



Государственное бюджетное образовательное учреждение высшего образования
Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

ПРИНЯТО
Решением Ученого совета ГБОУ ВО МО
«Технологический университет»
Протокол № 9
«28» сентября 2020 г.



УТВЕРЖДАЮ
Ректор ГБОУ ВО МО
«Технологический университет»
Т.Е. Старцева
«28» сентября 2020 г.

**ОСНОВНАЯ ПРОФЕССИОНАЛЬНАЯ
ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
ВЫСШЕГО ОБРАЗОВАНИЯ**

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Год набора: 2020

Королев
2020

Руководитель ОПОП: к.т.н., доцент Вихров А.П. Основная профессиональная образовательная программа высшего образования 10.03.01 Информационная безопасность, профиль: «Безопасность телекоммуникационных систем (в аэрокосмической сфере)» - Королев МО: Технологический университет, 2020.

Основная профессиональная образовательная программа высшего образования 10.03.01 Информационная безопасность, профиль: «Безопасность телекоммуникационных систем (в аэрокосмической сфере)» составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки бакалавров 10.03.01 Информационная безопасность и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 28.04.2020 года.

Основная профессиональная образовательная программа рассмотрена и одобрена на заседании кафедры «Информационной безопасности» протокол № 8 от 26.03.2020 года.

Основная профессиональная образовательная программа рекомендована на заседании УМС протокол № 7 от 28.04.2020 года.

Рецензия
на основную профессиональную
образовательную программу высшего образования
квалификации выпускника «Бакалавр»
по направлению подготовки 10.03.01 «Информационная безопасность»,
профиль «Безопасность телекоммуникационных систем (в аэрокосмической сфере)»,
разработанную ГБОУ ВО МО «Технологический университет»

Основная профессиональная образовательная программа высшего образования (далее – ОПОП) разработана кафедрой информационной безопасности ГБОУ ВО МО «Технологический университет».

Образовательная программа обеспечивает: проведение учебных занятий в различных формах по дисциплинам (модулям); проведение практик, проведение контроля качества освоения образовательной программы посредством текущего контроля успеваемости, промежуточной аттестации и государственной итоговой аттестации обучающихся.

• Структура ОПОП разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования (далее – ФГОС) по направлению подготовки 10.03.01 «Информационная безопасность» от 1 декабря 2016 года №1515 (Зарегистрировано в Мinedu России 20 декабря 2016 года № 44821); Приказа Минобрнауки России от 05.04.2017 № 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры», а также с учетом потребностей рынка труда; Методические рекомендации по разработке программ обучения по IT-технологиям и предпринимательству для студентов в рамках регионального компонента профессионального образования, утвержденные приказом Министерства образования Московской области от 05 июня 2020 г. № Исх-9727/16-20 с.

В характеристике ОПОП указаны: цели и задачи ОПОП; срок освоения ОПОП; квалификация, присваиваемая выпускникам; виды профессиональной деятельности, к которым готовятся выпускники; планируемые результаты освоения ОПОП, кадровое, учебно-методическое, информационное, материально-техническое и финансовое обеспечение и др.

Компетентностная модель выпускника отражает все требования ФГОС по направлению подготовки 10.03.01 «Информационная безопасность».

Базовая часть ОПОП является обязательной и обеспечивает формирование у обучающихся компетенций, установленных ФГОС.

Вариативная часть образовательной программы направлена на расширение и углубление компетенций, установленных ФГОС, и включает в себя дисциплины (модули) и практики, установленные с учетом требований работодателей. Содержание вариативной части сформировано в соответствии с направленностью образовательной программы.

Образовательная программа представляет собой комплекс основных характеристик образования, организационно-педагогических условий, форм аттестации и определяет цели, ожидаемые результаты, содержание, условия и технологии реализации образовательного процесса, оценку качества подготовки выпускника по данному направлению подготовки. Включает в себя: учебный план, календарный учебный график, рабочие программы дисциплин (модулей), фонды оценочных средств для проведения промежуточной и итоговой аттестации обучающихся и другие материалы, обеспечивающие качество подготовки обучающихся, а также программы практик и методические материалы, обеспечивающие реализацию соответствующей образовательной технологии.

В образовательной программе определены: планируемые результаты освоения образовательной программы - компетенции обучающихся; планируемые результаты обучения, по каждой дисциплине (модулю) и практике - знания, умения, навыки (опыт) деятельности, характеризующие этапы формирования компетенций и обеспечивающие достижение планируемых результатов освоения образовательной программы.

Объем ОПОП (ее составной части) определен как трудоемкость учебной нагрузки обучающегося при освоении образовательной программы (ее составной части), включает в себя все виды его учебной деятельности, предусмотренные учебным планом для достижения планируемых результатов обучения. В качестве унифицированной единицы измерения трудоемкости учебной нагрузки обучающегося при указании объема ОПОП и ее составных частей используется зачетная единица. Объем ОПОП, ее составных частей, выражен целым числом зачетных единиц. Общая трудоемкость программы составляет 240 зачетных единиц (1 зачетная единица равна 36 академическим часам).

ОПОП предусматривает изучение следующих блоков:

-Блок 1 «Дисциплины (модули)», включающий дисциплины (модули), относящиеся к базовой части программы, и дисциплины (модули), относящиеся к ее вариативной части.

-Блок 2 «Практики», включающий учебную практику и производственную практику в полном объеме относящийся к вариативной части программы.

-Блок 3 «Государственная итоговая аттестация», относящийся к базовой части программы и завершающийся присвоением квалификации.

Рабочие программы базовых дисциплин, дисциплин вариативной части и дисциплин по выбору обучающегося, построены по единой схеме. Программы содержат аннотацию с определением цели и задач дисциплины; общую трудоемкость дисциплины; результаты обучения; образовательные технологии; формы текущего контроля и промежуточной аттестации; учебно-методическое, информационное и материально-техническое обеспечение дисциплины.

Образовательные технологии обучения характеризуются не только общепринятыми формами (лекции, занятия семинарского типа, практические занятия, лабораторные занятия), но и интерактивными формами обучения.

Программа государственной итоговой аттестации по направлению подготовки 10.03.01 «Информационная безопасность». в полной мере устанавливает уровень готовности выпускника к выполнению профессиональных задач.

Обучаемые участвуют в проектно-технологической, экспериментально исследовательской, организационно-управленческой, эксплуатационной деятельности.

Направленность ОПОП предусматривает возможность проведения по профилю анализ функциональных процессов объектов информационной безопасности и их составляющих, формировать предложения по оптимизации обеспечения процессов ИБ объектов с целью повышения их устойчивости к деструктивным информационным воздействиям, тактике защиты и локализации последствий на защищаемые информационные объекты, обосновывать целесообразный комплекс мер по обеспечению информационной безопасности объектов защиты, организовывать его внедрение и последующее сопровождение, осуществлять контроль защищенности информационных объектов в соответствии с нормативными документами.

Ресурсное обеспечение ОПОП по направлению подготовки 10.03.01 «Информационная безопасность» соответствует всем требованиям ФГОС, а указанная среда ГБОУ ВО МО «Технологический университет» в полной мере обеспечивает гармоничное развитие личности выпускника. Нормативно-методическое обеспечение ОПОП по направлению подготовки 10.03.01 «Информационная безопасность» охватывает все аспекты системы оценки качества освоения обучающимися установленных стандартами необходимых компетенций.

В качестве сильных сторон рецензируемой образовательной программы следует отметить:

- актуальность и практикоориентированность;
- привлечение для реализации ОПОП опытного профессорско-преподавательского состава, а также представителей работодателей;
- учет требований работодателей при формировании дисциплин учебного плана;
- углубленное изучение областей знаний.

Выводы:

1. ОПОП подготовки бакалавров, реализуемая ГБОУ ВО МО «Технологический университет» по направлению подготовки 10.03.01 Информационная безопасность, соответствует требованиям ФГОС;
2. ОПОП учитывает потребности на рынке труда Москвы и Московской области и (профессионального сообщества региона) и может быть использована для осуществления образовательной деятельности по направлению подготовки 10.03.01 «Информационная безопасность», профиль «Безопасность телекоммуникационных систем (в аэрокосмической сфере)».

Генеральный директор

Дата «02» июля 2020г.



И.Н. Землячев.

1. Общие положения

Основная профессиональная образовательная программа высшего образования (далее – ОПОП ВО), реализуемая Государственным бюджетным образовательным учреждением высшего образования Московской области «Технологический университет» (далее – МГОТУ) по направлению подготовки 10.03.01 «Информационная безопасность» (квалификация (степень) «бакалавр»), представляет собой комплекс документов, разработанный на основе федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 «Информационная безопасность» (далее ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность»), разработана на основании следующих нормативных документов:

- Закон РФ от 29.12.2012 № 273 «Об образовании в Российской Федерации»;
- Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.03.01 Информационная безопасность (квалификация (степень) «бакалавр»), утвержденный приказом Министерства образования и науки Российской Федерации от «01» декабря 2016 г. № 1515 (Зарегистрировано в Минюсте России 20 декабря 2016 года № 44821) (далее- ФГОС ВО);
- Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам магистратуры, программам специалитета, утвержденный приказом Минобрнауки России от 5 апреля 2017 года № 301;
- О внесении изменения в Приказ Министерства образования и науки РФ от 12 сентября 2012 года № 1061 «Об утверждении перечня специальностей и направлений подготовки высшего образования» от 25 марта 2015 года № 270;
- Порядок проведения государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры, утвержденный приказом Минобрнауки России от 29 июня 2015 г. № 636;
- Приказ Министерства образования и науки РФ от 15 декабря 2017 г. № 1225 «О внесении изменений в Положение о практике обучающихся, осваивающих основные профессиональные образовательные программы высшего образования, утвержденное приказом Министерства образования и науки Российской Федерации от 27 ноября 2015 г. № 1383»;
- Методические рекомендации по разработке программ обучения по IT-технологиям и предпринимательству для студентов в рамках регионального компонента профессионального образования, утвержденные приказом Министерства образования Московской области от 05 июня 2020 г. № Исх-9727/16-20 с.
- Приказ Министерства образования и науки Российской Федерации от 23.08.2017 № 816 «Об утверждении Порядка применения организациями,

осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;

- Иные нормативные документы Министерства науки и высшего образования, а также локальные акты Университета, регламентирующие ведение образовательной деятельности.

ОПОП ВО бакалавриата имеет своей **целью** развитие у студентов личностных качеств и формирование компетенций в соответствии с действующим образовательным стандартом по направлению подготовки 10.03.01 Информационная безопасность.

Нормативный срок освоения ОПОП ВО – 4 года. Сроки освоения основной профессиональной образовательной программы бакалавриата по очной, очно-заочной и заочной формам обучения, а также в случае сочетания различных форм обучения увеличиваются не менее чем на 6 мес. и не более чем на 1 год по сравнению со сроком получения образования по **очной** форме обучения.

Общая трудоемкость освоения ОПОП ВО – 240 зачетных единиц. Трудоемкость основной профессиональной образовательной программы по **очной** форме обучения за учебный год равна 60 зачетным единицам.

Требования к уровню подготовки, необходимому для освоения ОПОП ВО

Абитуриент должен иметь документ государственного образца о среднем (полном) общем образовании или среднем профессиональном образовании и продемонстрировать необходимый уровень подготовки по предметам, предусмотренным перечнем вступительных испытаний.

2. Характеристика профессиональной деятельности выпускника ОПОП ВО по направлению подготовки 10.03.01 «Информационная безопасность»

Область профессиональной деятельности выпускников

В соответствии с ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность» область профессиональной деятельности выпускника включает: сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере.

Кроме того, профессиональная деятельность выпускника будет связана с регулированием и противодействиям правонарушениям в сфере экономической безопасности.

Выпускники обладают специальными знаниями по применению современных технологий информационной безопасности для региона, что открывает дополнительные перспективы и дает возможность трудоустройства не только в правоохранительных органах Российской Федерации, но и в государственных и коммерческих организациях, осуществляющих информационную безопасность различных информационных объектов и структур.

Выпускники данного направления подготовки могут применять свои профессиональные знания при работе в Федеральной службе по техническому и экспортному контролю, в администрациях субъектов РФ, федеральных и региональных органах управления и структурах предприятий любых форм собственности связанных, в том числе с внешнеэкономической деятельностью, правоохранительных органах, Федеральной службе безопасности, Федеральной службе охраны в торговых фирмах и организациях, занимающихся закупкой и поставкой специальных сил и средств по защите информации, в том числе и за рубежом, логистических фирмах, складах или терминалах различного назначения, торговых сетях, транспортно-экспедиционных компаниях.

Объекты профессиональной деятельности выпускника

В соответствии с ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность»:

объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, информационные ресурсы и информационные технологии в условиях существования угроз в информационной сфере;

технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах;

процессы управления информационной безопасностью защищаемых объектов.

Виды профессиональной деятельности выпускника

В соответствии с ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность» видами профессиональной деятельности, к которым готовятся обучающиеся по специальности:

- эксплуатационная;
- проектно-технологическая;
- экспериментально-исследовательская;
- организационно-управленческая.

Задачи профессиональной деятельности выпускника

В соответствии с ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность» бакалавр должен быть подготовлен к решению следующих профессиональных задач в соответствии с видами профессиональной деятельности и профилем подготовки:

в эксплуатационной деятельности: установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований; администрирование подсистем информационной

безопасности объекта; участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;

в проектно-технологической деятельности: сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности; проведение проектных, расчетов элементов систем обеспечения информационной безопасности; участие в разработке технологической и эксплуатационной документации; проведение предварительного технико-экономического обоснования проектных расчетов;

в экспериментально-исследовательской деятельности: сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования; проведение экспериментов по заданной методике, обработка и анализ результатов; проведение вычислительных экспериментов с использованием стандартных программных средств;

в организационно-управленческой деятельности: осуществление организационно-правового обеспечения информационной безопасности объекта защиты; организация работы малых коллективов исполнителей; участие в совершенствовании системы управления информационной безопасностью; изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа; контроль эффективности реализации политики информационной безопасности объекта защиты.

в соответствии с направленностью (профилем) «Безопасность телекоммуникационных систем (в аэрокосмической сфере)»: проводить совместный анализ функционального процесса объекта защиты и его информационных составляющих с целью определения возможных источников угроз, их вероятных целей и тактики; участие в формировании предложений по оптимизации функционального процесса и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов; участие в разработке комплекса мер по обеспечению информационной безопасности объекта и организации его внедрения и последующего сопровождения; участие в организации контроля защищенности объектов в соответствии с нормативными документами.

3. Компетенции выпускника, формируемые в результате освоения данной ОПОП ВО

В результате освоения программы бакалавриата у выпускника должны быть сформированы общекультурные, общепрофессиональные, профессиональные и соответствующие направленности (профилю) программы бакалавриата профессионально-специализированные

компетенции.

В процессе освоения основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность обучающийся должен обладать следующими **общекультурными компетенциями (ОК):**

способностью использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1);

способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2);

способностью анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3);

способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);

способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);

способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);

способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7);

способностью к самоорганизации и самообразованию (ОК-8);

способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9).

Выпускник, освоивший программу бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, должен обладать следующими **общепрофессиональными компетенциями (ОПК):**

способностью анализировать физические явления и процессы для решения профессиональных задач (ОПК-1);

способностью применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2);

способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач (ОПК-3);

способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4);

способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5);

способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях

чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности (ОПК-6);

способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7).

Выпускник, освоивший программу бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, должен обладать **профессиональными компетенциями (ПК)**, соответствующими видам профессиональной деятельности, на которые ориентирована данная программа:

Эксплуатационная деятельность:

способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);

способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);

способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3);

способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);

способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5);

способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6);

Проектно-технологическая деятельность:

способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7);

способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8);

Экспериментально-исследовательская деятельность:

способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9);

способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10);

способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов (ПК-11);

способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12);

Организационно-управленческая деятельность:

способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13);

способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14);

способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15).

В процессе освоения основной профессиональной образовательной программы обучающиеся также приобретают следующие **профессионально-специализированные компетенции**, которые реализуют подготовку бакалавров в соответствии с профилем «Организация и технология защиты информации» (ПСК):

способность проводить совместный анализ функционального процесса защиты ТКС и ее информационных составляющих с целью определения возможных источников угроз, их вероятных целей (ПСК-1);

способность формировать предложения по оптимизации функционального процесса и его компонентов с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и меры по информационной защите ТКС (ПСК-2);

способность организовывать контроль и анализ защищенности объектов ТКС в соответствии с нормативными документами (ПСК-3);

способность организовать реализацию принятых мер по управлению защитой информационных потоков на пакетном уровне с комплексной оценкой информационной безопасности ТКС (ПСК-4).

Приобретенные компетенции способствуют формированию профессиональных качеств квалифицированного специалиста, отвечающего требованиям профессиональных стандартов. Расширение спектра формируемых компетенций обучаемых увеличивает конкурентоспособность выпускников университета на рынке труда.

4. Документы, регламентирующие содержание и организацию образовательного процесса при реализации ОПОП ВО по направлению подготовки 10.03.01 Информационная безопасность

В соответствии с ФГОС ВО по направлению подготовки «Информационная безопасность» содержание и организация

образовательного процесса при реализации ОПОП ВО регламентируются следующими документами:

- календарным учебным графиком;
- учебным планом;
- рабочими программами учебных дисциплин (модулей);
- программами практик;
- программой государственной итоговой аттестации;
- учебно-методическими материалами, обеспечивающими реализацию соответствующих образовательных технологий.

ОПОП предусматривает изучение обязательной (базовой) и вариативной (профильной) частей включающих группы учебных дисциплин (модулей), физической культуры; учебной и производственной практики; государственной итоговой аттестации, рекомендуемых ФГОС ВО, устанавливаемую Университетом. Вариативная (профильная) часть дает возможность расширения и/или углубления знаний, умений и навыков, определяемых содержанием базовых (обязательных) дисциплин (модулей), позволяет студенту получить углубленные знания и навыки для успешной профессиональной деятельности и/или обучение в послевузовского образовании.

Календарный учебный график

График учебного процесса определяет логическую последовательность реализации ОПОП ВО по годам (по курсам и семестрам), включая теоретическое обучение, практики, промежуточные и итоговую аттестации, каникулы.

Календарный учебный график по направлению подготовки 10.03.01 Информационная безопасность приведен в Приложении 1.

Учебный план

В учебном плане отображается логическая последовательность освоения блоков, разделов ОПОП ВО, учебных дисциплин, модулей и практик, обеспечивающих формирование компетенций. Указывается общая трудоемкость дисциплин, модулей, практик в зачетных единицах, а также их общая и аудиторная трудоемкость в академических часах.

Для каждой дисциплины, модуля, практики указываются виды учебной работы и формы промежуточной аттестации.

Учебный план подготовки бакалавра по направлению подготовки 10.03.01 Информационная безопасность приведен в Приложении 2.

Аннотация рабочих программ дисциплин в соответствии с учебным планом подготовки бакалавров по направлению подготовки 10.03.01 Информационная безопасность

Блок 1. Дисциплины (модули)

Б1.Б.01 «Философия»

Дисциплина «Философия» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой гуманитарных и социальных дисциплин.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «История», «Основы права», отдельных разделах «Экономика предприятия и организация производства» и компетенциях: ОК-2,3; ОПК-4, 6; ПК-4,7.

Дисциплина направлена на формирование следующих компетенций:

ОК-1: способность использовать основы философских знаний для формирования мировоззренческой позиции:

ОК-8: способностью к самоорганизации и самообразованию.

Содержание дисциплины включает в себя круг философских проблем и методов их исследования, в том числе связанных с будущей профессией; основные разделы философского знания; философия, ее предмет и значение, исторические типы философии, онтология, гносеология, философия и методология науки, социальная философия, философия истории, философская антропология.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы, 108 часов. Преподавание дисциплины ведется на 1 курсе во 2 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 2 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин гуманитарной направленности и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.02 «История»

Дисциплина «История» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой гуманитарных и социальных дисциплин.

Изучение данной дисциплины базируется на знаниях, полученных на предыдущем уровне образования (среднее общее или среднее профессиональное) и компетенциях: ОК-5,6; ОПК-5,7; ПК-9,14.

Дисциплина направлена на формирование следующих компетенций:

ОК-3: способность анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма.

Содержание дисциплины включает в себя круг вопросов, направленных на формирование целостного представления об историческом пути России в контексте общемирового исторического развития; развитие патриотического сознания студенчества.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 1 курсе во 2 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена во 2 семестре.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения дисциплины «История защиты информации в РФ» и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.03 «Иностранный язык» (английский, французский, немецкий языки)

Дисциплина «Иностранный язык» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой иностранного языка.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

ОК-7: способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности.

Предметом учебного курса является иностранный язык (английский, французский, немецкий) в единстве двух его составляющих - общей, реализующейся как средство международного общения, и специальной, позволяющей осуществлять профессиональную деятельность. Лексический

минимум курса составляет 4000 лексических единиц общего и терминологического характера.

Цель курса – формирование умений письменного и устного общения, совершенствование навыков чтения, устной речи, аудирования и письма на иностранном языке, необходимых для выполнения профессиональной деятельности.

Структура курса состоит из четырех частей, соответствующих семестрам обучения. Каждая часть содержит тематический и грамматический модули. При этом в тематических модулях частей I–II преобладают слова и тексты общего характера, начиная с части III – идет углубленное изучение профессиональной тематики и работа с профессионально-ориентированными текстами.

Общая трудоемкость освоения дисциплины составляет 10 зачетных единиц, 360 часов. Преподавание дисциплины ведется на 1 и 2 курсах в 1-4 семестрах для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме зачета в 1 и 3 семестрах и в форме контрольной работы и экзамена во 2 и 4 семестрах в форме контрольной работы и экзамена для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Экономика информационной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.04 «Безопасность жизнедеятельности»

Дисциплина «Безопасность жизнедеятельности» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой управления качеством и стандартизации.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

ОК-4: способность использовать основы правовых знаний в различных сферах деятельности.

