.

В процессе разработки комплексного подхода к решению задачи информационной безопасности используется множество различных инструментов, среди которых:

– инструменты, предназначенные для разграничения доступа к информационным ресурсам со стороны различных групп пользователей;

– инструменты, предназначенные для проверки учетных записей, с которых ведется работа с информационными ресурсами;

– инструменты, предназначенные для шифрования и кодирования защищаемой информации.

Для высокой эффективности функционирования систем безопасности информационных ресурсов необходимо соблюдать ряд основных правил:

– постоянный контроль выполнения и соблюдения всех установленных правил и ограничений;

– применение комплексного метода решения вопросов информационной безопасности;

– обеспечение максимального уровня синхронизации работы всех технических средств защиты информационных ресурсов.

С целью обеспечения безопасности речевой и акустической информации необходимо обеспечить выполнение следующих правил: рациональное расположение помещений, в которых необходимо обеспечить безопасность акустической информации; определение границ работы средств защиты информационных ресурсов; осуществление контроля за всеми лицами, пытающимися получить доступ к информации на охраняемой территории.

Для успешного решения вопросов защиты информационных ресурсов необходимо систематически проводить проверку всех территорий и помещений на предмет наличия технических средств хищения данных.

В качестве дополнительных мер, для усиления безопасности информационных ресурсов, используются следующие инструменты: акустическая изоляция защищаемых помещений, обеспечение высокого уровня изоляции защищаемой информационной системы в случае угрозы, обеспечение возможности полной изоляции информационной системы от внешнего воздействия.

Среди технических методов обеспечения информационной безопасности следует выделить комплекс активных и пассивных механизмов, с помощью которых обеспечивается защита речевой информации. Активными средствами защиты акустической информации являются: генераторы шума и помех. К пассивным средствам относятся различные экранирующие приспособления и материалы, а также акустические фильтры.

Данные и информация, которые обрабатываются и подлежат передаче, защищаются следующими способами:

– проверка всех пользователей, которые осуществляют обработку и обмен информационными ресурсами сети;

– разграничение прав доступа к данным со стороны различных групп пользователей;

– использование технических средств кодирования информации;

– использование программных средств, которые обеспечивают использование пользователями персональных ключей;

– использование программного обеспечения, предусматривающего безопасное соединение при работе в сети Интернет.

Исследуя представленные методы обеспечения безопасности, следует отметить, что самым распространенным способом ограничения круга лиц, которые могут работать с защищаемыми информационными ресурсами, является процедура аутентификация. Данная процедура предусматривает наличие у каждого пользователя персонально логина и пароля. Аутентификация также широко применяется для ограничения доступа

отдельных групп пользователей к определенной части информации, хранящейся в сети. Помимо аутентификации, пользователи могут быть наделены различными правами для совершения различных операций с имеющейся информацией.

Процедура кодирования информации является эффективным средством обеспечения информационной безопасности. Кодирование данных реализуется системой EFS (Encrypting File System).

Для того, чтобы гарантировать безопасность соединений, используются специализированные информационные каналы, которые построены по принципу «клиент-клиент» или «клиент-сервер».

IPsec представляет собой комплексное решение, основная задача которого заключается в защите ресурсов сети, которые передаются в соответствии с IP-протоколом (Internet Protocol).

Все мероприятия в рамках технических и организационных составляющих системы информационной защиты должны лежать в рамках границ, установленных соответствующими правовыми нормативными документами РФ.В результате проведенного патентного поиска, было найдено несколько патентов в исследуемой области [6].

1. *Патент РФ № 2445692* – Метод защиты информационных ресурсов в процессе работы в сети Интернет. Рассматриваемая методика основана на применении стека коммуникационных протоколов TCP/IP при работе пользователей в сети Интернет. С помощью этого стека достигается высокий уровень безопасности информационных ресурсов. Протокол TCP/IP предназначен для работы с базами данных, которые хранятся в различных сетевых компьютерных структурах.

Данная методика обеспечивает высокий уровень безопасности данных путем шифрования и кодирования информации, которая отражает точное местоположение выхода в сеть Интернет. Безопасность информационных ресурсов достигается за счет работы socks-серверов, с помощью которых генерируется большое количество вариантов доступа к ресурсам сети Интернет. Также эти серверы предусматривают возможность постоянной смены точек выхода. Смена точек доступа необходима в те моменты, когда существует потенциальная угроза безопасности информационных ресурсов.

Существует методика обеспечения информационной безопасности ресурсов сети, которая описана в патенте РФ № 2002125855, класс G06F 17/30, G06F 13/00, от 2001.03.23.

2. *Патент РФ № 2469391* – Методика прохождения процедур аутентификации пользователей.

Рассматриваемый патент описывает методику идентификации клиентов сетей различных платежных систем. В результате использования этой методики обеспечивается высокая эффективность защиты средств от несанкционированного доступа. В состав системы идентификации пользователей входят следующие компоненты: процессор для работы с

криптографической информацией, набор ключей для работы с криптографическими данными, набор инструментов для работы с обрабатываемой информацией, интерфейс.

3. *Патент РФ № 2528078* – Методика обеспечения безопасности сетевого соединения. Данный патент рассматривает один из способов обеспечения безопасных сеансов связи при использовании сети Интернет. При использовании данного организационно – технического решения достигается высокая степень защищенности обрабатываемой информации путем сегментации ключей доступа. Рассматриваемая методика подразумевает обмен информационными ресурсами в защищенном режиме. Обмен информацией осуществляется между узлами N1 и N2. Каждый из узлов содержит информацию о генерируемых ключах безопасности.