ОПК-6: способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях

чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности.

Целями изучения дисциплины являются: формирование профессиональной культуры безопасности, под которой понимается готовность и способность личности использовать в профессиональной деятельности приобретенную совокупность знаний, умений и навыков для обеспечения безопасности в сфере профессиональной деятельности; формирование, развитие и закрепление у студентов сложившихся в науке теоретических знаний и практических навыков, необходимых для оценки негативных воздействий среды обитания естественного, техногенного и антропогенного происхождения; разработка и реализация мер защиты человека от негативных воздействий; знание правового регулирования безопасности жизнедеятельности; основ управленческой деятельности для обеспечения устойчивости функционирования объектов и технических систем в штатных и чрезвычайных ситуациях.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 1 курсе в 1 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета во 1 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Физическая защита информационных объектов», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.05 «Русский язык и культура речи»

Дисциплина «Русский язык и культура речи» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой иностранных языков.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

ОК-7: способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности.

Курс русского языка и культуры речи нацелен на формирование и развитие у будущего бакалавра - участника профессионального общения комплексной коммуникативной компетенции на русском языке, представляющей собой совокупность знаний, умений, способностей, инициатив личности, необходимых для установления межличностного контакта в социально-культурной, профессиональной (учебной, научной, производственной и др.) сферах и ситуациях человеческой деятельности. Он предполагает знание литературных норм и умение применять их в речи.

Целью курса является формирование образцовой языковой личности высокообразованного бакалавра, речь которого соответствует принятым в образованной среде нормам, отличается выразительностью и красотой.

Структура курса предполагает рассмотрение основных понятий, связанных с русским языком и культурой речи.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 1 курсе в 1 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 1 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Основы управления информационной безопасностью», «Основы информационной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.06 «Основы управленческой деятельности»

Дисциплина «Основы управленческой деятельности» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой управления.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

ОК-6: способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия;

ПК-14: способность организовывать работу малого коллектива исполнителей в профессиональной деятельности.

Курс представляет собой изложение теоретических и практических основ современного менеджмента, рассмотрение основных понятий и направлений управленческой деятельности, принципов обеспечения и

организации планирования управления, подходов к принятию управленческих решений.

Целью курса является формирование понимания методов и функций управленческой деятельности, умения осуществлять постановку управленческих задач, обосновывать принятие решений, определять ресурсы для их выполнения, давать оценку эффективности управления в различных условиях функционирования объекта.

Структура курса предполагает рассмотрение основных понятий, связанных с управленческой деятельностью, концепций современных теорий управления, методов анализа управления, общей методики принятия управленческих решений.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 1 курсе в 1 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 1 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Основы управления информационной безопасностью», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.07 «Документоведение»

Дисциплина «Документоведение» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой управления.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

ОК-7: способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности;

ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности.

Содержание курса раскрывает вопросы, связанные с документированием правовой, управленческой, экономической, социальной, технической и научной информации, формированием систем документации,

защитой документированной информации, а также основами документационного обеспечения управления.

Целью курса является формирование понимания закономерностей образования документов и способов их создания, развития систем документации и систем документирования, рассмотрение документа как объекта защиты и нападения, усвоение технологии эффективного поиска информации по профилю деятельности.

Структура курса предполагает рассмотрение теоретических и прикладных аспектов документирования информации: свойств, функций и признаков документа, способов и средств документирования, структуры документа, порядка его составления и оформления, методов и способов защиты документа и документированной информации, классификации документов и систем документации, основ документационного обеспечения управления.

Общая трудоемкость освоения дисциплины 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 1 курсе в 1 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 1 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.08 «Экономика предприятия и организация производства»

Дисциплина «Экономика предприятия и организация производств» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой экономики.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

ОК-2: способность использовать основы экономических знаний в различных сферах деятельности;

ПК-7: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.

Содержание дисциплины охватывает круг вопросов, связанных с изучением закономерностей экономической жизни общества, способов

решения базовых экономических проблем в рамках экономических систем различных типов; основных микро- и макроэкономических подходов и особенностей их применения в России на современном этапе; закономерностей и принципов поведения экономических агентов в современной экономике; основных понятий, категорий и методов экономической теории; экономических законов и основных особенностей ведущих школ и направлений экономической науки.

Общая трудоемкость освоения дисциплины составляет 6 зачетных единицы, 216 часов. Преподавание дисциплины ведется на 1 курсе во 2 семестре и на втором курсе в 3 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета во 2 семестре и контрольной работы и экзамена в 3 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Экономика информационной безопасности», «Математическая логика и теория алгоритмов», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Блок Б1.Б.09 Группа учебных дисциплин (модулей)

«Математические основы обеспечения информационной безопасности»

Б1.Б.09.01 «Линейная алгебра и аналитическая геометрия»

Дисциплина «Линейная алгебра и аналитическая геометрия» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой математики и естественнонаучных дисциплин.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач.

Целью изучения дисциплины является: формирование способности к восприятию, обобщению и анализу информации; освоение необходимого математического аппарата, применяемого при решении различных профессиональных задач; формирование готовности применять методы

математического анализа и моделирования в профессиональной деятельности.

Содержание дисциплины охватывает круг вопросов, связанных с классическими разделами математики: линейная и векторная алгебра, аналитическая геометрия, дифференциальное и интегральное исчисления, теория функций многих переменных, дифференциальные уравнения и ряды.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 часов. Преподавание дисциплины ведется на 1-ом курсе, в 1-ом семестре, продолжительностью 16 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме контрольной работы и экзамена в 1-ом семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Криптографические методы защиты информации», «Математическая логика и теория алгоритмов», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.09.02 «Математический анализ»

Дисциплина «Математический анализ» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой математики и естественнонаучных дисциплин.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач.

Целью изучения дисциплины является: формирование способности к восприятию, обобщению и анализу информации; освоение необходимого математического аппарата, применяемого при решении различных профессиональных задач; формирование готовности применять методы математического анализа и моделирования в профессиональной деятельности.

Содержание дисциплины охватывает круг вопросов, связанных с классическими разделами математики: линейная и векторная алгебра, аналитическая геометрия, дифференциальное и интегральное исчисления, теория функций многих переменных, дифференциальные уравнения и ряды.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 часов. Преподавание дисциплины ведется на 1-ом курсе, во 2-ом семестре, продолжительностью 16 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме контрольной работы и экзамена во 2-ом семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Криптографические методы защиты информации», «Математическая логика и теория алгоритмов», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.09.03 «Теория графов»

Дисциплина «Теория графов» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой математики и естественнонаучных дисциплин.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач.

Целью изучения дисциплины является: формирование способности к восприятию, обобщению и анализу информации; освоение необходимого математического аппарата, применяемого при решении различных профессиональных задач; формирование готовности применять методы математического анализа и моделирования в профессиональной деятельности. Содержание дисциплины охватывает круг вопросов, связанных с классическими разделами математики: линейная и векторная алгебра, аналитическая геометрия, дифференциальное и интегральное исчисления, теория функций многих переменных, дифференциальные уравнения и ряды.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 2-ом курсе в 3 семестре, продолжительностью 16 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме контрольной работы и экзамена в 3 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Криптографические методы защиты информации», «Математическая логика и теория алгоритмов», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.09.04 «Теория информации»

Дисциплина «Теория информации» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Безопасность жизнедеятельности», «Экономика предприятия и организация производства», «Документоведение», «Математический анализ» и компетенциях: ОК-2,4,7; ОПК-2,5,6; ПК-7.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач;

ПК-11: способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов.

Курс освещает вопросы, связанные с теоретическими и практическими аспектами теории информации, в частности с формированием практических навыков по применению методов теории информации для защиты информации в компьютерных системах.

Целью курса является приобретение навыков работы с понятиями теории информации и её использования в информационной безопасности; формирование умения применять алгоритмы эффективного, помехозащищенного и криптографического кодирования; формирование понимания сути информационных процессов в системах передачи, хранения и преобразования данных.

Содержание курса охватывает основные понятия теории информации, необходимые для использования защиты информации в компьютерных системах, а именно: понятие информации, подходы к измерению информации, свойства меры информации, характеристики канала связи, понятие кодирования, алгоритмы кодирования (эффективное кодирование, помехозащищенное кодирование, криптографическое кодирование). Рассматриваются коды Шеннона-Фэно, Хаффмана, блочные помехозащищенные коды, совершенные и квазисовершенные помехозащищенные коды; вопросы шифрования с симметричным и несимметричным ключом.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа. Преподавание дисциплины ведется на 2 курсе в 3 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета с оценкой в 3 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Техническая защита информации», «Физическая защита информационных объектов», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.09.05 «Теория вероятностей и математическая статистика»

Дисциплина «Теория вероятностей и математическая статистика» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой математики и естественнонаучных дисциплин.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Математический анализ», «Информатика» и компетенциях: ОПК-2,4.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач.

Содержание дисциплины охватывает круг вопросов, связанных со случайными явлениями, которые носят массовый характер и раскрывает основные понятия и теоремы теории вероятностей с характеристикой наиболее важных законов распределения случайных величин, применением статистических методов оценивания параметров распределений, владением техникой проверки статистических гипотез.

Цель курса: сформировать базовые представления о теории вероятностей и математической статистике под углом зрения их практического приложения в различных областях научных исследований по направлению подготовки.

Содержание курса состоит из двух разделов. В разделе «Теория вероятностей» рассматриваются алгебра событий, вероятностное пространство, основные теоремы теории вероятностей, одномерные случайные величины, числовые характеристики случайных величин, основные распределения случайных величин, многомерные случайные

величины и их числовые характеристики, функции случайных величин и предельные теоремы.

В разделе «Математическая статистика» рассматриваются выборочный метод, оценки параметров распределения, статистическая проверка гипотез, теория корреляции, однофакторный дисперсионный анализ, метод статистических испытаний.

Общая трудоемкость освоения дисциплины составляет 6 зачетных единиц, 216 часов. Преподавание дисциплины ведется на 2 курсе в 3-4 семестрах для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 3 семестре и в форме контрольной работы и экзамена в 4 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Криптографические методы защиты информации», «Экономика информационной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.09.06 «Дискретная математика»

Дисциплина «Дискретная математика» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой математики и естественнонаучных дисциплин.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Математический анализ», «Теория вероятностей и математическая статистика», «Теория информации» и компетенциях: ОПК-2; ПК-11.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач.

Содержание дисциплины охватывает базовые знания основных понятий дискретной математики и формулировки основных теорем.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 5 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Криптографические методы защиты информации», «Экономика информационной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

**Блок Б1.Б.10 Группа учебных дисциплин (модулей)
«Физико-технические основы
обеспечения информационной безопасности»**

Б1.Б.10.01 «Физика»

Дисциплина «Физика» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой математики и естественнонаучных дисциплин.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Математический анализ», «Информатика», «Экономика предприятия и организация производства» и компетенциях: ОК-2, ОПК-1,2,4 и ПК-7.

Дисциплина направлена на формирование следующих компетенций:

ОК-8: способность к самоорганизации и самообразованию;

ОПК-1: способность анализировать физические явления и процессы для решения профессиональных задач;

ПК-11: способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов.

Содержание дисциплины охватывает круг вопросов, связанных с классическими разделами физики: механика, молекулярная физика и термодинамика, электродинамика, оптика, так и с современными: специальная теория относительности, квантовая механика и изложение на их основе элементов квантовой оптики, атомной и ядерной физики, а также элементов физики твердого тела.

Общая трудоемкость освоения дисциплины составляет 6 зачетных единиц, 216 часов. Преподавание дисциплины ведется на 1-2 курсах в 2-3 семестрах для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (решения задач и лабораторные работы), самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в

форме контрольной работы и зачета во 2 семестре и контрольной работы и экзамена в 3 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организационное и правовое обеспечение информационной безопасности», «Электротехника», «Электроника и схемотехника», «Физическая защита информационных объектов», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.10.02 «Электротехника»

Дисциплина «Электротехника» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Физика», «Математический анализ», «Теория вероятностей и математическая статистика» и компетенциях: ОК-8; ОПК-1,2; ПК-11.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач;

ОПК-3: способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач.

Курс охватывает вопросы, связанные с анализом и расчетом электрических цепей различной сложности, а также изучением современных методов расчета электрических цепей, основанных на компьютерных технологиях.

Целью курса является формирование понимания аналитических и машинных методов расчета электрических цепей, изучение физических явлений и эффектов, имеющих в современной электронной аппаратуре и их учета при защите информации.

Курс объединяет ряд логически связанных разделов. Первый - базируется на разделе «электростатика» курса физики, и раскрывает методы расчета электрических цепей постоянного тока. Во втором и третьем разделах рассматриваются цепи переменного тока с синусоидальными и импульсными источниками. В последующих разделах анализируются цепи с нелинейными и многополюсными элементами (диоды, транзисторы, операционные усилители), применяемыми в современной электронной аппаратуре.

Общая трудоемкость освоения дисциплины 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 2 курсе в 4 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (решения задач и лабораторные работы), самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 4 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Программно-аппаратные средства защиты информации», «Криптографические методы защиты информации», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», «Радиоэлектронные системы и средства как объекты информационной безопасности», «Основы радиоэлектронной разведки (РЭР)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.10.03 «Электроника и схемотехника»

Дисциплина «Электроника и схемотехника» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Физика», «Математический анализ», «Теория вероятностей и математическая статистика», «Электротехника» и компетенциях: ОК-8;ОПК-1,2,3;ПК-11.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач;

ОПК-3: способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач.

Курс охватывает вопросы, связанные с функционированием типовых аналоговых и цифровых электронных устройств. В лабораторном практикуме курса применяется компьютерная симуляция - программными средствами моделируется техническая задача и на этой основе отрабатываются различные варианты технических решений.

Целью курса является изучение принципов действия и особенностей применения типовых аналоговых и цифровых электронных устройств в современных технических средствах.

Курс объединяет ряд разделов. Первый раздел вводит в основы современной полупроводниковой электроники. Во втором разделе рассматриваются полупроводниковые приборы - транзисторы. В третьем разделе изучаются усилительные схемы, принципы и особенности их работы. В четвертом разделе изучается операционный усилитель, применяемый в различных областях схемотехники. В последнем разделе рассмотрено применение транзисторов в цифровой технике.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 5

семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (решения задач и лабораторные работы), самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 5 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Программно-аппаратные средства защиты информации», «Криптографические методы защиты информации», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», «Радиоэлектронные системы и средства как объекты информационной безопасности», «Основы радиоэлектронной разведки (РЭР)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Блок Б1.Б.11 Группа учебных дисциплин (модулей) «Информационные технологии»

Б1.Б.11.01 «Информатика»

Дисциплина «Информатика» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач;

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.

Курс освещает вопросы, связанные с систематизацией теоретических знаний и практических приемов создания, хранения, обработки и передачи информации с использованием средств вычислительно-коммуникационной техники.

Целью курса является изучение теоретических основ информатики, приобретение практических знаний в области использования автоматизированных информационных систем.

Содержание курса охватывает вопросы изучения основных понятий информатики (информация, автоматика, информационные процессы, системы и технологии); аспектов моделирования и представления

информации и алгоритмизации информационных процессов; сущности и классификации информационных технологий; базовых информационно-коммуникационных технологий обработки и передачи информации. В прагматическую составляющую курса включены вопросы изучения: способов представления и преобразования информации в вычислительных системах, в том числе, структур их файловых систем; использования и настройки интерфейса операционных систем; основ работы с универсальными пакетами офисных приложений - текстового процессора, электронных таблиц и презентаций; способов обмена данными между приложениями; интерфейса и принципов работы систем управления базами данных; способов коммуникации, навигации и поиска информации в распределенных информационно- вычислительных сетях.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 часа. Преподавание дисциплины ведется на 1 курсе в 1 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (решения задач и лабораторные работы), самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 1 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Программно-аппаратные средства защиты информации», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.11.02 «Языки программирования»

Дисциплина «Языки программирования» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Математический анализ», «Теория вероятностей и математическая статистика», «Теория информации» и компетенциях: ОПК-2 и ПК-11.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач;

ПК-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач.

Курс направлен на изучение объектно-ориентированных языков программирования семейства С (С++, С#) и охватывает круг вопросов, связанных с понятиями объектно-ориентированного программирования, абстрактного типа данных, объекта, метода, функции, наследования, инкапсуляции, класса, конструкторов и деструкторов, потоков ввода-вывода, виртуальных функций.

Целью курса является формирование компетенций в области использования современных промышленных языков программирования и средств разработки программного обеспечения для решения прикладных задач информационной безопасности на базе объектно-ориентированного подхода.

Содержание курса охватывает особенности объектно-ориентированных языков программирования, их достоинства и недостатки; включает основные элементы С++ (базовые структуры и типы данных, виды доступа, классы и объекты, техника указателей, базовые классы и указатели, производные классы: иерархия наследования, виртуальные функции и абстрактные классы, динамическое распределение памяти, потоки ввода / вывода, конструкторы и деструкторы, функции-друзья, обобщение операторов определения), и механизмы их использования (работа с файлами, вызов конструкторов функций оператора сложения, конверсия, программирование команд меню); отражает современные тенденции в развитии языка С++ (универсальные платформы Microsoft.NET и технологии программирования Microsoft.NET Framework) и характерные особенности языка С# (система типов, делегаты, события, интерфейсы, атрибуты, механизм сериализации и классы-коллекции).

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Преподавание дисциплины ведется на 2 курсе в 4 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 4 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Программно-аппаратные средства защиты информации», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.11.03 «Технологии и методы программирования»

Дисциплина «Технологии и методы программирования» относится к базовой части основной профессиональной образовательной программы

подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Математический анализ», «Теория вероятностей и математическая статистика», «Теория информации», «Языки программирования» и компетенциях: ОПК-2,7 и ПК-2,11.

Дисциплина направлена на формирование следующих компетенций:

ОПК-7: способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

ПК-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач.

Курс направлен на изучение современных методов и технологий программирования, поддерживающих процесс программирования на всех этапах конструирования и жизненного цикла программной системы (ПС) и базирующихся на методологии структурного анализа и проектирования программных средств и объектно-ориентированного анализа предметной области.

Целью курса является формирование компетенций студентов в области основных технологий и методов программирования, применяемых при разработке современных ПС; усвоение теоретических знаний, связанных с проектированием, спецификацией, разработкой, тестированием и отладкой ПС, а также документированием приложений; приобретение практических навыков в области использования технологий программирования (кодирование, отладка и тестирование) в конкретных приложениях; формирование представлений о принципах и методах программирования в современных языках: модульности, структурности, композиции и декомпозиции.

Содержание курса охватывает следующие основные вопросы: модели жизненного цикла ПС, спецификация программ, структурный подход к проектированию ПС, модульное программирование, основные характеристики и организация программного модуля, нисходящий и восходящий методы конструирования ПС, разработка интерфейса пользователя, тестирование ПС, автономная и комплексная отладка ПС, показатели качества ПС, основные парадигмы и методы программирования, эволюция языков программирования, методы представления знаний и данных в ПС, абстрагирование типов и инкапсуляция, полиморфизм, перекрытие и перегрузка методов, внутренняя организация объекта, таблицы динамических и виртуальных методов, технологии документирования и стандартизации ПС, современные CASE-технологии проектирования ПС, системы UML-моделирования.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 5 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Программно-аппаратные средства защиты информации», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.11.04 «Информационные технологии»

Дисциплина «Информационные технологии» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Теория вероятностей и математическая статистика», «Теория информации», «Языки программирования», «Технологии и методы программирования», «Аппаратные средства вычислительной техники», «Сети и системы передачи информации» и компетенциях: ОПК-2,4,7 и ПК-2,3,11.

Дисциплина направлена на формирование следующих компетенций:

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-7: способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

ПК-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

ПК-3: способность администрировать подсистемы информационной безопасности объекта защиты.

Курс ориентирован на теоретическое изучение и практическое освоение основных классов современных информационно-коммуникационных технологий по осваиваемым профилям подготовки.

Целью курса является формирование компетенций в области выбора, адаптации, использования и синтеза информационно-коммуникационных технологий, обеспечивающих функционирование информационных систем в рамках заданной политики безопасности.

Содержание курса охватывает классы современных компьютерных (автоматизированных) информационно-коммуникационных технологий общего назначения, в том числе, управления и принятия решений, системного анализа, формирования и использования коллективных источников знаний, массовых вычислений и моделирования, проектирования и разработки информационных систем, поддержки образовательного процесса и научных исследований.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 5 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Криптографические методы защиты информации», «Программно-аппаратные средства защиты информации», «Разработка политики информационной безопасности в организациях», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.11.05 «Аппаратные средства вычислительной техники»

Дисциплина «Аппаратные средства вычислительной техники» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Математический анализ», «Теория вероятностей и математическая статистика», «Теория информации», «Языки программирования», «Технологии и методы программирования» и компетенциях: ОПК-2,5; ПК-2,11.

Дисциплина направлена на формирование следующих компетенций:

ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности;

ПК-1: способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

ПК-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач.

Предметом учебного курса являются вопросы, связанные с устройством и функционированием аппаратных средств вычислительной техники.

Целью курса является приобретение знаний и умений, необходимых для деятельности, связанной с эксплуатацией и обслуживанием современных средств вычислительной техники, а также подготовка обучаемых к грамотному и эффективному использованию компьютера как инструмента решения задач различной степени сложности в области информационной безопасности.

Содержание курса охватывает следующие вопросы: арифметические и логические основы цифровых машин, элементы и узлы ЭВМ, принцип программного управления и микропроцессоры, периферийные устройства ЭВМ, архитектура и принцип работы ПЭВМ, основы построения компьютерных сетей.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (решения задач и лабораторные работы), самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 6 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Программно-аппаратные средства защиты информации», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Криптографические методы защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.11.06 «Сети и системы передачи информации»

Дисциплина «Сети и системы передачи информации» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Математический анализ», «Теория вероятностей и математическая статистика», «Теория информации», «Языки

программирования», «Технологии и методы программирования», «Аппаратные средства вычислительной техники» и компетенциях: ОПК-2,5,7 и ПК-1,2,11.

Дисциплина направлена на формирование следующих компетенций:

ОПК-7: способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

ПК-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач.

Курс ориентирован на теоретическое изучение и практическое освоение принципов построения и применения современных сетей и систем передачи данных.

Целью курса является формирование знаний в области выбора, анализа и применения сетей и систем передачи данных.

Содержание курса охватывает основные понятия и определения передачи информации, эталонную модель взаимодействия открытых систем (модель ISO/OSI), модель TCPDP, архитектуру и средства взаимодействия процессов в сетях, основные принципы построения и современные тенденции развития сетей. Рассматривается архитектура и топологии построения современных ЛВС, технологии Ethernet (FastEthernet, GigabitEthernet), TokenRing, FDDI - стандарты, принципы работы, сравнительные характеристики, преимущества и недостатки, основные средства построения современных ЛВС, классификации, внутренняя архитектура, режимы работы, протоколы сетевого уровня модели ISO/OSI. Изучаются основы организации и функционирования, архитектура и принципы построения сети Internet, протоколы маршрутизации, кроме того - мультисервисные сети, особенности построения таких сетей, технологии передачи голосового трафика VoIP, IP-телефония.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 часов. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (решения задач и лабораторные работы), самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 6 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Криптографические методы защиты информации», «Информационная безопасность автоматизированных систем», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

**Блок Б1.Б.12 Группа учебных дисциплин (модулей)
«Методы и средства обеспечения информационной безопасности»**

Б1.Б.12.01 «Основы информационной безопасности»

Дисциплина «Основы информационной безопасности» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Информатика», «Введение в профессию», «Основы исследований информационной безопасности» и компетенциях: ОК-5; ОПК-2,4,5,7; ПК-8,9,11,12.

Дисциплина направлена на формирование следующих компетенций:

ОК-5: способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.

Содержание дисциплины охватывает круг вопросов, связанных с сущностью и значением информационной безопасности, её местом в системе национальной безопасности, определением теоретических, концептуальных, методологических и организационных основ обеспечения безопасности объектов информатизации, анализом методов и средств защиты информации.

Целью курса является формирование знаний о совокупности проблем в сфере науки, техники и технологий, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере, понимания основных принципов, направлений и методов обеспечения информационной безопасности.

В курсе изучаются понятийный аппарат и базовые положения законодательных и нормативных документов по информационной безопасности; рассматриваются сущность и содержание информационной безопасности, её место в системе национальной безопасности, основные требования по обеспечению информационной безопасности государства, общества, личности; раскрываются объекты безопасности, состав защищаемой информации, структура угроз информации, средства обеспечения безопасности, направления, виды и методы деятельности по обеспечению информационной безопасности, а также основные задачи государственной системы (органов) защиты информации.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 часа. Преподавание дисциплины ведется на 1-2 курсе в 2-3 семестрах для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета во 2 семестре и в форме контрольной работы и зачета с оценкой в 3 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организационное и правовое обеспечение информационной безопасности», «Техническая защита информации», «Основы управления информационной безопасностью», «Организация защиты персональных данных на предприятии», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.12.02 «Организационное и правовое обеспечение информационной безопасности»

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Информатика», «Введение в профессию», «Основы исследований информационной безопасности», «Основы информационной безопасности» и компетенциях: ОК-4,5, ОПК-2,4,5,7 и ПК-8,9,10,11,12.

Дисциплина направлена на формирование следующих компетенций:

ОК-4: способность использовать основы правовых знаний в различных сферах деятельности;

ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности;

ПК-8: способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

ПК-10: способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;

ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Курс охватывает круг вопросов, связанных с целями, функциями и структурой правового обеспечения информационной безопасности и обеспечивающих ее мер и средств правовой защиты информации, структурой законодательства в информационной сфере.

Целью курса (1 часть) является приобретение знаний по основным положениям законодательства и нормативным правовым актам в области информационной безопасности, умения определять направления развития и совершенствования правового обеспечения в информационной сфере, а также формирование навыков использования законодательных и нормативно-методических документов, организационно-правовых мер и средств по обеспечению защиты информации.

Целью курса (2 часть) является приобретение умения формировать системы организационной защиты информации, анализировать эффективность и разрабатывать направления развития таких систем; подготавливать нормативно-методические документы по регламентации организационного обеспечения информационной безопасности; организовывать охрану объектов и носителей; вести работу с персоналом, владеющим конфиденциальной информацией.

Содержание курса (1 часть) раскрывает информационная сфера как объект правовых отношений, дает понятие тайны (государственной, коммерческой, служебной, профессиональной), как правового режима ограничения доступа к информации, рассматривает особенности правового регулирования отношений в сфере обращения информации о персональных данных граждан, а также основные положения гражданского законодательства о правах на результаты интеллектуальной деятельности и средства индивидуализации, правовые нормы сертификации средств защиты информации и правовое регулирование лицензионной деятельности в области защиты информации, вопросы о Курс освещает вопросы, связанные с теоретическими и практическими проблемами создания и функционирования систем организационного обеспечения информационной безопасности, а также формированием практических навыков по организационной защите информации, рассматриваются вопросы определения стратегических целей организационного обеспечения информационной безопасности, основанное на анализе внутренних и внешних факторов угроз; установление приоритетов и последовательности решения задач, привлечение и распределение ресурсов организации, основанные на методах программно-целевого планирования.

Содержание курса (2 часть) предусматривает изучение сущности организационного обеспечения информационной безопасности, организацию работы по ограничению доступа к информации, лицензированию деятельности предприятий в области защиты информации, вопросам кадрового обеспечения и допуска граждан к государственной тайне, организационные аспекты деятельности персонала по защите информации, регламентацию системы доступа к защищаемой информации, организацию пропускного и внутри объектового режимов, организационные требования к

режимным помещениям, организацию совещаний (переговоров), издательской, рекламно-выставочной деятельности, проведение внутренних расследований по конфиденциальным вопросам

Общая трудоемкость освоения дисциплины составляет 5 зачетных единиц, 180 часов. Преподавание дисциплины ведется на 2 курсе в 4 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме экзамена в 4 семестре и курсовой работы для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины «Криптографические методы защиты информации», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», «Лицензирование и сертификация в области защиты информации», являются базовыми для изучения всех последующих дисциплин, прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.12.03 «Основы управления информационной безопасностью»

Дисциплина «Основы управления информационной безопасностью» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Информатика», «Основы информационной безопасности», «Математический анализ» и компетенциях: ОК-5; ОПК-2,3,4,7 и ПК-3,6.

Дисциплина направлена на формирование следующих компетенций:

ОПК-7: способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

ПК-13: способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.

Содержание дисциплины охватывает вопросы, связанных с изучением сущности и стандартных процедур управления безопасностью объектов информационной инфраструктуры, анализом методов и систем управления информационной безопасностью, требований к аудиту систем управления защитой информации.

Целью курса является формирование знаний по основам управления информационной безопасностью предприятия (организации) и методам повышения эффективности системы управления безопасностью объекта информатизации.

Структура курса раскрывает требования международных и российских стандартов по информационной безопасности, классификацию систем управления, меры и средства управления информационной безопасностью, этапы внедрения систем управления, а также аудит и оценку эффективности систем управления информационной безопасностью предприятия (организации).

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольная работа и зачета в 5 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Эффективность защищенных информационных систем», «Социотехносферная безопасность объектов информационной защиты», «Правовая охрана результатов интеллектуальной деятельности», «Разработка политики информационной безопасности в Интернет-системах», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.12.04 «Техническая защита информации»

Дисциплина «Техническая защита информации» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Информатика», «Введение в профессию», «Основы исследований информационной безопасности», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности» и компетенциях: ОК-4,5; ОПК-2,4,5,7; ПК-3,5,6,8,9,10,11,12,15.

Дисциплина направлена на формирование следующих компетенций:

ОПК-4: способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ПК-3: способностью администрировать подсистемы информационной безопасности объекта защиты;

ПК-5: способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;

ПК-6: способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

ПК-12: способность принимать участие в проведении экспериментальных исследований системы защиты информации.

В курсе освещены вопросы, связанные с анализом возможных технических каналов утечки информации и защиты объектов информатизации техническими способами и средствами, в том числе, проведение специальных исследований, обследований и специальных проверок.

Целью курса является рассмотрение возникновения технических каналов утечки информации и возможности защиты информации техническими средствами.

В курсе рассматриваются объекты информационной защиты, виды угроз информации, вопросы образования технических каналов утечки информации, способы преднамеренного воздействия на информацию, способы добывания информации злоумышленником, методы и способы защиты информации техническими средствами защиты.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часов. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (решения задач и лабораторные работы), курсовая работа, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме экзамена в 6 семестре и курсовой работы для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Нормативные акты и стандарты по информационной безопасности», «Аттестация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.12.05 «Криптографические методы защиты информации»

Дисциплина «Криптографические методы защиты информации» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Аппаратные средства вычислительной техники», «Языки программирования», «Информатика», «Основы информационной безопасности», «Математический анализ», «Основы управления информационной безопасностью» и компетенциях: ОК-5; ОПК-2,3,4,5,7; ПК-1,2,4,7,13.

Дисциплина направлена на формирование следующих компетенций:

ОПК-3: способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач;

ПК-1: способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

ПК-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

ПК-7: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.

В курсе в систематизированном виде излагаются вопросы обеспечения безопасности каналов передачи информации, систем электронных платежей, электронного документооборота с использованием криптографических методов.

Целью курса является приобретение знаний о базовых криптографических системах и схемах, их основных параметрах и умений применять на практике имеющиеся криптографические средства.

Содержание курса охватывает общетеоретические вопросы криптографической защиты информации и практики применения ее методов и средств в современных информационных системах, синтеза и анализа криптографических протоколов, закономерности построения сложных криптосистем, а также конкретные виды базовых криптографических протоколов и схем, получивших широкое применение в качестве инструментария для создания систем электронных платежей и систем документооборота в электронной коммерции.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (лабораторные работы), самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 7 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Комплексное обеспечение

защиты информации объекта информатизации (предприятия)», «Экономика информационной безопасности», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.12.06 «Программно-аппаратные средства защиты информации»

Дисциплина «Программно-аппаратные средства защиты информации» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Аппаратные средства вычислительной техники», «Языки программирования», «Информатика», «Основы информационной безопасности», «Математика», «Основы управления информационной безопасностью», «Криптографические методы защиты информации» и компетенциях: ОК-5; ОПК-2,3,4,5,7; ПК-1,2,4,6,7,9,13.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач;

ПК-1: способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

ПК-6: способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

ПК-9: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.

Предмет курса - механизмы и практические методы защиты информации в автономных и распределенных компьютерных системах.

Цель курса - формирование знаний о современных средствах защиты информации в компьютерных системах, овладение методами решения профессиональных задач, умения ориентироваться в продуктах и тенденциях развития средств защиты информационных технологий.

В рамках курса рассматриваются основные понятия программно-аппаратной защиты информации, уязвимости компьютерных систем, политики безопасности в компьютерных системах, вопросы оценки защищенности, базовые сервисы безопасности (идентификация и аутентификация субъектов доступа, регистрация событий и аудит, механизмы контроля целостности информации), функции безопасности ОС

WINDOWS, функции безопасности ОС UNIX, разграничение доступа в СУБД, особенности защиты информации в распределенных системах, аппаратно-программные средства защиты информации (СЗИ и СКЗИ «Secret Net»), средства аппаратной поддержки (смарт-карты, гмб-токены и т.п.), сетевые угрозы, уязвимости и атаки, средства обнаружения уязвимостей, межсетевые экраны, виртуальные частные сети (VPN), безопасность уровня сетевого взаимодействия.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (лабораторные работы), курсовая работа, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме экзамена в 7 семестре и курсовой работы для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Экономика информационной безопасности», «Лицензирование и сертификация в области защиты информации», «Аттестация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.12.07 «Комплексное обеспечение защиты информации объекта информатизации (предприятия)»

Дисциплина «Комплексное обеспечение защиты информации объекта информатизации (предприятия)» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Аппаратные средства вычислительной техники», «Языки программирования», «Информатика», «Основы информационной безопасности», «Математический анализ», «Основы управления информационной безопасностью», «Криптографические методы защиты информации» и компетенциях: ОК-5, ОПК-2,3,4; ПК-1,2,4,7,13.

Дисциплина направлена на формирование следующих компетенций:

ОК-5: способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;

ОПК-7: способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их

реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

ПК-10: способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;

ПСК-1: способность проводить совместный анализ функционального процесса защиты ТКС и ее информационных составляющих с целью определения возможных источников угроз, их вероятных целей;

ПСК-3: способность организовывать контроль и анализ защищенности объектов ТКС в соответствии с нормативными документами.

Целями изучения дисциплины являются: дать студентам знания по организации целесообразных мероприятий по защите информации на предприятиях (организациях и учреждениях) с различными формами собственности с учетом современных требований в области теории обеспечения информационной безопасности на основе комплексного подхода; выработать и закрепить у студентов базовые умения и навыки по практической организации и реализации современных технологий защиты информации на предприятиях (организациях и учреждениях) с различными формами собственности с учетом современных международных и отечественных стандартов информационной безопасности.

Общая трудоемкость освоения дисциплины составляет 8 зачетных единиц, 288 часов. Преподавание дисциплины ведется на 4 курсе в 7-8 семестрах для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, курсовая работа, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме зачета в 7 семестре и в форме экзамена в 8 семестре и курсовой работы для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

**Блок Б1.Б.13 Дисциплины (модули) профиля:
«Безопасность телекоммуникационных систем (в аэрокосмической
сфере)»**

**Б1.Б.13.01 «Устройства формирования и передачи сигналов в
телекоммуникационных системах»**

Дисциплина «Устройства формирования и передачи сигналов в телекоммуникационных системах» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на ранее изученных дисциплинах группы «Физико-технические основы обеспечения информационной безопасности»: «Физика», «Электротехника», «Электроника и схемотехника» и компетенциях: ОК-8; ОПК-1; ОПК-2; ОПК-3; ПК-11.

Дисциплина направлена на формирование следующих компетенций:

ОК-8; ОПК-2; ПК-2; ПСК-1.

ОК-8: способность к самоорганизации и самообразованию;

ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач;

ПК-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

ПСК-1: способность проводить совместный анализ функционального процесса защиты ТКС и ее информационных составляющих с целью определения возможных источников угроз, их вероятных целей.

Курс рассматривает основные понятия современных сетей и систем передачи информации и средства их защиты как основы для проектирования ТКС.

Целью курса является изучение принципов построения и эксплуатации различных основных элементов телекоммуникационных сетей и систем и методов их компьютерного моделирования, а также современных технических средств, применяемых при построении ТКС.

Содержание курса включает рассмотрение таких вопросов как первичные сигналы электросвязи, каналы передачи информации, общие принципы формирования и передачи сигналов в цифровых системах и особенности работы систем передачи с временным и частотным разделением каналов, разностные методы кодирования, иерархия цифровых систем передачи.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 2 курсе 4 семестре для очной и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 4 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Системы аэрокосмической и наземной подвижной связи», «Беспроводные системы связи и их безопасность», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.13.02 «Устройства приема и обработки сигналов в телекоммуникационных системах»

Дисциплина «Устройства приема и обработки сигналов в телекоммуникационных системах» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах группы «Физико-технические основы обеспечения информационной безопасности»: «Физика», «Электротехника», «Электроника и схемотехника» и компетенциях: ОК-8; ОПК-1; ОПК-2; ОПК-3; ПК-11.

Дисциплина направлена на формирование следующих компетенций:

ОК-5: способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;

ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач;

ОПК-3: способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач;

ПК-3: способность администрировать подсистемы информационной безопасности объекта защиты;

ПК-6: способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

ПСК-1: способность проводить совместный анализ функционального процесса защиты ТКС и ее информационных составляющих с целью определения возможных источников угроз, их вероятных целей.

Курс освещает вопросы, связанные с исследованием, разработкой, созданием и эксплуатацией ТКС, технологиями приема и обработки информации.

Целью курса является формирование понимания основ физических процессов, теории и принципов построения и функционирования устройств приема и обработки сигналов, используемых в различных телекоммуникационных системах.

Содержание курса включает изучение характеристик радиоприемных устройств, усилителей и преобразователей радиочастот, детекторов сигналов и электромагнитных помех.

Рассматриваются методы цифровой фильтрации, корреляционный анализ и случайные сигналы. Излагаются основные вопросы построения цифровых фильтров адаптивной обработки сигналов.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 часов. Преподавание дисциплины ведется на 2 курсе в 3-4 семестрах для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 3 семестре и в форме экзамена в 4 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин «Системы аэрокосмической и наземной подвижной связи», «Беспроводные системы связи и их безопасность», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.13.03 «Сетевые технологии»

Дисциплина «Сетевые технологии» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Математическая логика и теория алгоритмов» и компетенциях: ОК-4, ОПК-5 и ПК-6,9.

Дисциплина направлена на формирование следующих компетенций:

ОК-4: способность использовать основы правовых знаний в различных сферах деятельности;

ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности;

ПК-6: способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

ПК-9: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

ПСК-1: способность проводить совместный анализ функционального процесса защиты ТКС и ее информационных составляющих с целью определения возможных источников угроз, их вероятных целей;

ПСК-2: способность формировать предложения по оптимизации функционального процесса и его компонентов с целью повышения их

устойчивости к деструктивным воздействиям на информационные ресурсы и меры по информационной защите ТКС;

ПСК-4: способность организовать реализацию принятых мер по управлению защитой информационных потоков на пакетном уровне с комплексной оценкой информационной безопасности ТКС.

Предмет изучения курса - проблемы построения и совершенствования распределенных компьютерных систем и протоколов по сферам применения и анализ вопросов аппаратно-программного и организационного обеспечения работы распределенных компьютерных систем.

Цель курса – освоение принципов, методов, и технологий построения локальных, территориальных и глобальных компьютерных сетей и информационных систем, а также изучение обобщенных технических решений по компьютерным сетям и распределенным системам обработки информации.

Содержание курса включает рассмотрение современных корпоративных вычислительных сетей и их основных характеристик. Изучаются вопросы управления функционированием и безопасностью сети, а также современные технологии защиты корпоративных сетей.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (лабораторные работы), самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 5 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Беспроводные системы связи и их безопасность», «Проектирование элементов защищенных ТКС», «Нормативные акты и стандарты по информационной безопасности», «Математическое моделирование защищенных систем ТКС», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.13.04 «Защита информации в телекоммуникационных системах»

Дисциплина «Защита информации в телекоммуникационных системах» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности» и компетенциях: ОК-4,5, ОПК-2,3,4,5 ПК-6,8,10,15.

Дисциплина направлена на формирование следующих компетенций:

ОК-9: способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности;

ОПК-1: способность анализировать физические явления и процессы для решения профессиональных задач;

ОПК-6: способность применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности;

ПК-1: способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.

ПСК-1: способность проводить совместный анализ функционального процесса защиты ТКС и ее информационных составляющих с целью определения возможных источников угроз, их вероятных целей;

ПСК-3: способность организовывать контроль и анализ защищенности объектов ТКС в соответствии с нормативными документами

ПСК-4: способность организовать реализацию принятых мер по управлению защитой информационных потоков на пакетном уровне с комплексной оценкой информационной безопасности ТКС.

Целью дисциплины является изучение методов и средств защиты информации в телекоммуникационных системах.

Дисциплина включает в себя рассмотрение направлений обеспечения информационной безопасности телекоммуникационных систем, телекоммуникационных систем и сетей связи как объектов защиты, рекомендаций и требований законодательства Российской Федерации в области обеспечения информационной безопасности телекоммуникационных систем, вопросов администрирования аппаратных, программных и программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (лабораторные работы), самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 5 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность операционных систем и баз данных», «Защита общества от информации, запрещенной к распространению», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.13.05 «Системы аэрокосмической и наземной подвижной связи»

Дисциплина «Системы аэрокосмической и наземной подвижной связи» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Математическая логика и теория алгоритмов» и компетенциях: ОК-4,5, ОПК-4,5, ПК-8,10,15 и ПСК-2.

Дисциплина направлена на формирование следующих компетенций:

ОК-4: способность использовать основы правовых знаний в различных сферах деятельности;

ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности;

ПК-5: способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;

ПК-8: способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

ПК-13: способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;

ПСК-2: способность формировать предложения по оптимизации функционального процесса и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов;

ПСК-4: способность организовать реализацию принятых мер по управлению защитой информационных потоков на пакетном уровне с комплексной оценкой информационной безопасности ТКС.

Целями курса являются:

– формирование знаний о принципах построения систем спутниковой и наземной подвижной связи, навигации, орбитах спутников, применяемых в системах связи и навигации, возможностях, структуре, технических

характеристиках бортовых и наземных командно-измерительных систем управления, методах передачи сообщений в спутниковых системах, методах и средствах информационной безопасности телекоммуникаций космических и наземных систем;

– формирование умений в оценке основных проблем защищенного телеуправления космическими аппаратами, определении основных параметров и структур информационных сообщений космических систем, оценке реальных и предельных возможностей пропускной способности, помехоустойчивости и информационной безопасности телеуправления космическими аппаратами, записи математических моделей сигналов при различных видах модуляции.

Содержание дисциплины несет в себе информацию о принципах построения систем спутниковой связи и навигации, орбитах спутников, применяемых в системах связи и навигации, методах передачи сообщений в спутниковых системах, отечественных и зарубежных стандартах взаимодействия космических и наземных систем, методах и средствах информационной безопасности телекоммуникаций космических и наземных систем.