Данный патент разработан с целью обеспечения безопасного Интернет соединения за счет использования средств кодирования и шифрования данных, которые передаются через глобальную сеть.

Обобщая исследования в данной области, можно констатировать, что методы защиты конфиденциальной информации в любой сфере человеческой деятельности можно представить следующей классификацией (Рис.1).

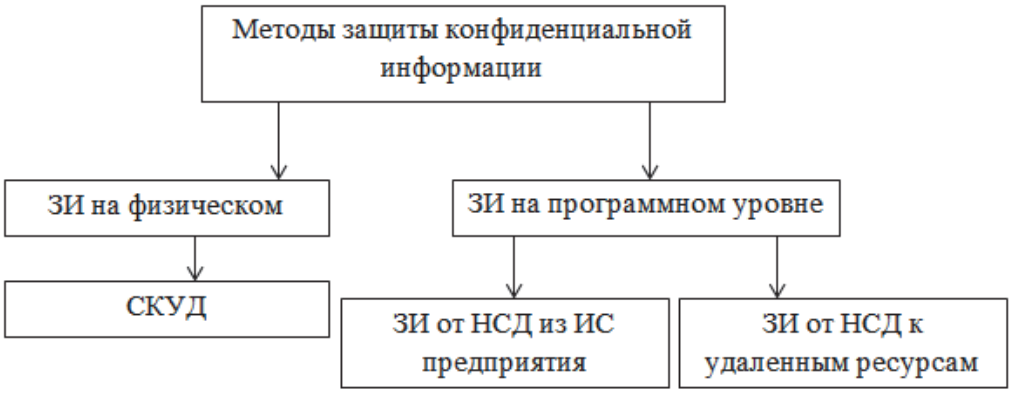


Рисунок 1 – Общая классификация методов защиты конфиденциальной информации

Система контроля и управления доступом(СКУД) выполняет функции управления доступом посторонних лиц и сотрудников на территорию охраняемого объекта. Данная система по установленным условиям в автоматическом режиме контролирует списки физических лиц, которые обладают доступом на территорию компании. Такие системы, как правило, устанавливается на проходных и кроме функций ограничения доступа выполняют функции учета рабочего времени сотрудников, нарушений режима, ведения баз данных, содержащих сведения, о сотрудниках и временных посетителях и так далее [3].

Следующий компонент организации безопасности - это средства защиты от несанкционированных утечек данных из информационных систем. Для этого имеются технологии, которые используют программные продукты

или различные программно-аппаратные устройства, производящие анализ информации, передаваемой во внешние сети.

Программно-аппаратные системы в самом общем случае классифицируются по двум направлениям:

- сетевые (шлюзовые), контролирующие Интернет-трафик локальной вычислительной сети;

- системы уровня хост, в которых составные части встраиваются в рабочие станции ЛВС (Локальная вычислительная сеть – LAN – англ.) и проводят наблюдение за записью информационных ресурсов на внешних носителях [4].

Программно-аппаратные системы являются важнейшей частью всей системы информационной безопасности, так как помимо своих непосредственных задач по предотвращению утечки информации, они позволяют экономить Интернет-трафик предприятия, распознать нецелевое использование информационных ресурсов предприятия, обнаружить не только утечку, но и приток нежелательной информации.

Третьим компонентом классификации методов обеспечения безопасности информации, являются средства защиты от несанкционированного доступа к удаленным информационным ресурсам.

Выводы: Финансовая информация, наряду с другими видами информации, как правило, организована в виде БД на предприятиях и в учреждениях. Ввиду её значимости, она подлежит защите при помощи создания систем защиты информации. Методы защиты подлежат лицензированию и узаконены нормативно-правовыми документами РФ. Важную роль в методах защиты информации занимают программные системы, как неотъемлемая составляющая современных компьютерных систем и технологий.

Литература

1. Бабенко, Л.К. Современные алгоритмы хеширования и методы их анализа: учебное пособие для студентов вузов, обучающихся по группе специальностей в обл. информ. безопасности / Л.К. Бабенко, Е.А. Ищукова. – М.: Гелиос АРВ, 2018. – 376 с.

2. Белов Е.Б. Основы информационной безопасности. Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. -М.: Горячая линия - Телеком, 2019. - 544с.

3. Бен-Ган Ицик. Microsoft SQL Server 2012 Основы T-SQL - М.: Эксмо, 2018. — 401 с.

4. Брассар, Ж. Современная криптология : [пер. с англ.] / Ж. Брассар. – М.: Полимед, 2018. – 176 с.

5. Закон «Обеспечение безопасности информационных ресурсов». Электронный ресурс. - Код доступа: http://www.consultant.ru/document/ (Дата обращения 14.04.2022)

6. Патенты. Электронный ресурс. - Код доступа: http://allpatents.ru/patent/2445692.html// (Дата обращения 14.04.2022)
7. Сертификация технических средств обеспечения информационной безопасности// Электронный ресурс. - Код доступа: https://www.garant.ru/products/ipo/prime/doc/71842006/ (Дата обращения 14.04.2022)

Научное издание

СОВРЕМЕННЫЕ ИННОВАЦИИ В ЭКОНОМИКЕ, ТЕХНИКЕ И ОБЩЕСТВЕ

V Ежегодная научная конференция магистрантов Технологического университета

Сборник материалов

Дата подписания к использованию 30.08.22

Тираж 500 экз.

Издательство Научный консультант
123007, Москва, Хорошевское ш., 35к2, офис 508.
Тел.: +7 (926) 609–32–93, +7 (499) 195–60–77 www.n–ko.ru keyneslab@gmail.com