По итогам изучения дисциплины студенты способны оценивать основные проблемы защищенного телеуправления космическими аппаратами, основные параметры и структуры информационных сообщений космических систем, оценивать реальные и предельные возможности пропускной способности, помехоустойчивости и информационной безопасности телеуправления космическими аппаратами, записывать математические модели сигналов при различных видах модуляции.

Также приобретаются навыки применения математического аппарата к анализу непрерывных, дискретных и цифровых сигналов и систем, и формирования команд управления космическим аппаратами и обработки телеметрической информации.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета с оценкой в 7 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Экономика информационной безопасности», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Лицензирование и сертификация в области защиты информации», «Аттестация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.13.06 «Беспроводные системы связи и их безопасность»

Дисциплина «Беспроводные системы связи и их безопасность» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Математическая логика и теория алгоритмов» и компетенциях: ОК-4,5,8, ОПК-4; ПК-8,10,15 и ПСК-2.

Дисциплина направлена на формирование следующих компетенций:

ОК-5: способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;

ОК-8: способность к самоорганизации и самообразованию;

ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

ПК-7: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;

ПК-9: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

ПСК-2: способность формировать предложения по оптимизации функционального процесса и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов;

ПСК-4: способность организовать реализацию принятых мер по управлению защитой информационных потоков на пакетном уровне с комплексной оценкой информационной безопасности ТКС.

Цель преподавания дисциплины «Беспроводные системы связи и их безопасность» состоит в том, чтобы дать студентам общее понимание задач защиты информации, решаемых в системах мобильной связи различных типов.

Содержание дисциплины предусматривает изучение принципов построения систем сотовой связи, поколений мобильной связи 1G-5G, трафика и емкости сотовых систем.

Рассматриваются угрозы передаваемой информации в сетях сотовой связи, методы обеспечения безопасности в сетях GSM. Рассматриваются вопросы анализа защищенности информации, методы применения и оценки качества генераторов ПСП.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (лабораторные работы), самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 7 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Экономика информационной безопасности», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.13.07 «Проектирование элементов защищенных телекоммуникационных системах»

Дисциплина «Проектирование элементов защищенных телекоммуникационных системах» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Физическая защита информационных объектов», «Основы управления информационной безопасностью» и компетенциях: ОК-4,9; ОПК-2,5,6; ПК-1,6,9.

Дисциплина направлена на формирование следующих компетенций:

ОПК-1: способность анализировать физические явления и процессы для решения профессиональных задач;

ПК-2: способностью применять программные средства системного, прикладного и специального назначения;

ПК-3: способность администрировать подсистемы информационной безопасности объекта защиты;

ПК-6: способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

ПК-12: способность принимать участие в проведении экспериментальных исследований системы защиты информации;

ПСК-1: способность проводить совместный анализ функционального процесса защиты ТКС и ее информационных составляющих с целью определения возможных источников угроз, их вероятных целей;

ПСК-2: способность формировать предложения по оптимизации функционального процесса и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов;

ПСК-3: способность организовывать контроль и анализ защищенности объектов ТКС в соответствии с нормативными документами;

ПСК-4: способность организовать реализацию принятых мер по управлению защитой информационных потоков на пакетном уровне с комплексной оценкой информационной безопасности ТКС.

Целью дисциплины является ознакомление со специфическими особенностями решения задач создания систем защиты информации в телекоммуникационных системах и выработка практических навыков применения теории проектирования защищенных телекоммуникационных систем в исследовательской и инженерной деятельности.

Содержание дисциплины предполагает рассмотрение основных принципов создания надежной и безопасной инфраструктуры, изучение сегментирования защищенных телекоммуникационных сетей на канальном уровне, межсетевое экранирование, как метода защиты периметра, политики межсетевое экранирование. Рассматриваются технологии туннелирования в защищенных телекоммуникационных сетях, вопросы аутентификация и хранения учетных записей.

В дисциплине изучаются основные параметры и структуры информационных сообщений космических систем, оценка реальных и предельных возможностей пропускной способности, помехоустойчивости и информационной безопасности телеуправления космическими аппаратами.

Дисциплина содержит информацию о правилах применения требований ЕСКД и Единой системы программной документации при разработке технической документации, о методах анализа показателей качества проектируемых сетей и систем телекоммуникаций и их элементов.

Большое внимание уделяется вопросам составления рабочего проекта с пониманием содержания основных этапов процесса проектирования.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа. Преподавание дисциплины ведется на 3 курсе в 7 семестре для очной и предусматривает проведение учебных занятий

следующих видов: лекции, лабораторные, практические занятия (лабораторные работы), самостоятельная работа обучающихся.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 7 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Экономика информационной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.13.08 «Математическое моделирование защищенных систем ТКС»

Дисциплина «Математическое моделирование защищенных систем ТКС» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Нормативные акты и стандарты по информационной безопасности», «Информационные технологии» и компетенциях: ОК-4,5, ОПК-2,3,4,5; ПК-6,8,10,15.

Дисциплина направлена на формирование следующих компетенций:

ОК-5: способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ПК-9: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

ПК-10: способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;

ПК-12: способность принимать участие в проведении экспериментальных исследований системы защиты информации;

ПСК-1: способность проводить совместный анализ функционального процесса защиты ТКС и ее информационных составляющих с целью определения возможных источников угроз, их вероятных целей;

ПСК-2: способность формировать предложения по оптимизации функционального процесса и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов;

ПСК-3: способность организовывать контроль и анализ защищенности объектов ТКС в соответствии с нормативными документами;

ПСК-4: способность организовать реализацию принятых мер по управлению защитой информационных потоков на пакетном уровне с комплексной оценкой информационной безопасности ТКС.

Целями дисциплины являются: обучение студентов основным понятиям и методам одного из этапов системного анализа – моделирования; рассмотрение языков и систем моделирования; изучение процесса постановки задачи построения модели, планирования эксперимента, оценки точности и достоверности результатов моделирования.

Содержание дисциплины включает:

- методы математического моделирования телекоммуникационных систем;

- методологические основы моделирования и понятийный аппарат аналитического и имитационного моделирования;

- сведения из теории систем и системный подход к моделированию;

- принципы построения математических моделей и их классификацию;

- моделирование векторных случайных величин;

- методы моделирования случайных процессов и планирования экспериментов.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа. Преподавание дисциплины ведется на 4 курсе в 8 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 8 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.13.09 «Физические основы волоконно-оптических линий связи (ВОЛС)»

Дисциплина «Физические основы волоконно-оптических линий связи (ВОЛС)» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Экономика предприятия и организация производства», «Основы права», «История», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», и компетенциях: ОК-2,5,8; ОПК-4,6; ПК-4,7,9 и ПСК-2.

Дисциплина направлена на формирование следующих компетенций:

ОК-2: способность использовать основы экономических знаний в различных сферах деятельности;

ПК-7: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.

Цели дисциплины:

– получение необходимых знаний по физическим и теоретическим основам функционирования оптических систем связи и обработки информации;

– получение необходимых знаний по основам построения оптических систем связи и обработки информации.

В содержании курса раскрываются физические основы оптической связи, физические основы генерации и детектирования оптического излучения, физические основы волоконно-оптической связи (ВОЛС). Изучаются основные параметры передачи излучения с помощью оптических волокон, основы построения пассивных компонентов ВОЛС, основы построения передающих и приемных устройств волоконно-оптических систем передачи.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 4 курсе в 8 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 8 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.Б.14 «Физическая культура»

Дисциплина «Физическая культура» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой гуманитарных и социальных дисциплин.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

ОК-9: способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности.

Целью изучения дисциплины является:

формирование физической культуры личности и способности направленного использования разнообразных средств физической культуры, спорта и туризма для сохранения и укрепления здоровья, психофизической подготовки и самоподготовки к будущей профессиональной деятельности.

Критерием успешности освоения учебного материала является экспертная оценка преподавателя, учитывающая регулярность посещения учебных занятий, знаний теоретического раздела программы, выполнение установленных тестов общей физической и спортивно-технической подготовки.

Обязательные тесты проводятся в начале учебного года как контрольные, характеризующие уровень физической подготовленности первокурсника при поступлении в вуз и физическую активность студента в каникулярное время, и в конце учебного года – как определяющие сдвиг в уровне физической подготовленности за прошедший учебный год.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 1 курсе во 2 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме зачета во 2 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Элективные курсы по физической культуре и спорту», «Физическая защита информационных объектов», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Вариативная часть

Б1.В.01 Дисциплины (модули) образовательной организации

Б1.В.01.01 «Основы исследований информационной безопасности»

Дисциплина «Основы исследований информационной безопасности» относится к обязательным дисциплинам вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ПК-8: способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

ПК-9: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

ПК-11: способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;

ПК-12: способность принимать участие в проведении экспериментальных исследований системы защиты информации.

Целью изучения дисциплины является формирование у студентов понимания роли и места научной деятельности для выбранной профессии, а также получение первичных навыков научных исследований с учётом особенностей обучения и решения специфических теоретических и практических задач в области информационной безопасности.

Основными задачами дисциплины являются: подготовка студентов к грамотному выполнению заданий по специальным дисциплинам и к участию в научно-исследовательских работах, проводимых на кафедре, факультете и академии; ознакомление студентов со спецификой и методологией научной деятельности; ознакомление студентов с математическими и аналитическими методами, применяемыми в научных исследованиях, способами их организации и проведения, а также оформления полученных результатов; осознание тесной взаимосвязи деятельности в области информационной безопасности с научными исследованиями.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 1 курсе в 1 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в

форме контрольной работы и экзамена в 1 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Управление информационной безопасностью», «Экономическая теория информационной безопасности», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.01.02 «Основы социального государства и гражданского общества»

Дисциплина «Основы социального государства и гражданского общества» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой гуманитарных и социальных дисциплин.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности;

ПК-14: способность организовывать работу малого коллектива исполнителей в профессиональной деятельности.

Содержание дисциплины охватывает круг вопросов связанных с изучением основ функционирования социального государства, принципов, целей и направлений социальной политики государства; сущность и принципы формирования гражданского общества; приоритеты социального развития РФ, теоретические основы возникновения социального государства, как государства нового цивилизационного типа.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 1 курсе в 1 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 1 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Философия», «История», «Основы права», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.01.03 «Пакеты прикладных программ»

Дисциплина «Пакеты прикладных программ» относится к обязательным дисциплинам вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач;

ПК-1: способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

ПК-2: способностью применять программные средства системного, прикладного и специального назначения.

Курс направлен на профессиональное освоение существующих пакетов прикладных программ современного офиса (на примере Microsoft Office), а также способов оптимального решения повседневных деловых задач с использованием средств автоматизации на основе вышеупомянутого пакета.

Целью курса является развитие у студентов теоретических знаний в области использования прикладного программного обеспечения и формирование умений и практических навыков, необходимых для успешного применения в профессиональной деятельности полной конфигурации офисного пакета Microsoft Office.

Содержание курса охватывает основные задачи офисной деятельности и технологии их решения, проблему выбора и адаптации Пакета прикладных офисных программ к конкретным задачам заданной предметной области. Детально изучаются базовые компоненты пакета Microsoft Office (текстовый и табличный процессор, средства презентаций, система управления базой данных, почтовая служба и деловой органайзер, средства управления вводом-выводом, распознаванием и обработкой мультимедийной информации), его основные возможности, принципы и приемы разработки и использования различных классов OLE-связанных документальных материалов (деловая переписка, планирующие и отчетные документы, учебно-методические и научные работы). В дополнение к пакету Microsoft Office затрагиваются офисные средства телекоммуникаций и IP-телефонии (ICQ, Skype) и OCR (FineReader), системы машинного перевода (локальные и сетевые сервисы), Интернет-технологии поиска и управления коллективными информационными ресурсами, системы управления проектами.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часов. Преподавание дисциплины ведется на 2 курсе в 3 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 3 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность кредитно-финансовых операций», «Защищенные электронные технологии банка», «Информационно-психологическая безопасность персонала предприятия», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.01.04 «Социально-психологические основы управленческой деятельности»

Дисциплина «Социально-психологические основы управленческой деятельности» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой гуманитарных и социальных дисциплин.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Безопасность жизнедеятельности», «Профессиональные адаптации инвалидов и лиц с ОВЗ» и компетенциях: ОК-4,5; ОПК-6,7 и ПК-9.

Дисциплина направлена на формирование следующих компетенций:

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ПК-14: способность организовывать работу малого коллектива исполнителей в профессиональной деятельности.

Курс содержит основные сведения и базовые знания о предприятиях (организациях) различных форм собственности, включая существующие организационно-правовые формы, в которых может осуществляться их деятельность; дает представление о нормативно-правовых документах, необходимых для создания и функционирования предприятий; позволяет определять наиболее эффективные способы организации и управления предприятиями различных форм собственности.

Целью курса является формирование представлений о сложившемся в экономике России равноправии форм собственности и обеспечении экономической свободы для инициативной хозяйственной деятельности

различных организационно-правовых структур в рамках действующего законодательства.

Содержание курса охватывает круг вопросов, связанных с изучением особенностей практической деятельности всех перечисленных в Гражданском кодексе РФ юридических лиц, классифицируемых по основной цели деятельности, организационно-правовой форме и характеру прав, возникающих у их учредителей (участников) в связи с их участием в образовании имущества учреждаемого ими юридического лица.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 2 курсе в 3 семестре для очной и на 2 курсе в 4 семестре очно - заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 3 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационные технологии в профессиональной деятельности», «Адаптированные информационные технологии», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.01.05 «Основы проектной деятельности»

Дисциплина «Основы проектной деятельности» относится к обязательным дисциплинам вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «История», «Основы права», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности» и компетенциях: ОК-3, 4; ОПК-4,5,6 и ПК-4,8,9,10,11,12,15.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способностью применять соответствующий математический аппарат для решения профессиональных задач;

ОПК-3: способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач;

ОПК-4: способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-7: способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их

реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

ПК-4: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

ПК-5: способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;

ПК-6: способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

ПК-7: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;

ПК-8: способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

ПК-11: способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;

ПК-12: способность принимать участие в проведении экспериментальных исследований системы защиты информации;

ПК-13: способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;

ПК-14: способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности;

ПК-15: способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ПСК-2: способностью формировать предложения по оптимизации функционального процесса и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов;

ПСК-3: способностью разработать комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение и последующее сопровождение;

ПСК-4: способностью организовать контроль защищенности объектов в соответствии с нормативными документами.

Целью курса является формирование знаний основам проектной деятельности. Выявлению существующих проблем в рамках обеспечения функционирования объекта информатизации. Системы управления

информационной безопасностью объекта. Выполнению всестороннего анализа на предмет соответствия системе требований, предъявляемых к такого рода объектам в соответствии с нормативно-правовой базой по защите обрабатываемого информационного ресурса в соответствии закономерностями и тенденциям развития системы защиты информации в России, а также эволюции существующих и представлений, взглядов, научных концепций, связанных со структурой и методами защиты информации.

Содержание курса связано с изучением состава защищаемой информации на различных этапах функционирования объекта информатизации, структуры угроз конфиденциальной информации, развития методов несанкционированного доступа к ней, изменения государственной политики в области защиты информации, развития и совершенствования нормативной базы, состава органов защиты информации, направлений и методов обеспечения информационной безопасности, факторов, определяющих современную систему защиты информации.

Выбор темы, требования к ее обоснованию. Разработка учебного плана. Библиографический список, сбор, анализ, и обобщение литературных источников. Основные части работы: содержание, введение, основная часть, заключение, глоссарий, библиография, оформление работы, подготовка к защите, содержание презентации, процедура публичной защиты.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа. Преподавание дисциплины ведется на 2 курсе в 3 и 4 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 3 семестре и контрольной работе и зачета с оценкой в 4 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Технико-экономическое обоснование проекта», «Разработка и реализация проекта», «Информационно-психологическая безопасность персонала предприятия», «Защита общества от информации, запрещенной к распространению», «Разработка политики информационной безопасности в организациях», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.01.06 «История защиты информации в РФ»

Дисциплина «История защиты информации в РФ» относится к обязательным дисциплинам вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «История», «Основы права», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности» и компетенциях: ОК-3, 4; ОПК-4,5,6 и ПК-4,8,9,10,11,12,15.

Дисциплина направлена на формирование следующих компетенций:

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ПК-9: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.

Курс рассматривает вопросы становления и развития систем и органов защиты информации в России с XV века по настоящее время в общем историческом контексте.

Целью курса является формирование знаний по закономерностям и тенденциям развития системы защиты информации в России, а также эволюции исторических представлений, взглядов, научных концепций, связанных со структурой и методами защиты информации.

Содержание курса связано с изучением состава защищаемой информации на различных этапах развития государства по видам тайны, структуры угроз конфиденциальной информации, развития методов несанкционированного доступа к ней, изменения государственной политики в области защиты информации, развития и совершенствования нормативной базы, состава органов защиты информации, направлений и методов обеспечения информационной безопасности, факторов, определяющих современную систему защиты информации.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и в 6 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета с оценкой в 5 семестре для очной формы обучения и зачета с оценкой в 6 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационно-психологическая безопасность персонала предприятия», «Защита общества от информации, запрещенной к распространению», «Разработка политики информационной безопасности в организациях», прохождения практики,

государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.01.07 «Информационная безопасность автоматизированных систем»

Дисциплина «Информационная безопасность автоматизированных систем» относится к обязательным дисциплинам вариативной части, основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Техническая защита информации» и компетенциях: ОК-4,5; ОПК-2,3,4,5 и ПК-2,3,5,6,8,9,10,12,15.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач;

ОПК-3: способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач;

ПК-2: способностью применять программные средства системного, прикладного и специального назначения;

ПК-5: способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;

ПК-8: способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Курс охватывает круг вопросов, связанных с проблематикой разработки и развития методов обеспечения информационной безопасности автоматизированных систем, а также выбором эффективных механизмов для их реализации.

Цель курса - формирование базовых знаний в области обеспечения информационной безопасности автоматизированных систем; навыков организации работы по проектированию и оценке эффективности систем безопасности, оптимального выбора и интеграции механизмов обеспечения информационной безопасности.

Содержание курса включает рассмотрение понятийного базиса в области обеспечения информационной безопасности автоматизированных систем, классов и типовых моделей автоматизированных систем; причин

нарушения безопасности систем, существо проблемы обеспечения информационной безопасности, концептуальную модель безопасности, формирование требований к безопасности, основные механизмы обеспечения информационной безопасности систем; безопасный доступ к информационным ресурсам, формирование доверенных сред, антивирусная защита, обнаружение вторжений, межсетевое экранирование, виртуализация как механизм защиты информации в сетях; элементы криптографической защиты; основы безопасности программного обеспечения; вопросы организации обеспечения информационной безопасности систем: нормативная база, структура и принципы построения системы обеспечения информационной безопасности, рубежи защиты систем и связанные с ними задачи, виды и этапы обеспечения информационной безопасности, элементы управления информационной безопасностью автоматизированных систем.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (лабораторные работы), самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 7 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Лицензирование и сертификация в области защиты информации», «Аттестация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.02 «Основы права»

Дисциплина «Основы права» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой гуманитарных и социальных дисциплин.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-6: способность применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности;

ПК-4: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.

Содержание дисциплины охватывает круг вопросов, связанных с изучением основных юридических понятий, предметов, принципов и специфики основных отраслей отечественного законодательства, изучением вопросов защиты прав и интересов участников конституционных правоотношений, рассмотрение вопросов, обеспечивающих правовую основу практических умений решения студентами юридических проблем в сфере публичного права.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 1 курсе в 1 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 1 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организационное и правовое обеспечение информационной безопасности», «Правовая охрана результатов интеллектуальной деятельности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.03 «Безопасность информационных технологий»

Дисциплина «Безопасность информационных технологий» относится к обязательным дисциплинам вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Математическая логика и теория алгоритмов» и компетенциях: ОК-4,5;ОПК-2,3,4,5 и ПК-3,6,8,10,15.

Дисциплина направлена на формирование следующих компетенций:

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-7: способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

ПК-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

ПК-8: способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Курс ориентирован на теоретическое изучение и практическое освоение основных классов современных информационно-коммуникационных технологий.

Целью курса является формирование компетенций в области выбора, адаптации, использования и синтеза информационно-коммуникационных технологий, обеспечивающих функционирование информационных систем в рамках заданной политики безопасности.

Содержание курса охватывает существующие программные продукты и защищенные технологии финансовых структур и менеджмента предприятий и организаций. Защитные мероприятия в структуре городского хозяйства и различных ситуационных центров. Особенности защиты интеллектуальной собственности в различных информационных ресурсах. Технология применения ЭЦП и др. активных средств противодействия утечки информации и подслушивания. Методология применения цифровых водяных знаков в организации защиты информационных объектов и документов на предприятии.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме зачета с оценкой в 6 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность кредитно-финансовых операций», «Защищенные электронные технологии банка», «Разработка политики информационной безопасности в

организациях», «Аттестация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.04 «Гуманитарные аспекты (профессиональная этика) информационной безопасности»

Дисциплина «Гуманитарные аспекты (профессиональная этика) информационной безопасности» относится к обязательным дисциплинам вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Математическая логика и теория алгоритмов» и компетенциях: ОК-4,5; ОПК-4,5,7 и ПК-4,6,8,9,10,15.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности;

ОПК-7: способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

ПК-10: способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.

Предметом изучения курса являются теоретические, методологические и практические вопросы изучения основных категорий общечеловеческой и профессиональной этике в области информационной безопасности современного информационного общества. Дисциплина построена на основе использования системного подхода разрешению сложнейших социально-гуманитарных проблем, возникающих в ходе построения и развертывания новейших вариантов обеспечения информационной безопасности различных информационных объектов и субъектов.

Целью курса является:

формирование у обучающихся представление о характере и механизме действия норм профессиональной этики специалиста по информационной безопасности;

умение оценивать профессиональную деятельность на основе существующих этико-профессиональных критериев в единстве и взаимодействии с требованиями общественной морали в процессе организации комплексного обеспечения информационной безопасности современных социотехнических систем.

Тематика курса объединена в виде логически увязанных двух разделов. Первый носит общегуманитарные аспекты информационной безопасности и включает: понятие и содержание гуманитарных аспектов информационной безопасности в современном информационном обществе; этапы развития и основные проблемы обеспечения информационной безопасности новейших информационных технологий. Во втором разделе освещаются основы профессиональной этики в области информационной безопасности. Рассматриваются: нравственные аспекты этики поведения в сети (локальной, корпоративной и Интернет – сети) и интеллектуальной собственности; преодоление цифрового неравенства в современном информационном обществе; понятие и характеристика кодексов этики профессиональных организаций и специалистов в области информационной безопасности.

Предметом изучения курса является профессиональная этика поведения организаций, специалистов и граждан современного информационного общества в области информационной безопасности. Использование этических знаний позволяет осуществлять поиск наиболее эффективных решений по обеспечению информационной безопасности.

Целевая направленность курса предусматривает формирование у студентов, профессионалов в области информационной безопасности, нравственно-мотивированной, социально-ответственной, целостной и компетентной личности, владеющей этическими знаниями, охватывающими становление и развитие нравственности и профессиональной этики в области информационной безопасности современного информационного общества.

Задачами дисциплины следует рассматривать:

- изучение истории развития морали и общечеловеческой этики, основных категорий и норм профессиональной этики в области информационной безопасности;

- формирование понятия нравственной культуры и факторов ее успешной реализации в профессиональной деятельности специалистов по информационной безопасности.

Изучаемый учебный материал базируется на анализе отечественного и международного опыта по формированию этических профессиональных кодексов, выработанных для области обеспечения информационной безопасности в современном информационном обществе.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 6 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Лицензирование и сертификация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.05 Элективные курсы по физической культуре и спорту

Дисциплина «Элективные курсы по физической культуре и спорту» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой гуманитарных и социальных дисциплин.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

ОК-8: способностью к самоорганизации и самообразованию;

ОК-9: способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности.

Целью изучения дисциплины является: формирование физической культуры личности и способности направленного использования разнообразных средств физической культуры, спорта и туризма для сохранения и укрепления здоровья, психофизической подготовки и самоподготовки к будущей профессиональной деятельности.

Критерием успешности освоения учебного материала является экспертная оценка преподавателя, учитывающая регулярность посещения учебных занятий, знаний теоретического раздела программы, выполнение установленных тестов общей физической и спортивно-технической подготовки.

Обязательные тесты проводятся в начале учебного года как контрольные, характеризующие уровень физической подготовленности первокурсника при поступлении в вуз и физическую активность студента в каникулярное время, и в конце учебного года – как определяющие сдвиг в уровне физической подготовленности за прошедший учебный год.

Общая трудоемкость освоения дисциплины составляет 9 зачетных единиц, 328 часов для очной формы обучения. Преподавание дисциплины ведется на 1-3 курсах в 1-6 семестрах для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции,

самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме зачета в 1-6 семестрах для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Физическая культура», «Физическая защита информационных объектов», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.01 Дисциплины по выбору Блок 1В.ДВ.1

Б1.В.ДВ.01.01 «Операционные системы, среды и оболочки»

Дисциплина «Операционные системы, среды и оболочки» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Математический анализ», «Теория информации», «Основы управленческой деятельности», «Информатика» и компетенциях: ОК-6; ОПК-2, ОПК-4 и ПК-11,14.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-2: способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах.

Курс освещает вопросы, связанные с теоретическими и практическими аспектами функционирования современных операционных систем и оболочек, а также формированием практических навыков по настройке и администрированию встроенных средств защиты информации операционных систем (ОС).

Целью курса является приобретение понимания архитектуры и внутреннего устройства современных ОС, знакомство с базовыми элементами графического и консольного интерфейсов, получения навыков выбора и реализации безопасных конфигураций систем, как в автономном, так и в сетевом исполнении.

Содержание курса охватывает вопросы эволюции и развития операционных систем и оболочек, архитектуры, реализации функций, возлагаемых на ОС, в части обеспечения пользовательского интерфейса и интерфейса к аппаратной платформе, поддержки многозадачности, распределения ресурсов между конкурентными процессами, организацию виртуальной памяти и файловой системы, взаимодействия между процессами. Отдельным блоком рассматриваются вопросы, относящиеся к подсистеме защиты информации. Подробно изучаются компоненты, реализующие базовые сервисы безопасности, такие как аутентификация пользователей, разграничение доступа к защищаемым ресурсам и регистрация событий.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 2 курсе в 4 семестре для очной обучения и в 5 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работе и зачета в 4 семестре для очной формы обучения и зачета в 5 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Защищенные электронные технологии банка», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.01.02. «Базы данных, системы управления базами данных»

Дисциплина «Базы данных, системы управления базами данных» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Математический анализ», «Теория информации», «Основы управленческой деятельности», «Информатика» и компетенциях: ОК-6; ОПК-2, ОПК-4 и ПК-11,14.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач;

ПК-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач.

В курсе излагаются основные понятия и методы организации реляционных баз данных и манипулирования ими, а также описываются базовые подходы к проектированию реляционных баз данных. Важную часть курса составляют вопросы защиты информации в базах данных.

Целью курса является формирование понимания основных принципов реляционной модели данных, навыков проектирования систем управления базами данных с использованием диаграммных моделей.

В курсе рассматриваются основные понятия реляционной модели данных, структурная, манипуляционная и целостная составляющие модели. Изучаются важные аспекты теории баз данных, связанные с функциональными зависимостями, процесс проектирования реляционных баз данных, на основе принципов нормализации, а также подходы к проектированию реляционных баз данных с использованием диаграммных семантических моделей данных. Также рассмотрены вопросы формирования запросов к базе данных и основные элементы языка SQL. Изучается общая концепция защиты информации, в частности вопросы определения прав и привилегий пользователей.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 2 курсе в 4 семестре для очной обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 4 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Защищенные электронные технологии банка», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.02 Дисциплины по выбору Блок1.В.ДВ.2

Б1.В.ДВ.02.01 «Основы алгоритмизации и программирования»

Дисциплина «Основы алгоритмизации и программирования» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Информатика» и компетенциях: ОПК-2,4.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач;

ПК-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач.

Цель дисциплины состоит в изучении методов алгоритмизации, основ программирования на алгоритмических языках высокого уровня и в использовании полученных навыков при решении инженерных задач.

Задачи курса:

- формирование базовых знаний по алгоритмизации и программированию - о стиле написания программ, о рациональных методах их разработки и оптимизации, о стратегии отладки и тестирования программ;

- получение базового уровня по программированию на языке Си с использованием простых типов данных: базовых типов данных и массивов;

- изучение структур данных в памяти и в файлах и алгоритмов работы с ними с использованием языка Си;

- знакомство с основными принципами организации хранения и поиска данных, алгоритмами сортировки и поиска;

- приобретение навыков использования базового набора фрагментов и алгоритмов в процессе разработки программ, навыков анализа и “чтения” программ;

- изучение основ технологии программирования и методов решения вычислительных задач и задач обработки символьных данных;

- формирование уровня знания языка, позволяющего свободно оперировать типами данных и переменными произвольной сложности и модульными алгоритмами их обработки.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 1 курсе во 2 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета во 2 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.02.02 «Пакеты прикладных математических программ»

Дисциплина «Пакеты прикладных математических программ» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Информатика» и компетенциях: ОПК-2,4.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач;

ПК-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач.

Курс направлен на изучение существующих пакетов прикладных математических программ и на этой основе освоение эффективных способов решения задач обеспечения информационной безопасности.

Целью курса является формирование практических навыков использования современных пакетов прикладных математических программ при проведении расчетного и имитационного моделирования информационных процессов и систем в прикладных задачах информационной безопасности.

Содержание курса включает обзор наиболее популярных специализированных и универсальных пакетов прикладных математических программ, математических пакетов с открытым кодом и интегрированных пакетов системного моделирования; основные подходы к организации интерфейса и реализации командных языков; функциональные возможности и предназначение пакетов; основные вычислительные процедуры, реализуемые изучаемыми программными средствами; аспекты теоретико-вероятностного моделирования процессов и систем; синтез и манипулирование теоретико-графовыми объектами; мультимедийная визуализация математических моделей; имитационно-функциональное моделирование сложных систем.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 1 курсе во 2 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета во 2 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.03 Дисциплины по выбору Блок1.В.ДВ.3

Б1.В.ДВ.03.01 «Информационная безопасность кредитно-финансовых операций»

Дисциплина «Информационная безопасность кредитно-финансовых структур» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОК-5,6; ОПК-2,4,6; ПК-4,14.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач;

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ПК-7: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;

ПК-11: способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;

ПСК-3: способность разработать комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение и последующее сопровождение.

Целью изучения дисциплины является: Ускоренная адаптация студентов в предметную область информационная безопасность, опираясь на весь спектр научных воззрений, на развитие и защиту информационно - телекоммуникационной инфраструктуры и компьютерной информации при проведении кредитно-финансовых операций; повысить уровень специальных знаний, которые необходимы обучающимся для высоко профессиональной деятельности во всех сферах информационной безопасности с учетом требований высшей школы, для активизации их учебной и исследовательской деятельности; Формирование у студентов специализированной базы знаний по основным понятиям в области банковских информационных систем и технологий кредитно-финансовых операций; приобретение студентами первичных навыков по практическому формированию комплекса документов, составляющих правовую базу защиты информации в банковской сфере (обеспечение электронной коммерции и интернет – расчетов).

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 5 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б3.В.ДВ.03.02 «Защищенные электронные технологии банка»

Дисциплина «Защищенные электронные технологии банка» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОК-5,6; ОПК-2,4,6; ПК-4,14.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач;

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ПК-7: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;

ПК-11: способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;

ПСК-3: способность разработать комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение и последующее сопровождение.

Предметом изучения курса являются основы банковского бизнеса - технологии расчетной, депозитной, кредитной, бухгалтерской работы банков и пр., с применением для этого информационных технологий.

Целью дисциплины является формирование знаний в области использования информационных технологий для организации эффективной работы банков.

Содержание курса охватывает следующие темы: формы и технология безналичных расчетов в РФ, технологии межбанковских платежей, нетто-расчеты и брутто-расчеты, система ВРРВ Банка России. Корреспондентские отношения между банками (расчеты по счетам «лоро»/«ностро»), расчеты через клиринговые организации, внутрибанковские и межфилиальные расчеты, унифицированные форматы электронных банковских сообщений; организация наличного денежного оборота, дистанционное банковское обслуживание, розничные платежные системы, системы платежей по банковским картам, системы «электронных денег», «виртуальных счетов» и «виртуальных чеков»; формы и технологии международных расчетов, расчеты платежными сообщениями через систему SWIFT, расширения языка XML для передачи финансовой информации; депозитная работа в коммерческом банке, кредитная работа в коммерческом банке, операции с ценными бумагами, депозитарное обслуживание, операции с драгоценными металлами, обслуживание «металлических» счетов; управление ликвидностью коммерческого банка, управление банковскими рисками, основы бухгалтерского учета в коммерческом банке, банковский маркетинг.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 5 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.03.03 «Технические каналы утечки конфиденциальной информации (ОАО «НОВО», НТЦ «ЗАРЯ»»

Дисциплина «Технические каналы утечки конфиденциальной информации (ОАО «НОВО», НТЦ «ЗАРЯ»» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется базовой кафедрой защиты информации.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОК-5,6; ОПК-2,4,6; ПК-4,14.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач;

ОПК-3: способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач;

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ПК-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

ПК-7: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;

ПК-11: способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов.

Предметом изучения курса являются технические каналы утечки конфиденциальной информации

Целью дисциплины является формирование знаний в области подготовки обучающихся по вопросам защиты информации от утечки по техническим каналам на объектах и в выделенных помещениях.

Содержание курса охватывает следующие темы:

Системный подход к защите информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической защиты информации. Представление сил и средств защиты информации в виде системы. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации. Распространение сигналов в технических каналах утечки информации. Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях. Распространение оптических сигналов в атмосфере и в светопроводах. Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи. Основные концептуальные положения технической защиты информации. Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации. Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации. Особенности информации как предмета защиты. Свойства информации, влияющие на ее безопасность. Виды, источники и

носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ.

Моделирование случайных величин. Законы распределения случайных величин. Статистические оценки и их точность. Аппроксимация результатов статистического моделирования. Моделирование инженерно-технической защиты информации. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты. Задачи защиты информации ТКС в условиях конфликта. Понятие конфликта. Способы разрешения конфликта в ТКС. Информационный конфликт (виды, варианты реализации). Стратегии противоборствующих сторон в динамике развития информационного конфликта ТКС с системами воздействия. Понятия стратегия, тактика обеспечения защиты информации, воздействия на ТКС. Конфликтная матрица реализации стратегий (тактик) защиты и воздействия.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 5 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.04 Дисциплины по выбору Блок1.В.ДВ.4

Б1.В.ДВ.04.01 «Информационно-психологическая безопасность персонала предприятия»

Дисциплина «Информационно-психологическая безопасность персонала предприятия» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика»,

«Основы права», «Основы управленческой деятельности» и компетенциях: ОК-5,6; ОПК-2,4,6; ПК-4,14.

Дисциплина направлена на формирование следующих компетенций:

ПК-14: способность организовывать работу малого коллектива исполнителей в профессиональной деятельности;

ПСК-3: способность разработать комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение и последующее сопровождение.

Целями изучения дисциплины является: обучение студентов принципам и средствам обеспечения информационной безопасности личности (сотрудников), коллективов (организационных структур предприятий) и в целом общества (предприятий); получение студентами фундаментальных основ по формированию научного мировоззрения, развитию системного мышления и интеграции полученных ранее знаний по обеспечению информационной безопасности.

Основные задачи дисциплины – дать основные знания, умения и навыки по вопросам обеспечения информационной безопасности личности (сотрудника), коллектива сотрудников (отделов, служб) и, в целом, всего коллектива предприятия как общества.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (лабораторные работы), самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета с оценкой в 6 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Лицензирование и сертификация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.04.02 «Защита общества от информации, запрещенной к распространению»

Дисциплина «Защита общества от информации, запрещенной к распространению» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОК-5,6; ОПК-2,4,6; ПК-4,14.

Дисциплина направлена на формирование следующих компетенций:

ПК-14: способность организовывать работу малого коллектива исполнителей в профессиональной деятельности;

ПСК-3: способность разработать комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение и последующее сопровождение.

Курс содержит основные сведения, касающиеся организации и технологии организационно-правовой защиты общества от информации, законодательно запрещенной для создания и последующего распространения, в том числе информации, возбуждающей социальную, расовую, национальную и религиозную ненависть и вражду, призывающей к войне или пропагандирующей войну, а также посягающей на честь и достоинство гражданина, на деловую репутацию физического или юридического лица.

Цель курса - сформировать взгляды на обеспечение информационной безопасности как на системную научно-практическую деятельность и научить способам организационно-правовой защиты личности и общества от информации, законодательно запрещенной для создания и последующего распространения.

В структуре курса подробно рассматриваются способы организационно-правовой защиты от создания и распространения ненадлежащей рекламы и меры ответственности за нарушение российского рекламного законодательства. Отдельный раздел дисциплины предусматривает изучение общих принципов, которые могут быть использованы для обеспечения организационно-правовой и технической защиты пользователей сети Интернет от законодательно запрещенной к распространению информации, а также изучение концепции государственной политики в области защиты детей от информации, причиняющей вред их здоровью и развитию.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (лабораторные работы), самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета с оценкой в 6 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты

персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Лицензирование и сертификация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.04.03 «Организация защиты конфиденциальной информации от несанкционированного доступа (ОАО «НОВО», НТЦ «ЗАРЯ»)

Дисциплина «Организация защиты конфиденциальной информации от несанкционированного доступа (ОАО «НОВО», НТЦ «ЗАРЯ») относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется базовой кафедрой защита информации.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОК-5,6; ОПК-2,4,6; ПК-4,14.

Дисциплина направлена на формирование следующих компетенций:

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

ПК-8: способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

ПК-9: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

ПК-10: способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;

ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Курс содержит основные сведения, касающиеся организации и технологии организационной защиты конфиденциальной информации от НСД. Обеспечивает выполнение установленных правовых норм, объединяет методы защиты, которые обеспечивают защиту информации от НСД либо самостоятельно, либо в комплексе с методами и средствами других

направлений, с помощью организационных методов методы и средства всех направлений объединяются в сложную систему.

Цель курса - сформировать взгляды на обеспечение информационной безопасности как на системную научно-практическую деятельности и научить способам в соответствии с нормативными документами предприятия осуществлять регулирование и организацию и выполнения работ.

В структуре курса подробно рассматриваются обеспечение защиты информации установленной технологией выполнения работ, исключаяющей утрату носителей информации и несанкционированный доступ к информации или к ее носителям, либо путем введения прямых правил, регулирующих организацию защиты информации от НСД.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (лабораторные работы), самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета с оценкой в 6 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Лицензирование и сертификация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.05 Дисциплины по выбору Блок1.В.ДВ.5

Б1.В.ДВ.05.01 «Разработка политики информационной безопасности в организациях»

Дисциплина «Разработка политики информационной безопасности в организациях» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОК-5,6; ОПК-2,4,6; ПК-4,14.

Дисциплина направлена на формирование следующих компетенций:

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

ПК-9: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Предмет изучения курса - практические правила по разработке политики безопасности и внедрению системы управления информационной безопасностью (СУИБ) для различных предприятий и организаций.

Целью курса является формирование умения планировать и обосновывать мероприятия по разработке и внедрению СУИБ, распределять роли и ответственности за обеспечение информационной безопасности, планировать измерение эффективности СУИБ.

Содержание курса последовательно раскрывает все этапы работы по разработке структуры и внедрению политики безопасности предприятия (организации), в том числе: инициирование проекта, определение области действия и политики безопасности, проведение анализа предприятия (организации), оценку рисков и планирование обработки рисков, проектирование СУИБ, планирование внутренних аудитов и мониторинга показателей эффективности информационной безопасности.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 6 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Лицензирование и сертификация в области защиты информации», «Аттестация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.05.02 «Разработка политики информационной безопасности в Интернет - системах»

Дисциплина «Разработка политики информационной безопасности в Интернет-системах» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОК-5,6; ОПК-2,4,6; ПК-4,14.

Дисциплина направлена на формирование следующих компетенций:

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

ПК-9: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Предмет изучения курса - практические правила по разработке политики безопасности и внедрению системы управления информационной безопасностью (СУИБ) для различных предприятий и организаций.

Целью курса является формирование умения планировать и обосновывать мероприятия по разработке и внедрению СУИБ, распределять роли и ответственности за обеспечение информационной безопасности, планировать измерение эффективности СУИБ.

Содержание курса последовательно раскрывает все этапы работы по разработке структуры и внедрению политики безопасности предприятия (организации), в том числе: инициирование проекта, определение области действия и политики безопасности, проведение анализа предприятия (организации), оценку рисков и планирование обработки рисков, проектирование СУИБ, планирование внутренних аудитов и мониторинга показателей эффективности информационной безопасности.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и предусматривает проведение учебных занятий

следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 6 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Лицензирование и сертификация в области защиты информации», «Аттестация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.05.03 «Оценка защищенности конфиденциальной информации по техническим каналам и от несанкционированного доступа (ООО «НОВО», НТЦ «ЗАРЯ»)

Дисциплина «Оценка защищенности конфиденциальной информации по техническим каналам и от несанкционированного доступа (ООО «НОВО», НТЦ «ЗАРЯ»))» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется базовой кафедрой защиты информации.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОК-5,6; ОПК-2,4,6; ПК-4,14.

Дисциплина направлена на формирование следующих компетенций:

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

ПК-9: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Предмет изучения курса - практические правила по разработке политики безопасности и внедрению системы управления информационной

безопасностью (СУИБ) для различных предприятий и организаций по защите информации по техническим каналам от НСД.

Целью курса является формирование умения планировать и обосновывать мероприятия по оценке защищенности конфиденциальной информации по техническим каналам и от несанкционированного доступа, распределять роли и ответственности за обеспечение информационной безопасности, планировать измерение эффективности системы ЗИ.

Содержание курса последовательно раскрывает все этапы работы по разработке структуры и внедрению изменений в политику безопасности предприятия (организации), по оценке защищенности конфиденциальной информации по техническим каналам и от несанкционированного доступа.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 6 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Лицензирование и сертификация в области защиты информации», «Аттестация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.06 Дисциплины по выбору Блок1.В.ДВ.6

Б1.В.ДВ.06.01 «Организации защиты персональных данных на предприятии»

Дисциплина «Организация защиты персональных данных на предприятии» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности», «Информационная безопасность кредитно-финансовых операций», «Информационно-психологическая безопасность персонала предприятия», «Разработка политики информационной безопасности в организациях» и компетенциях: ОК-5,6; ОПК-2,4,6; ПК-4,7,9,11,14,15 и ПСК-3.

Дисциплина направлена на формирование следующих компетенций:

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Содержание дисциплины охватывает круг вопросов, связанных с организацией обработки персональных данных, в соответствии с требованиями российского законодательства, применительно к различным категориям исполнителей на предприятии (от руководителей предприятий и структурных подразделений до непосредственно отвечающих за защиту информации и работающих с персональными данными). Анализируются изменения российского законодательства в части персональных данных, последствия внесения этих изменений для деятельности операторов, способы минимизации рисков, связанных с обработкой персональных данных и затрат на их защиту.

Цель курса - формирование знаний и умений для организации комплекса мероприятий по обеспечению конфиденциальности обработки персональных данных с использованием правовых, организационных и организационно-технических мер, определенных с учетом актуальности угроз безопасности персональных данных и используемых информационных технологий, способы снижения рисков утечки персональных данных.

Структура курса предполагает рассмотрение теоретических и практических аспектов в работе с персональными данными на предприятии, а также разбор на практических примерах действий операторов персональных данных в рамках трудовых отношений с собственным персоналом, гражданско-правовых отношениях, связанных с передачей и представлением персональных данных третьим лицам, в том числе органам государственной власти.

Общая трудоемкость освоения дисциплины 4 зачетных единицы, 144 часа. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 7 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Лицензирование и

сертификация в области защиты информации», «Аттестация в области защиты информации», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Экономика информационной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.06.02 «Правовая охрана результатов интеллектуальной деятельности»

Дисциплина «Правовая охрана результатов интеллектуальной деятельности» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности», «Информационная безопасность кредитно-финансовых операций», «Информационно-психологическая безопасность персонала предприятия», «Разработка политики информационной безопасности в организациях» и компетенциях: ОК-5,6; ОПК-2,4,6; ПК-4,7,9,11,14,15 и ПСК-3.

Дисциплина направлена на формирование следующих компетенций:

ОК-4: способность использовать основы правовых знаний в различных сферах деятельности;

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-7: способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

ПК-8: способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

ПК-9: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.

В курсе раскрываются базовые понятия и определения в сфере интеллектуальной собственности, т.е. различных результатов интеллектуальной деятельности и средств индивидуализации производителей товаров и услуг, в том числе понятия интеллектуальных прав, исключительного права и личных прав авторов, защиты исключительных и личных прав и ответственности за нарушение указанных прав. Рассматриваются особенности различных институтов интеллектуальной собственности, включая авторское право и смежные права,

патентное право, права на средства индивидуализации, права на секреты производства. Даются механизмы правовой охраны, используемые в глобальных сетях и в отношениях между партнерами из разных государств на основе многосторонних конвенций в сфере интеллектуальной собственности.

Целью курса является формирование представлений об эффективном использовании норм законодательства, регламентирующих механизмы охраны исключительных прав и защиты прав как на отдельные результаты интеллектуальной деятельности (изобретения, промышленные образцы, полезные модели, произведения авторского права и объекты смежных прав), так и на приравненные к ним средства индивидуализации производителей товаров и услуг.

Содержание курса охватывает круг вопросов, связанных с изучением законодательных и иных нормативно-правовых актов, регламентирующих деятельность в сфере охраны прав на результаты интеллектуальной деятельности; с правовым регулированием взаимоотношений работодателей и работников в части результатов интеллектуальной деятельности; с регулированием гражданско-правовых отношений, возникающих в связи с использованием прав на результаты интеллектуальной деятельности; с защитой прав правообладателей результатов интеллектуальной деятельности и средств индивидуализации.

Общая трудоемкость освоения дисциплины 4 зачетных единицы, 144 часа. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 7 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Лицензирование и сертификация в области защиты информации», «Аттестация в области защиты информации», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Экономика информационной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.06.03 «Методы и средства защиты информации от утечки по техническим каналам (ООО «НОВО», НТЦ «ЗАРЯ»))»

Дисциплина «Методы и средства защиты информации от утечки по техническим каналам (ОАО «НОВО», НТЦ «ЗАРЯ»))» относится к дисциплинам по выбору вариативной части основной профессиональной

образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется базовой кафедрой защиты информации.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Электротехника», «Электроника и схемотехника», «Физика», «Математический анализ», «Теория вероятностей и математическая статистика», «Иностранный язык» и компетенциях: ОК-7,8; ОПК-1,2,3 и ПК-11.

Дисциплина направлена на формирование следующих компетенций:

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-7: способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

ПК-8: способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

ПК-9: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Цель изучения дисциплины является: - получение новых знаний и умений, повышения уровня профессиональной компетентности студентов в области защиты информации от утечки по техническим каналам.

В процессе изучения данного модуля необходимо учесть весь спектр научных воззрений на техническую защиту информационных объектов; повысить уровень специальных знаний, которые необходимы обучающимся для высоко профессиональной деятельности во всех сферах информационной безопасности с учетом требований высшей школы, для активизации их учебной и исследовательской деятельности; Формирование у студентов специализированной базы знаний по основным понятиям в области технической защиты информации; приобретение студентами навыков по практическому формированию мероприятий защиты информации от утечки по техническим каналам.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часов. Преподавание дисциплины ведется на 4 курсе в 7

семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 7 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.07 Дисциплины по выбору Блок1.В.ДВ.7

Б1.В.ДВ.07.01 «Защита профессиональной тайны в различных сферах деятельности»

Дисциплина «Защита профессиональной тайны в различных сферах деятельности» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОК-5,6; ОПК-2,4,6 и ПК-2,4,14.

Дисциплина направлена на формирование следующих компетенций:

ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности;

ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

ПК-13: способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.

Содержание дисциплины охватывает круг вопросов, связанных с нормативно-правовыми аспектами защиты профессиональной тайны. Общая проблема защиты профессиональной деятельности имеет две стороны. Приводятся сведения об оформлении заявочных материалов на изобретение, полезную модель и промышленный образец. Подробно рассматриваются вопросы правовой защиты объектов интеллектуальной промышленной собственности (патентное право).

Основные положения дисциплины должны быть использованы в дальнейшем при изучении следующих дисциплин: информационная безопасность предприятия (организации), управление информационной безопасностью.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 6 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.07.02 «Информационная безопасность операционных систем и баз данных»

Дисциплина «Информационная безопасность операционных систем и баз данных» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОК-5,6; ОПК-2,4,6 и ПК-2,4,14.

Дисциплина направлена на формирование следующих компетенций:

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ПК-1: способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

ПК-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

ПК-6: способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых

программных, программно-аппаратных и технических средств защиты информации;

ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Курс охватывает круг вопросов, связанных с проблематикой разработки и развития методов обеспечения информационной безопасности операционных систем и баз данных, а также выбором эффективных механизмов для их реализации.

Цель курса - формирование базовых знаний в области обеспечения информационной безопасности операционных систем и баз данных; навыков организации работы по проектированию и оценке эффективности систем безопасности, оптимального выбора и интеграции механизмов обеспечения информационной безопасности.

Содержание курса включает рассмотрение понятийного базиса в области обеспечения информационной безопасности операционных систем и баз данных; причин нарушения безопасности систем, существо проблемы обеспечения информационной безопасности, концептуальную модель безопасности, формирование требований к безопасности, основные механизмы обеспечения информационной безопасности систем; безопасный доступ к информационным ресурсам, формирование доверенных сред, антивирусная защита, обнаружение вторжений, межсетевое экранирование, виртуализация как механизм защиты информации в сетях; элементы криптографической защиты; основы безопасности программного обеспечения; вопросы организации обеспечения информационной безопасности систем: нормативная база, структура и принципы построения системы обеспечения информационной безопасности, рубежи защиты систем и связанные с ними задачи, виды и этапы обеспечения информационной безопасности, элементы управления информационной безопасностью систем.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 6 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», прохождения

практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.07.03 «Подготовка объекта информатизации к аттестации по требованиям безопасности информации (ООО «НОВО», НТЦ «ЗАРЯ»)

Дисциплина «Подготовка объекта информатизации к аттестации по требованиям безопасности информации (ОАО «НОВО», НТЦ «ЗАРЯ») относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется базовой кафедрой защиты информации.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОК-5,6; ОПК-2,4,6 и ПК-2,4,14.

Дисциплина направлена на формирование следующих компетенций:

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности;

ПК-1: способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

ПК-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

ПК-6: способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

ПК-13: способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;

ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Курс охватывает круг вопросов, связанных с проблематикой

разработки и развития аттестации объектов информационной безопасности операционных систем и баз данных, а также выбором эффективных механизмов для их реализации.

Цель курса - формирование базовых знаний в области аттестации критически важных информационных объектов; навыков организации работы по аттестации проектированию и оценке эффективности систем безопасности, оптимального выбора и интеграции механизмов обеспечения информационной безопасности.

Содержание курса включает рассмотрение понятийного базиса в области обеспечения аттестации объектов информационной безопасности; причин нарушения безопасности систем, существо проблемы обеспечения информационной безопасности, концептуальную модель безопасности, формирование требований к безопасности, основные механизмы обеспечения информационной безопасности систем; безопасный доступ к информационным ресурсам, формирование доверенных сред, антивирусная защита, обнаружение вторжений, межсетевое экранирование, виртуализация как механизм защиты информации в сетях; элементы криптографической защиты; основы безопасности программного обеспечения; вопросы организации обеспечения информационной безопасности систем: нормативная база, структура и принципы построения системы обеспечения информационной безопасности, рубежи защиты систем и связанные с ними задачи, виды и этапы обеспечения информационной безопасности, элементы управления информационной безопасностью систем.

В курсе рассматриваются функции органов аттестации, испытательных центров, заявителей и их взаимодействие при проведении аттестации объектов информатизации. Изучается порядок проведения аттестации (разработка заявки на проведение аттестации, программы и методики аттестационных испытаний, их проведение), оформление и регистрация аттестата соответствия.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 6 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.08 Дисциплины по выбору Блок1.В.ДВ.8

Б1.В.ДВ.08.01 «Лицензирование и сертификация в области защиты информации»

Дисциплина «Лицензирование и сертификация в области защиты информации» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности», «Информационная безопасность кредитно-финансовых операций», «Информационно-психологическая безопасность персонала предприятия», «Разработка политики информационной безопасности в организациях», «Организация защиты персональных данных на предприятии» и компетенциях: ОК-5,6; ОПК-2,4,6; ПК-4,1,9,11,14,15 и ПСК-3.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач;

ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности;

ПК-8: способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

ПК-10: способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;

ПК-12: способность принимать участие в проведении экспериментальных исследований системы защиты информации;

ПК-14: способность организовывать работу малого коллектива исполнителей в профессиональной деятельности;

ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ПСК-4: способность организовать контроль защищенности объектов в соответствии с нормативными документами.

В курсе освещены вопросы организации и проведения работ с конфиденциальной информацией по лицензированию и сертификации деятельности предприятий, связанных с использованием сведений, составляющих государственную тайну,

для данного предприятия, установленном нормативными правовыми актами и методологическими документами, получить лицензию на

осуществление этого вида деятельности. Знание всех видов деятельности, подлежащих лицензированию в сфере защиты государственной тайны, алгоритм работы лицензирующего органа по лицензированию деятельности предприятий.

Целью курса является формирование навыков организации проведения комплекса мероприятий (лицензирования и сертификации), в результате которых устанавливается соблюдение требований законодательных и иных нормативных актов по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ; наличие в структуре предприятия подразделения по защите государственной тайны и необходимого числа специально подготовленных сотрудников для работы по ЗИ; наличие на предприятии средств защиты информации, имеющих сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности и нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России.

В курсе рассматриваются функции органов лицензирования и сертификации, испытательных центров, заявителей и их взаимодействие при проведении лицензирования объектов информатизации. Изучается порядок проведения лицензирования (разработка заявки на проведение лицензирования, программы и методики сертификационных испытаний, их проведение), оформление и регистрация лицензии соответствия.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 4 курсе в 8 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 8 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.08.02 «Аттестация в области защиты информации»

Дисциплина «Аттестация в области защиты информации» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности», «Информационная безопасность кредитно-финансовых операций», «Информационно-психологическая безопасность персонала предприятия», «Разработка

политики информационной безопасности в организациях», «Организация защиты персональных данных на предприятии» и компетенциях: ОК-5,6; ОПК-2,4,6; ПК-4,1,9,11,14,15 и ПСК-3.

Дисциплина направлена на формирование следующих компетенций:

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ПК-14: способность организовывать работу малого коллектива исполнителей в профессиональной деятельности.

В курсе освещены вопросы организации и проведения аттестации защищаемого объекта информатизации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

Целью курса является формирование навыков организации проведения комплекса организационно-технических мероприятий (аттестационных испытаний), в результате которых устанавливается соответствие защищаемого объекта требованиям стандартов и нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России.

В курсе рассматриваются функции органов аттестации, испытательных центров, заявителей и их взаимодействие при проведении аттестации объектов информатизации. Изучается порядок проведения аттестации (разработка заявки на проведение аттестации, программы и методики аттестационных испытаний, их проведение), оформление и регистрация аттестата соответствия.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 4 курсе в 8 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 8 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.08.03 «Разработка объекта информатизации в защищенном исполнении (ООО «НОВО», НТЦ «ЗАРЯ»)»

Дисциплина «Разработка объекта информатизации в защищенном исполнении (ОАО «НОВО», НТЦ «ЗАРЯ»)» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется базовой кафедрой защита информации.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности», «Информационная безопасность кредитно-финансовых операций», «Информационно-психологическая безопасность персонала предприятия», «Разработка политики информационной безопасности в организациях» и компетенциях: ОК-5,6; ОПК-2,4,6; ПК-4,1,9,11,14,15 и ПСК-3.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач;

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности;

ПК-8: способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

ПК-10: способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;

ПК-12: способность принимать участие в проведении экспериментальных исследований системы защиты информации;

ПК-14: способность организовывать работу малого коллектива исполнителей в профессиональной деятельности;

ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ПСК-4: способность организовать контроль защищенности объектов в соответствии с нормативными документами.

Содержание дисциплины охватывает круг вопросов, связанных с организацией работ на объекте информатизации в защищенном исполнении (ООО «НОВО»)), в соответствии с требованиями российского законодательства, применительно к различным категориям исполнителей на предприятии (от руководителей предприятий и структурных подразделений до непосредственно отвечающих за защиту информации и работающих с данными). Анализируются изменения российского законодательства, последствия внесения изменений для деятельности операторов, способы минимизации рисков, связанных с обработкой информационного ресурса и затрат на их защиту.

Цель курса - формирование знаний и умений для организации комплекса мероприятий по обеспечению функционирования объекта в защищенном исполнении с использованием правовых, организационных и организационно-технических мер, определенных с учетом актуальности

угроз безопасности информационного объекта и используемых информационных технологий, способы снижения рисков утечки данных.

Общая трудоемкость освоения дисциплины 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 4 курсе в 8 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 8 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Лицензирование и сертификация в области защиты информации», «Аттестация в области защиты информации», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Экономика информационной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.09 Дисциплины по выбору Блок1.В.ДВ.9

Б1.В.ДВ.09.01 «Радиоэлектронные системы и средства как объекты информационной безопасности»

Дисциплина «Радиоэлектронные системы и средства как объекты информационной безопасности» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Электротехника», «Электроника и схемотехника», «Физика», «Математический анализ», «Теория вероятностей и математическая статистика», «Иностранный язык» и компетенциях: ОК-7,8; ОПК-1,2,3 и ПК-11.

Дисциплина направлена на формирование следующих компетенций:

ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности;

ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

ПК-9: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Цель изучения дисциплины является: - получение новых знаний и умений, повышения уровня профессиональной компетентности студентов в области радиоэлектронных основ информационной безопасности. В процессе изучения данного модуля необходимо учесть весь спектр научных воззрений на радиоэлектронную защиту информационных объектов; повысить уровень специальных знаний, которые необходимы обучающимся для высоко профессиональной деятельности во всех сферах информационной безопасности с учетом требований высшей школы, для активизации их учебной и исследовательской деятельности; Формирование у студентов специализированной базы знаний по основным понятиям в области радиоэлектронных основ информационной безопасности; приобретение студентами первичных навыков по практическому формированию мероприятий радиоэлектронной защиты объектов.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 6 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.09.02 «Основы радиоэлектронной разведки (РЭР)»

Дисциплина «Основы радиоэлектронной разведки (РЭР)» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Электротехника», «Электроника и схемотехника», «Физика», «Математический анализ», «Теория вероятностей и математическая статистика», «Иностранный язык» и компетенциях: ОК-7,8; ОПК-1,2,3 и ПК-11.

Дисциплина направлена на формирование следующих компетенций:

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-7: способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

ПК-14: способность организовывать работу малого коллектива исполнителей в профессиональной деятельности.

Цель изучения дисциплины является: - получение новых знаний и умений, повышения уровня профессиональной компетентности студентов в области радиоэлектронных основ информационной безопасности. В процессе изучения данного модуля необходимо учесть весь спектр научных воззрений на радиоэлектронную защиту информационных объектов; повысить уровень специальных знаний, которые необходимы обучающимся для высоко профессиональной деятельности во всех сферах информационной безопасности с учетом требований высшей школы, для активизации их учебной и исследовательской деятельности; Формирование у студентов специализированной базы знаний по основным понятиям в области радиоэлектронных основ информационной безопасности; приобретение студентами первичных навыков по практическому формированию мероприятий радиоэлектронной защиты объектов.

Содержание курса охватывает: демаскирующие признаки радиоэлектронных объектов и особенности их вскрытия технической разведкой; анализ радиоэлектронной обстановки на информационных объектах и основы технического контроля функционирования радиоэлектронных систем и средств; основные демаскирующие признаки радиоэлектронных объектов и особенности их вскрытия радиоэлектронной разведкой; анализ радиоэлектронной обстановки на информационных объектах и основы технического контроля функционирования радиоэлектронных систем и средств.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 6 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», прохождения практики,

государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.09.03 «Методы и средства защиты информации от несанкционированного доступа (ООО «НОВО», НТЦ «ЗАРЯ»)»

Дисциплина «Методы и средства защиты информации от несанкционированного доступа (ООО «НОВО», НТЦ «ЗАРЯ»)» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется базовой кафедрой защиты информации.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОК-5,6; ОПК-2,4,6 и ПК-4,14.

Дисциплина направлена на формирование следующих компетенций:

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности;

ОПК-7: способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

ПК-9: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

ПК-14: способность организовывать работу малого коллектива исполнителей в профессиональной деятельности;

ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Предмет изучения курса - методы и средства защиты информации от несанкционированного доступа.

Целью курса является формирование умения планировать и обосновывать мероприятия по оценке защищенности конфиденциальной информации по техническим каналам и от несанкционированного доступа ,

распределять роли и ответственности за обеспечение информационной безопасности, планировать измерение эффективности системы ЗИ.

Содержание курса последовательно раскрывает все этапы работы по разработке структуры и внедрению изменений в политику безопасности предприятия (организации), по оценке защищенности конфиденциальной информации по техническим каналам и от несанкционированного доступа. Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета 6 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.10 Дисциплины по выбору Блок1.В.ДВ.10

Б1.В.ДВ.10.01 «Социотехносферная безопасность объектов информационной защиты»

Дисциплина «Социотехносферная безопасность объектов информационной защиты» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОК-5,6; ОПК-2,4,6 и ПК-4,14.

Дисциплина направлена на формирование следующих компетенций:

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ПК-14: способность организовывать работу малого коллектива исполнителей в профессиональной деятельности.

Целями изучения дисциплины являются: Дать студентам базовые знания по основам обеспечения социотехносферной безопасности ключевых объектов информационной защиты на предприятиях, организациях и учреждениях в современных условиях; Выработать и закрепить у студентов

первичные умения и навыки по организации и реализации технологий социотехносферной безопасности объектов информационной защиты на предприятиях (организациях и учреждениях) с различными формами собственности с учетом современных подходов обеспечения информационной безопасности.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена 6 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.10.02 «Эффективность защищенных информационных систем»

Дисциплина «Эффективность защищенных информационных систем» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОК-5,6; ОПК-2,4,6 и ПК-4,14

Дисциплина направлена на формирование следующих компетенций:

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности;

ПК-9: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными

правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Предмет курса – контроль состояния и эффективности защиты информации в процессе эксплуатации объектов информатизации.

Цель курса – формирование практических навыков проведения оценки эффективности защиты информации.

Содержание курса охватывает такие вопросы, как выявление уязвимостей и оценка рисков с использованием систем анализа защищенности, средства контроля защищенности (сканеры безопасности, системы обнаружения вторжений), формирование системы показателей эффективности, основные методы контроля состояния и эффективности защиты информации, оценка выполнения требований нормативных документов, обоснованности принятых мер защиты информации, аттестация автоматизированных систем.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме. Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена 6 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.10.03 «Методы и средства выявления демаскирующих признаков закладочных устройств в защищаемых помещениях (ООО «НОВО», НТЦ «ЗАРЯ»)

Дисциплина «Методы и средства выявления демаскирующих признаков закладочных устройств в защищаемых помещениях (ОАО «НОВО». НТЦ «ЗАРЯ») относится к дисциплинам по выбору вариативной

части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется базовой кафедрой защиты информации.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности», «Информационная безопасность кредитно-финансовых операций», «Информационно-психологическая безопасность персонала предприятия», «Разработка политики информационной безопасности в организациях», «Организация защиты персональных данных на предприятии» и компетенциях: ОК-5,6; ОПК-2,4,6; ПК-4,1,9,11,14,15 и ПСК-3.

Дисциплина направлена на формирование следующих компетенций:

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности;

ПК-9: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

ПК-14: способность организовывать работу малого коллектива исполнителей в профессиональной деятельности;

ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

В курсе освещены вопросы организации и проведения работ с конфиденциальной информацией по выявлению демаскирующих признаков закладочных устройств в защищаемых помещениях лицензированию и сертификации деятельности предприятий, связанных с использованием сведений, составляющих конфиденциальную информацию, для данного предприятия, установленном нормативными правовыми актами и методологическими документами.

Целью курса является формирование навыков организации проведения комплекса мероприятий направленных на выявление демаскирующих признаков закладочных устройств в защищаемых помещениях, в результате которых устанавливается соблюдение требований законодательных и иных нормативных актов по обеспечению защиты сведений, составляющих конфиденциальную информацию, в процессе выполнения работ; наличие в структуре предприятия подразделения по защите конфиденциальной информации и необходимого числа специально подготовленных сотрудников для работы по ЗИ; наличие на предприятии средств защиты информации, имеющих сертификат, удостоверяющий их соответствие требованиям по

защите сведений соответствующей степени секретности и нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 6 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.11 Дисциплины по выбору Блок1.В.ДВ.11

Б1.В.ДВ.11.01 «Введение в профессию»

Дисциплина «Введение в профессию» относится к обязательным дисциплинам вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

ОК-5: способность анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма;

ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности;

ОПК-7: способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

ПК-9: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.

Целью изучения дисциплины является ознакомление и закрепление базовых положений по обеспечению информационной безопасности на всех уровнях функционирования Российской Федерации: межгосударственном, государственном, ведомственном и отдельных граждан.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 1 курсе в 1 семестре для очной и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета с оценкой в 1 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Безопасность информационных технологий», «Гуманитарные аспекты (профессиональная этика) информационной безопасности», «Базы данных, системы управления базами данных», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.11.02 «Профессиональные адаптации инвалидов и лиц с ОВЗ»

Дисциплина «Профессиональная адаптация инвалидов и лиц с ОВЗ» относится к обязательным дисциплинам вариативной части, основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

ОК-5: способность анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма;

ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности;

ОПК-7: способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

ПК-9: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.

Целью изучения дисциплины является ознакомление и закрепление базовых положений по обеспечению информационной безопасности на всех уровнях функционирования Российской Федерации: межгосударственном, государственном, ведомственном и отдельных граждан.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 1 курсе в 1 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 1 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Безопасность информационных технологий», «Гуманитарные аспекты (профессиональная этика) информационной безопасности», «Базы данных, системы управления базами данных», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.12 Дисциплины по выбору Блок1.В.ДВ.12

Блок 2. Практики

В соответствии ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность» раздел ОПОП ВО «Практики» является обязательным. Основной целью проведения практики является закрепление и углубление знаний, полученных студентами в ходе теоретического обучения, развитие и накопление специальных практических навыков для решения профессиональных задач. Она представляет собой вид учебных занятий, непосредственно ориентированных на профессионально-практическую подготовку обучающихся.

Полнота и степень детализации практик регламентируется программами практик применительно к особенностям конкретных баз практик. При реализации данной программы по направлению подготовки 10.03.01 «Информационная безопасность» предусматриваются следующие виды практик:

учебная практика: практика по получению первичных профессиональных умений и навыков, технологическая практика;

производственная практика: проектно-технологическая практика, преддипломная практика.

Учебные и производственные практики проводятся на базе: ООО «Клио», НИИ КС им. А. А. Максимова - филиала ФГУП «ГКНПЦ им М. В. Хруничева», кафедры «Информационной безопасности, отдела защиты информации и секретного делопроизводства Министерства финансов Московской области, г. Москва, ЦБИ г. Юбилейный, ТРВ, РКК «Энергия», ОАО «НОВО», НТЦ «ЗАРЯ».

Практики планируются в соответствии с графиком учебного процесса и программами практик. От общей трудоемкости ОПОП ВО подготовки бакалавра (240 зачетных единиц) на практику предусматривается 648 часов 18 зачетных единиц (учебная практика 216 часов 6 зачетных единиц, а производственная практика 432 часа 12 зачетных единиц).

В процессе проведения всех видов практики основное внимание уделяется формированию у студентов общекультурных и профессиональных компетенций, позволяющих самостоятельно повышать уровень профессиональных знаний.

По итогам каждой из практик проводится аттестация: каждый студент представляет письменный отчет, дневник практики, характеристику руководителя практики о качестве ее прохождения; проводится обсуждение хода практики и ее результатов на кафедре, а также самооценка студента. На основании обсуждения результатов выставляется дифференцированная оценка.

Программы учебной и производственной практик приведены в Приложении 3, 4, 5.

Вариативная часть

Б2.В.01 (У) Практика по получению первичных профессиональных умений и навыков

Учебная (по получению первичных профессиональных умений и навыков) практика (2 недели, (108 часов), 3 зачетных единицы) проводится на 1 курсе во втором семестре для очной формы обучения с целью углубления и закрепления первичных профессиональных знаний и навыков, полученных при теоретическом обучении и формирования компетенций:

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности;

ПК-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

ПК-11: способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;

ПСК-1: способность проводить совместный анализ функционального процесса защиты ТКС и ее информационных составляющих с целью определения возможных источников угроз, их вероятных целей;

ПСК-4: способность организовать реализацию принятых мер по управлению защитой информационных потоков на пакетном уровне с комплексной оценкой информационной безопасности ТКС.

Практика проводится с целью отработки студентами навыков решения задач по защите информации на современном компьютерном оборудовании и в сетях, закрепление теоретических знаний, полученные по дисциплинам: «Теоретические основы защиты информации», «Защищенные информационные технологии», ознакомление студентов с основными методами защиты информации на персональных компьютерах и в сетях в качестве индивидуального пользователя, расширения и систематизации

знаний по специализированным дисциплинам, изученным студентами в соответствии с учебным планом в течение 1 курса и подготовка студентов к дальнейшему углубленному изучению дисциплин своей специализации, а также расширение их круга знаний в области защиты информации и применения различных методов, процедур и пакетов программ для решения различных задач информационной безопасности

Учебная практика проводится на базе лабораторий кафедры «Информационной безопасности»: Аудитория 2210: Лаборатория управления информационной безопасностью; Аудитория 2210а: Лаборатория защищенных технических средств и систем; Аудитория 2206: Лаборатория технологий обеспечения информационной безопасности.

Итогом проведения учебной практики является овладение студентами навыками использования контрольно-проверочной аппаратуры, программных продуктов, применяемых в целях подразделений информационной безопасности (защиты информации), заполнения специальной документации.

Программой предусмотрены следующие виды контроля: промежуточная аттестация в форме зачета с оценкой во втором семестре для очной формы обучения.

Б2.В.02(У) Технологическая практика

Учебная (технологическая) практика (2 недели, (108 часов), 3 зачетных единицы) проводится на 2 курсе в четвертом семестре для очной формы обучения с целью углубления и закрепления первичных профессиональных знаний и навыков, полученных при теоретическом обучении и формирования компетенций:

ОК-1: способностью использовать основы философских знаний для формирования мировоззренческой позиции;

ОПК-2: способностью применять соответствующий математический аппарат для решения профессиональных задач;

ОПК-4: способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-5: способностью использовать нормативные правовые акты в профессиональной деятельности

ОПК-6: способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности;

ПК-2: способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

ПК-6: способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых

программных, программно-аппаратных и технических средств защиты информации;

ПК-7: способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;

ПК-9: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

ПК-10: способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;

ПК-11: способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;

ПК-13: способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;

ПК-14: способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности;

ПК-15: способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ПСК-1: способность проводить совместный анализ функционального процесса защиты ТКС и ее информационных составляющих с целью определения возможных источников угроз, их вероятных целей;

ПСК-4: способность организовать реализацию принятых мер по управлению защитой информационных потоков на пакетном уровне с комплексной оценкой информационной безопасности ТКС.

Практика проводится с целью отработки студентами навыков решения задач по защите информации на современном компьютерном оборудовании и в сетях, закрепление теоретических знаний, полученные по дисциплинам: «Теоретические основы защиты информации», «Защищенные информационные технологии», ознакомление студентов с основными методами защиты информации на персональных компьютерах и в сетях в качестве индивидуального пользователя, расширения и систематизации знаний по специализированным дисциплинам, изученным студентами в соответствии с учебным планом в течение 2 курса и подготовка студентов к дальнейшему углубленному изучению дисциплин своей специализации, а также расширение их круга знаний в области защиты информации и применения различных методов, процедур и пакетов программ для решения различных задач информационной безопасности

Учебная (технологическая) практика проводится на базе лабораторий кафедры «Информационной безопасности»: Аудитория 2210: Лаборатория управления информационной безопасностью; Аудитория 2210а: Лаборатория защищенных технических средств и систем; Аудитория 2206: Лаборатория технологий обеспечения информационной безопасности.

Итогом проведения учебной (технологической) практики является овладение студентами навыками использования контрольно-проверочной аппаратуры, программных продуктов, применяемых в целях подразделений информационной безопасности (защиты информации), заполнения специальной документации.

Программой предусмотрены следующие виды контроля: промежуточная аттестация в форме зачета с оценкой в четвертом семестре для очной формы обучения.

Б2.В.03 (П) Проектно-технологическая практика

Производственная (проектно-технологическая) практика (2 недели, (108 часов), 3 зачетных единицы) проводится на 3 курсе в шестом семестре для очной формы обучения, с целью углубления и закреп навыков, полученных при теоретическом обучении и формирования компетенций:

ОК-1: способностью использовать основы философских знаний для формирования мировоззренческой позиции;

ОК-6: способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия;

ОК-8: способность к самоорганизации и самообразованию;

ОПК-2: способностью применять соответствующий математический аппарат для решения профессиональных задач;

ОПК-3: способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач;

ОПК-4: способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-5: способностью использовать нормативные правовые акты в профессиональной деятельности;

ОПК-6: способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности;

ОПК-7: способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

ПК-2: способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

ПК-5: способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;

ПК-6: способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

ПК-7: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;

ПК-8: способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

ПК-9: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

ПК-10: способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;

ПК-11: способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;

ПК-12: способность принимать участие в проведении экспериментальных исследований системы защиты информации;

ПК-13: способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;

ПК-14: способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности;

ПК-15: способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ПСК-1: способность проводить совместный анализ функционального процесса защиты ТКС и ее информационных составляющих с целью определения возможных источников угроз, их вероятных целей;

ПСК-2: способность формировать предложения по оптимизации функционального процесса и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов;

ПСК-3: способность организовывать контроль и анализ защищенности объектов ТКС в соответствии с нормативными документами;

ПСК-4: способность организовать реализацию принятых мер по управлению защитой информационных потоков на пакетном уровне с комплексной оценкой информационной безопасности ТКС.

Производственная практика проводится с целью отработки студентами навыков решения задач по защите информации на современном компьютерном оборудовании и в сетях, закрепление теоретических знаний, полученные по дисциплинам: «Теоретические основы защиты информации», «Защищенные информационные технологии», ознакомление студентов с основными методами защиты информации на персональных компьютерах и в сетях в качестве индивидуального пользователя, расширения и систематизации знаний по специализированным дисциплинам, изученным студентами в соответствии с учебным планом в течение 3 курса и подготовка студентов к дальнейшему углубленному изучению дисциплин своей специализации, а также расширение их круга знаний в области защиты информации и применения различных методов, процедур и пакетов программ для решения различных задач информационной безопасности.

Производственная (проектно-технологическая) практика проводится на базе лабораторий кафедры «Информационной безопасности»: Аудитория 2210: Лаборатория управления информационной безопасностью; Аудитория 2210а: Лаборатория защищенных технических средств и систем; Аудитория 2206: Лаборатория технологий обеспечения информационной безопасности, на базе ЗАО «Клио», «НИИ КС им. А. А. Максимова» - филиала ФГУП «ГКНПЦ им М. В. Хруничева», 18 ЦНИИ МО, ООО «НОВО», НТЦ «ЗАРЯ».

Итогом проведения производственной (проектно-технологической) практики является овладение студентами навыками использования контрольно-проверочной аппаратуры, программных продуктов, применяемых в целях информационной безопасности (защиты информации) в специальных подразделениях по защите информации, заполнения специальной документации.

Программой предусмотрены следующие виды контроля: промежуточная аттестация в форме зачета с оценкой в шестом семестре для очной формы обучения.

Б2.В.04(П) Преддипломная практика

Производственная (преддипломная) практика (6 недель, (324 часа), 9 зачетных единиц) проводится на 4 курсе в восьмом семестре для очной формы обучения с целью углубления и закрепления профессиональных знаний и навыков, полученных при теоретическом обучении и формирования компетенций:

ОК-1: способностью использовать основы философских знаний для формирования мировоззренческой позиции;

ОК-2: способностью использовать основы экономических знаний в различных сферах деятельности;

ОК-3: способностью анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма;

ОК-4: способностью использовать основы правовых знаний в различных сферах деятельности;

ОК-5: способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;

ОК-6: способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия;

ОК-7: способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности;

ОК-8: способность к самоорганизации и самообразованию;

ОК-9: способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности;

ОПК-1: способностью анализировать физические явления и процессы для решения профессиональных задач;

ОПК-2: способностью применять соответствующий математический аппарат для решения профессиональных задач;

ОПК-3: способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач;

ОПК-4: способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-5: способностью использовать нормативные правовые акты в профессиональной деятельности;

ОПК-6: способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности;

ОПК-7: способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

ПК-2: способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

ПК-3: способность администрировать подсистемы информационной безопасности объекта защиты;

ПК-4: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

ПК-5: способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;

ПК-6: способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

ПК-7: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;

ПК-8: способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

ПК-9: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

ПК-10: способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;

ПК-11: способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;

ПК-12: способность принимать участие в проведении экспериментальных исследований системы защиты информации;

ПК-13: способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;

ПК-14: способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности;

ПК-15: способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ПСК-1: способность проводить совместный анализ функционального процесса защиты ТКС и ее информационных составляющих с целью определения возможных источников угроз, их вероятных целей;

ПСК-2: способность формировать предложения по оптимизации функционального процесса и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов;

ПСК-3: способность организовывать контроль и анализ защищенности объектов ТКС в соответствии с нормативными документами;

ПСК-4: способность организовать реализацию принятых мер по управлению защитой информационных потоков на пакетном уровне с комплексной оценкой информационной безопасности ТКС.

Производственная (преддипломная) практика проводится с целью ознакомления студентов с существующей системой информационной безопасности реального информационного объекта, с методами, средствами и силами, используемыми в этой системе, закрепления, расширения, углубления и систематизации знаний по общепрофессиональным дисциплинам, изученным студентами в соответствии с учебным планом в течение 1, 2, 3 и 4 курсов, в число которых входят такие дисциплины, как «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Техническая защита информации» и др., подготовка у студентов практической базы для осознанного изучения специальных дисциплин, отражающих специфику их будущей работы, которые будут изучаться ими в рамках учебного плана четвертого курса. В их число входят такие дисциплины, как «Информационная безопасность предприятия», «Инженерно-техническая защита информации», «Технические средства охраны» и другие, осуществить сбор материалов, которые можно будет использовать в дальнейшем при курсовом проектировании и написании выпускной квалифицированной работы.

Производственная (преддипломная) практика проводится на базе ЗАО «Клио», «НИИ КС им. А. А. Максимова» - филиала ФГУП «ГКНПЦ им М. В. Хруничева», 18 ЦНИИ МО, кафедры «Информационной безопасности», лабораторий кафедры «Информационной безопасности»: Аудитория 2210: Лаборатория управления информационной безопасностью; Аудитория 2210а: Лаборатория защищенных технических средств и систем; Аудитория 2206: Лаборатория технологий обеспечения информационной безопасности, ОАО «НОВО», НТЦ «ЗАРЯ».

Итогом проведения производственной (преддипломной) практики является овладение студентами навыками использования контрольно-проверочной аппаратуры, программных продуктов, применяемых в целях информационной безопасности (защиты информации) в специальных подразделениях по защите информации, заполнения специальной документации и подготовка материалов для написания ВКР.

Программой предусмотрены следующие виды контроля: промежуточная аттестация в форме зачета с оценкой в восьмом для очной

формы обучения и зачета с оценкой в десятом семестре для очно-заочной формы обучения.

ФТД. Факультативы

Факультативные дисциплины призваны углублять, расширять научные и прикладные знания обучающихся в соответствии с их потребностями, приобщать их к исследовательской деятельности, создавать условия для самоопределения личности и ее самореализации, обеспечивать разностороннюю подготовку профессиональных кадров.

Выбор факультативных дисциплин проводится обучающимися самостоятельно в соответствии с их потребностями.

Вариативная часть

ФТД.В.01 «Технико-экономическое обоснование проекта»

Дисциплина «Технико-экономическое обоснование проекта» относится к факультативным дисциплинам основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «История», «Основы права», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Основы информационной безопасности», «Криптографические методы защиты информации», а также компетенциях и компетенциях: ОК-3, 4; ОПК-2,4,5,6 и ПК-4,7,8,9,10,11,12,15.

Дисциплина направлена на формирование следующих компетенций:

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способностью применять соответствующий математический аппарат для решения профессиональных задач;

ОПК-3: способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач;

ОПК-4: способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-7: способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

ПК-2: способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

ПК-3: способность администрировать подсистемы информационной безопасности объекта защиты;

ПК-4: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

ПК-5: способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;

ПК-6: способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

ПК-7: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;

ПК-8: способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

ПК-9: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

ПК-10: способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;

ПК-11: способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;

ПК-12: способность принимать участие в проведении экспериментальных исследований системы защиты информации;

ПК-13: способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;

ПК-14: способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности;

ПК-15: способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ПСК-2: способность формировать предложения по оптимизации функционального процесса и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на

информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов;

ПСК-3: способность организовывать контроль и анализ защищенности объектов ТКС в соответствии с нормативными документами;

ПСК-4: способность организовать реализацию принятых мер по управлению защитой информационных потоков на пакетном уровне с комплексной оценкой информационной безопасности ТКС.

Целью курса является формирование знаний основам проектной деятельности. Выявлению существующих проблем в рамках обеспечения функционирования объекта информатизации и подготовке предложений по приведению существующей системы информационной безопасности объекта в соответствие требованиям предъявляемых регуляторами к таким системам в соответствии с существующей нормативной базой и представленными на рынке средствами обеспечения информационной безопасности объектов информатизации.

Содержание курса связано с разработкой обоснованных предложений по совершенствованию механизмов защиты обрабатываемого ресурса на предприятии (организации).

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме зачета в 5 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Разработка и реализация проекта», «Информационно-психологическая безопасность персонала предприятия», «Защита общества от информации, запрещенной к распространению», «Разработка политики информационной безопасности в организациях», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

ФТД.В.02 «Разработка и реализация проекта»

Дисциплина «Разработка и реализация проекта» относится к факультативным дисциплинам основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Технико-экономическое обоснование проекта», «История», «Основы права», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности»,

«Основы информационной безопасности», «Криптографические методы защиты информации», а также компетенциях и компетенциях: ОК-3,4; ОПК-2,3,4,5,6,7 и ПК-1,2,3,4,5,6,7,8,9,10,11,12,13,14,15; ПСК-2,3,4.

Дисциплина направлена на формирование следующих компетенций:

ОПК-3: способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач;

ОПК-4: способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-7: способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

ПК-2: способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

ПК-3: способность администрировать подсистемы информационной безопасности объекта защиты;

ПК-4: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

ПК-5: способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;

ПК-6: способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

ПК-7: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;

ПК-8: способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

ПК-9: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

ПК-10: способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;

ПК-11: способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;

ПК-12: способность принимать участие в проведении экспериментальных исследований системы защиты информации;

ПК-13: способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;

ПК-14: способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности;

ПК-15: способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ПСК-2: способность формировать предложения по оптимизации функционального процесса и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов;

ПСК-3: способность организовывать контроль и анализ защищенности объектов ТКС в соответствии с нормативными документами;

ПСК-4: способность организовать реализацию принятых мер по управлению защитой информационных потоков на пакетном уровне с комплексной оценкой информационной безопасности ТКС.

Целью курса является формирование знаний основам проектной деятельности. Обоснование предложений по приведению системы информационной безопасности объекта информатизации в соответствие с уточненными требованиями предъявляемые к такого рода системам в соответствии с существующей нормативно-правовой базой.

Содержание курса связано с разработкой обоснованных предложений по совершенствованию механизмов защиты обрабатываемого ресурса на предприятии (организации). Проведение технико-экономических обоснований предлагаемых вариантов решения выявленных проблем, связанных с обеспечением системы информационной безопасности объекта информатизации. Осуществление нормативно-правового закрепления предложений в существующей системе документационного обеспечения управления предприятием (организацией) в рамках бесперебойного, функционирования системы информационной безопасности объекта информатизации.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа. Преподавание дисциплины ведется на 3 курсе в 6 семестре и в 7 семестре для очной формы обучения и предусматривает проведение учебных занятий следующих видов: практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме зачета с оценкой и курсового проекта, в 6 семестре для очной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

5. Фактическое ресурсное обеспечение ОПОП ВО по направлению подготовки 10.03.01 Информационная безопасность

ОПОП ВО бакалавриата «Информационная безопасность» обеспечена учебно-методической документацией и материалами по всем учебным дисциплинам, содержание каждой из учебных дисциплин представлено в сети Интернет на сайте Университета (<http://unitech-mo.ru/>).

Учебно-методическое и информационное обеспечение основывается как на традиционных, так и на новых телекоммуникационных технологиях, что соответствует требованиям ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность» (бакалавриат).

Основная профессиональная образовательная программа обеспечена учебно-методической документацией и материалами по всем учебным дисциплинам основной профессиональной образовательной программы. Содержание каждой из таких учебных дисциплин представлено в локальной сети образовательного учреждения.

Внеаудиторная работа обучающихся сопровождается методическим обеспечением и обоснованием времени, затрачиваемого на ее выполнение. Каждый обучающийся обеспечен доступом к электронно-библиотечной системе, содержащей издания по основным изучаемым дисциплинам и сформированной по согласованию с правообладателями учебной и учебно-методической литературы. При этом обеспечена возможность осуществления одновременного индивидуального доступа к такой системе всех обучающихся.

Библиотечно-информационное обеспечение учебного процесса осуществляется библиотекой Университета, которая удовлетворяет требованиям Федерального закона № 273-ФЗ «Об образовании в РФ» и ФГОС (ВО).

Основная задача библиотеки – полное и оперативное библиотечное и информационно-библиографическое обслуживание студентов, аспирантов, научных работников, профессорско-преподавательского состава, инженерно-технического персонала и других категорий читателей Университета в соответствии с информационными запросами на основе неограниченного доступа к электронным библиотечным системам (ЭБС) в соответствии с договорами, заключенными Университетом. Библиотека обеспечивает 100% охват научно-педагогических работников и обучающихся Университета

Библиотечный фонд МГОТУ укомплектован печатными и (или) электронными учебными изданиями по всем дисциплинам, входящим в реализуемые основные образовательные программы и специальности МГОТУ.

Основная и дополнительная учебная и учебно-методическая литература представлена в библиотеке в полном объеме. Источники учебной информации по всем дисциплинам учебных планов отличаются современным содержанием. Основная учебная и учебно-методическая литература, рекомендованная в качестве обязательной, отвечает требованиям ФГОС (ВО).

Библиотечный фонд укомплектован печатными изданиями из расчета не менее 50 экземпляров каждого из изданий основной литературы, перечисленной в рабочих программах дисциплин (модулей), практик, и не менее 25 экземпляров дополнительной литературы на 100 обучающихся. Фонд дополнительной литературы, помимо учебной, включает официальные, справочно-библиографические и специализированные периодические издания в расчете 1-2 экземпляра на каждые 100 обучающихся.

Библиотека использует современные информационные технологии для обеспечения высокого уровня образовательного процесса.

Значительная часть учебной и учебно-методической литературы представлена для изучения студентам в электронно-библиотечных системах и других электронных ресурсах, ссылки на которые доступны из раздела библиотеки на сайте Университета, а также в электронном каталоге библиотеки. Каждый обучающийся в Университете обеспечен доступом к электронно-библиотечным системам (ЭБС), которые содержат различные издания для информационного обеспечения образовательного и научно-исследовательского процесса.

Университет обеспечивает доступ к **7 электронным ресурсам**, которые включают электронно-библиотечные системы с единой точкой доступа, электронные библиотеки и полнотекстовые зарубежные базы: *Электронно-библиотечная система «Университетская библиотека онлайн»*; *Национальная электронная библиотека*; *«Национальный цифровой ресурс «Рукопт»*; *Электронно-библиотечная система «ИНФРА-М» ZNANIUM.com*; *Электронно-библиотечная система «Издательство «Лань»*; *Электронно-библиотечная система «Издательство «Юрайт»*; *международная база данных Ebrary*.

Университет является полноправным участником проекта «Сетевой университет» с ЭБС Лань.

На основе информационно-библиотечной системы «АИБС MARK-SQL» автоматизированы все основные технологические процессы. Обслуживание читателей ведется по персональному электронному билету на основе штрихового кодирования.

Для проведения анализа и получения информации об обеспеченности преподаваемых дисциплин в библиотеке формируется картотека книгообеспеченности в рамках подсистемы АИБС MARK SQL. Электронная

картотека книгообеспеченности формируется на основании данных дисциплин, предоставляемых учебными подразделениями Университета. Среди предоставляемых данных: учебная и учебно-методическая литература, электронные издания и периодические издания. Сведения по картам обеспеченности заносятся в модуль «Книгообеспеченность» для специалитета, бакалавриата и магистров. Такая же процедура получения и внесения данных происходит и для среднего профессионального образования. Учебная литература приобретается в библиотеку по заявкам учебных подразделений согласно нормативам.

Основным инструментом, обеспечивающим оперативный доступ к электронным ресурсам библиотеки и электронно-библиотечной системе, является Web-сайт, на котором формируется электронная библиотека. Сайт предоставляет возможность студентам и профессорско-преподавательскому составу Университета обратиться к основному фонду учебной и научной литературы посредством электронного каталога. Поиск необходимых документов возможен по типам: «Автор», «Название», «Ключевые слова», «Поиск по словарям». Реализована возможность единого поиска электронных и печатных изданий через электронный каталог.

Обеспечена возможность индивидуального неограниченного доступа к содержимому ЭБС из любой точки, в которой имеется доступ к сети Интернет, с предоставлением каждому обучающемуся возможности использования индивидуального логина и пароля для доступа к содержимому ЭБС в любое время и из любого места, без ограничения возможностей доступа каким-либо помещениями, территорией, временем или продолжительностью доступа, IP-адресами, точками доступа и другими причинами для ограничения. Университет обеспечивает доступ к ЭБС в соответствии с требованиями Федеральных государственных образовательных стандартов высшего образования и среднего профессионального образования для 100% обучающихся по всем образовательным программам, обеспечивается возможность полнотекстового поиска по содержимому ЭБС, предоставление изданий с сохранением вида страниц (оригинальной вёрстки) и формирования статистического отчета. В библиотеке Университета есть читальный зал, в котором имеются автоматизированные рабочие места, оснащенные компьютерами, подключёнными к Интернет. Обслуживание студентов всех форм обучения бесплатное.

Оперативный обмен информацией с отечественными и зарубежными вузами и организациями осуществляется с соблюдением требований законодательства Российской Федерации об интеллектуальной собственности и международных договоров Российской Федерации в области интеллектуальной собственности. Для обучающихся обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам.

Университет располагает материально-технической базой, обеспечивающей проведение всех видов дисциплинарной и

междисциплинарной подготовки, лабораторной, практической и научно-исследовательской работы обучающихся, которые предусмотрены учебным планом, и соответствующей действующим санитарным и противопожарным правилам и нормам.

Кадровое обеспечение

Доля научно-педагогических работников, имеющих образование и (или) ученую степень, соответствующее профилю преподаваемой дисциплины (модуля), в общем числе научно-педагогических работников, реализующих программу бакалавриата, составляет не менее 70%.

Доля научно-педагогических работников (в приведенных к целочисленным значениям ставок), имеющих ученую степень (в том числе ученую степень, присвоенную за рубежом и признаваемую в РФ) и (или) ученое звание (в том числе ученое звание, полученное за рубежом и признаваемое в РФ), в общем числе научно-педагогических работников реализующих программу бакалавриата, составляет не менее 50%.

Доля работников (в приведенных к целочисленным значениям ставок) из числа руководителей и работников организаций, деятельность которых связана с направленностью (профилем) реализуемой программы (имеющих стаж работы в данной профессиональной области не менее 3 лет) в общем числе работников, реализующих программу бакалавриата, составляет не менее 5%.

Материально-техническое обеспечение

Перечень материально-технического обеспечения:

- лекционные аудитории (оборудованные учебной мебелью, наглядными учебными пособиями и видеопроекторным оборудованием для презентаций, средствами звуковоспроизведения, экраном, и имеющие выход в Интернет);

- помещения для проведения семинарских, практических и лабораторных занятий (оборудованные учебной мебелью, видеопроекторным оборудованием для презентаций, средствами звуковоспроизведения, экраном, и имеющие выход в Интернет, компьютерная техника оснащена специализированным программным обеспечением);

- библиотеку (имеющую рабочие места для студентов, оснащенные компьютерами с доступом к базам данных и Интернет);

- компьютерные классы, учебно-научные лаборатории при кафедре информационной безопасности для проведения исследований: Аудитория 2210: Лаборатория управления информационной безопасности; Аудитория 2210а: Лаборатория защищенных технических средств и систем; Аудитория 2206: Лаборатория технологий обеспечения информационной безопасности.

При использовании электронных изданий Университет обеспечивает каждого обучающегося во время самостоятельной подготовки рабочим местом в компьютерном классе с выходом в Интернет в соответствии с

объемом изучаемых дисциплин из расчета не менее 1 точки удаленного доступа к сети Интернет на 4 студентов.

В случае необходимости применения электронного обучения, дистанционных образовательных технологий возможна замена специально оборудованных помещений их виртуальными аналогами, позволяющими обучающимся осваивать умения и навыки, предусмотренные профессиональной деятельностью.

Университет обеспечен необходимым комплектом лицензионного программного обеспечения, включающим пакеты наиболее распространенных программ прикладного характера для целей анализа социологических данных.

Финансовое обеспечение

Условия финансового обеспечения образовательной программы по направлению подготовки 10.03.01 Информационная безопасность определяются в соответствии с требованиями федерального государственного образовательного стандарта.

Финансовое обеспечение реализации программы бакалавриата осуществляется в объеме не ниже установленных Министерством образования и науки Российской Федерации базовых нормативных затрат на оказание государственной услуги в сфере образования для данного уровня образования и направления подготовки с учетом корректирующих коэффициентов, учитывающих специфику образовательных программ.

6. Характеристики среды Университета, обеспечивающие развитие общекультурных и социально-личностных компетенций выпускников

В Университете созданы и поддерживаются условия для развития личности и регулирования социально-культурных процессов, способствующих укреплению нравственных, гражданственных, общекультурных качеств обучающихся, для формирования общекультурных (социально-личностных) компетенций выпускников.

Концепция формирования среды Университета, обеспечивающей развитие социально-личностных компетенций обучающихся, определяется регламентирующими документами.

В формировании социокультурной среды и в воспитательной деятельности участвуют такие подразделения академии, как отдел организационно-массовой работы (далее – Отдел), центр развития студенческого творчества (далее – Центр). Их целевым предназначением является:

- проведение работы по эстетическому, духовно-нравственному, гражданскому и трудовому воспитанию и психологическому просвещению студентов;
- организация внеучебной работы всех уровней факультет, курс, группа);

- организация работы по профилактике негативных явлений в среде вузовской молодежи;

- содействие работе органов студенческого самоуправления, поддержка деятельности студентов по социально-значимой работе и проведению различных мероприятий Подмосковья, г. Королева.

В своей деятельности Отдел и Центр руководствуются Конституцией и законодательными актами РФ, нормативными документами Министерства образования и науки Российской Федерации, Уставом Университета, Положениями о работе Центра и Отдела, приказами и распоряжениями ректора Университета.

В Университете функционируют различные творческие объединения:

- театральная студия;
- танцевальные студии современного, эстрадно-спортивного танца;
- студии эстрадного и народного вокала;
- Лига КВН;
- студенческая редакция газеты «Молодежный формат»;
- Театр мод;
- фотоклуб.

На постоянной основе работают:

- Дискуссионный политклуб, цель которого – выработать навыки самостоятельного мышления, оценки современной ситуации, умения анализировать события и отстаивать собственную точку зрения;

- клуб Интернациональной дружбы, цель которого – объединение, сплочение студентов всех национальностей.

В Университете созданы и поддерживаются традиции:

- Посвящение первокурсников в студенты.
- Татьянин День (День Студента).
- Закладка аллеи первокурсников.
- Митинг «Вахта Памяти».
- Встреча с ветеранами.
- Торжественная церемония вручения дипломов «Выпускник».
- Участие студентов в творческих фестивалях, конкурсах и концертах академии (фестиваль студенческого творчества; отчетный концерт творческих коллективов; конкурс военно-патриотической песни, Мистер и Мисс Университет, «Фестос», «Студенческая весна Подмосковья» и т. д.) способствуют развитию творческих талантов у молодежи, формирует правильные увлечения.

Ежегодно проводятся конкурсы среди студентов и преподавателей на звание «Лучший преподаватель года», «Лучший студент года», «Лучшая академическая группа», «Лучший куратор», «Лучшая кафедра», «Лучший преподаватель».

Ежегодно в Университете проводятся культурно-массовые и спортивно-массовые студенческие мероприятия, крупные межвузовские мероприятия, в том числе, фестивали и игры Королевской Лиги КВН, в

которых участвуют команды вузов Москвы и Подмосковья. В Университете активно развивается студенческое самоуправление в лице Студенческого Совета и факультетов. Работает студенческая служба порядка. Созданы студенческое научное общество по специальностям академии. Цель студенческой научной работы – создание условий для раскрытия творческих способностей студентов в сфере научной деятельности и формирования у них навыков ведения научных исследований. Студенты – члены СНО – участвуют в студенческих конференциях, семинарах, круглых столах, конкурсах научных работ и инновационных проектах, организации «Недели науки», других научно-практических и научно-технических мероприятиях. Проводятся встречи студентов с ведущими учеными и специалистами. Формируются творческие коллективы студентов, выполняющих научные исследования на конкурс грантов.

В Университете функционирует Центр социально-психологической поддержки. Его работа осуществляется подготовленными квалифицированными специалистами. Центром реализуются программы по профилактике наркотической, алкогольной зависимостей и табакокурения, а также программы по профилактике правонарушений. Деятельность Центра осуществляется в тесном сотрудничестве с Королёвским наркологическим диспансером. В рамках своей работы Центр проводит следующие мероприятия:

- тренинги по адаптации студентов первого курса к условиям обучения в вузе;
- тематические тренинги по запросу руководителей структурных подразделений;
- индивидуальные консультации для студентов, родителей и сотрудников Университета.

В Центре действует студенческий «Психологический клуб» и «Телефон доверия». В подразделениях также проводятся тематические акции, по пропаганде здорового образа жизни: дни здоровья, круглые столы, лекции с привлечением различных специалистов.

Большое внимание в воспитательной работе уделяется организации досуга и отдыха студентов. Они имеют возможность провести каникулы в студенческих лагерях (зимой – в Подмосковье, летом – на побережье Черного моря); посещать музеи; совершать экскурсии по городам «Золотого кольца России».

Студенты, проявляющие интерес к спорту, могут заниматься в спортивных секциях по мини-футболу, волейболу и баскетболу. Функционируют два спортивных зала, два тренажерных зала, спортивная площадка.

Имеются пункты общественного питания: столовые и буфеты.

Лечебно-оздоровительная работа осуществляется здравпунктом Университета.

7. Нормативно-методическое обеспечение системы оценки качества освоения обучающимися ОПОП ВО по направлению подготовки 10.03.01 «Информационная безопасность» (ФГОС)

В соответствии с ФГОС ВО бакалавриата по направлению подготовки 10.03.01 «Информационная безопасность» (уровень - бакалавр) оценка качества освоения обучающимися образовательной программы включает:

- текущий контроль успеваемости;
- промежуточную аттестацию;
- государственную итоговую аттестацию обучающихся.

Нормативно-методическое обеспечение текущего контроля успеваемости и промежуточной аттестации обучающихся (зачетно-экзаменационной сессии) по ОПОП ВО осуществляется в соответствии с утвержденными в Университете документами:

- Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся.
- Положение об организации и проведении компьютерного тестирования текущих знаний студентов.

Студенты, обучающиеся в Университете по образовательным программам высшего образования, при промежуточной аттестации сдают в течение учебного года не более 10 экзаменов и 12 зачетов. В указанное число не входят экзамены и зачеты по физической культуре и факультативным дисциплинам.

Для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям соответствующей ОПОП ВО вуз создает и утверждает фонды оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации. Эти фонды включают:

- контрольные вопросы и типовые задания для практических занятий, лабораторных и контрольных работ, коллоквиумов, зачетов и экзаменов;
- тесты для компьютерных тестирующих программ;
- примерную тематику курсовых работ/проектов, рефератов и т.п.

Эти формы контроля позволяют оценить степень сформированности компетенций обучающихся.

Государственная итоговая аттестация ОПОП ВО «Информационная безопасность» включает в себя защиту выпускной квалификационной работы бакалавра.

Требования к содержанию, объему и структуре выпускной квалификационной работы (бакалаврской работы), определяются методическими указаниями по выполнению выпускной квалификационной работы.

Сроки подготовки и графики защиты бакалаврской выпускной квалификационной работы устанавливаются ежегодно в соответствии рабочим учебным планом.

Разработаны и утверждены требования к содержанию, объему и структуре выпускных квалификационных работ (ВКР), а также рекомендованные тематики ВКР.

Процедура государственной итоговой аттестации выпускников с ограниченными возможностями здоровья и инвалидов предусматривает предоставление необходимых технических средств и оказание технической помощи при необходимости.

При необходимости обучающимся предоставляется дополнительное время для подготовки ответа.

В Университете ежегодно по утвержденным показателям проводится мониторинг процессов, обеспечивающих качество подготовки выпускников.

По ежегодно утверждаемой программе в Университете проводятся внутренние аудиты деятельности подразделений, отдельных процессов и видов деятельности, по результатам которых планируются корректирующие и предупреждающие мероприятия, способствующие повышению качества подготовки специалистов.

Компетентность преподавателей отслеживается и оценивается на основе утвержденных в Университете регламентов:

- Положение о порядке замещения должностей научно-педагогических работников Университета.
- Фонды оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации.

8. Академическая мобильность

Академическая мобильность является неотъемлемой составляющей международной деятельности Технологического университета. Кроме того, это важный инструмент в обеспечении качества образования и его соответствия международным стандартам.

В своей международной деятельности, направленной на повышение рейтинга Университета в системе высшего образования России и дальнейшую интеграцию в мировое образовательное и научное пространство, ГБОУ ВО МО «Технологический университет» опирается в первую очередь на тех студентов, аспирантов и преподавателей, которые готовы представлять вуз на международной арене. С 2010 года в «МГОТУ» начато обучение иностранных студентов. В настоящее время в ГБОУ ВО МО «Технологический университет» по различным формам обучаются студенты из Туркменистана, Украины, Армении, Таджикистана, Турции, Азербайджана, Беларуси, Молдовы, Казахстана, Киргизии, Узбекистана, Латвии, Грузии. С каждым годом численность иностранных студентов увеличивается. С целью более активной интернационализации иностранных граждан в «МГОТУ» создан Интернациональный клуб, проводится Фестиваль национальных культур, организуются экскурсии по Москве и Подмосковию.

Академическая мобильность студентов, профессорско-преподавательского и административного штата вуза осуществляется по трем направлениям:

- двухсторонние межвузовские соглашения с зарубежными партнерами;
- в рамках программы академических обменов Евросоюза Erasmus +;
- по линии Министерства образования и науки РФ.

Срок обучения или научной стажировки может составлять от 1 месяца до 1 семестра.

Университет активно участвует в международных программах по различным формам академической мобильности с вузами-партнерами, в том числе в рамках программы «Приглашенный профессор». Ежегодно Технологический университет с целью обмена опытом посещают преподаватели и административные работники зарубежных университетов, со своей стороны преподаватели «МГОТУ» также выезжают в зарубежные вузы.

Академическая мобильность студентов в рамках Erasmus+ позволяет участникам проекта не только ознакомиться с зарубежным опытом обучения, но и приобрести навыки коммуникативного общения с представителями других культур и религий, совершенствовать знания иностранного языка и ознакомиться с культурным наследием страны пребывания. Опыт показывает, что почти все студенты, прошедшие обучение в «МГОТУ», хотели бы вернуться сюда еще раз.

Международные научно-практические конференции «Инновационные технологии в современном образовании» и «Перспективы, организационные формы и эффективность развития сотрудничества российских и зарубежных вузов», организуемые в «МГОТУ», проводятся в координации с вузами-партнерами. В работе конференций представители зарубежных университетов принимают участие как в очной форме, так и в режиме онлайн.

Заклучены рамочные соглашения с рядом высших учебных заведений Италии, Германии, Великобритании, Швейцарии, Болгарии, Чехии, Латвии, Словакии, Хорватии и ряда других стран мира. В рамках подписанных соглашений обучающиеся проходят языковые стажировки за рубежом, реализуются совместные научно-образовательные проекты. По приглашению зарубежных партнеров сотрудники «МГОТУ» принимают участие в научных конференциях, выступая с докладами, и публикуют статьи в научных сборниках.

Университет зарегистрирован в международной системе признания вузов АНАБИН, присвоен статус «Н+», позволяющий выпускникам нострифицировать свои дипломы в странах ЕС и участвовать в тендерах на получение научно-исследовательских и европейских образовательных грантов. Подписано Соглашение о сотрудничестве между ГБОУ ВО МО «Технологический университет» и Россотрудничеством - головным

ведомством, на которое возложена координация международного сотрудничества России в гуманитарной сфере. ГБОУ ВО МО «Технологический университет» стал первым региональным вузом, подписавшим подобный документ с Россотрудничеством. При поддержке Федерального Агентства с целью продвижения российского образования за рубежом ГБОУ ВО МО Технологический университет активно участвует в международных выставках образования в Туркменистане и Узбекистане, организует Дни открытых дверей и круглые столы на площадках представительств Россотрудничества в различных странах. Такие мероприятия способствуют привлечению иностранных граждан к получению высшего образования в Российской Федерации.

В настоящее время партнёрами «Технологический университет» являются более 30 зарубежных вузов и организаций: Россотрудничество, Витебский государственный технологический университет (Республика Беларусь), Хмельницкий национальный университет (Украина), Университет EuroSwiss (Швейцария), Университет Модены и Реджио-Эмилия (Италия), Университет «1 декабря 1918» Алба Юлия (Румыния), Рижский технический университет (Латвия), Русенский университет им. Ангел Кънчев (Болгария), Новый болгарский университет (Болгария), Гродненский государственный университет им. Я.Купалы (Белоруссия), Финансовая академия (Казахстан), Политехнический университет Меджимурья (Хорватия), Культурный центр им. Д.Неру при Посольстве Индии в Москве и ряд других зарубежных университетов.

Перечень необходимых приложений

Приложение 1. Календарный учебный график.

Приложение 2. Учебный план.

Приложение 3. Программа учебной практики (практика по получению первичных профессиональных умений и навыков, технологическая практика).

Приложение 4. Программа производственной практики (проектно-технологическая практика, преддипломная практика).

Приложение 5. Методические рекомендации по написанию Выпускной Квалификационной Работы

Приложение 2. Учебный план (ФОО)

МИНИСТЕРСТВО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ

Государственное бюджетное образовательное учреждение высшего образования Московской области «Технологический университет»

План одобрен Ученым советом факультета
Протокол № 9 от 28.04.2020

УЧЕБНЫЙ ПЛАН

по программе Бакалавриата

10.03.01

Направление Информационная Безопасность.

Профиль Безопасность телекоммуникационных систем (в аэрокосмической сфере)

Кафедра: Информационной Безопасности
Институт: Информационных систем и технологий

Квалификация: Бакалавр

Программа подготовки: государственная

Форма обучения: Очная

Срок обучения: 4а

| | | |
|---|----------|------------------------------------|
| + | Основной | Будь внимательным! |
| + | + | экспериментально-исследовательская |
| + | + | организационно-управленческая |
| + | + | эксплуатационная |
| + | + | проектно-технологическая |

Год начала подготовки (по учебному плану) 2020

Образовательный стандарт № 1515 от 01.12.2016

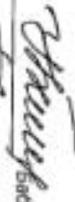
СОГЛАСОВАНО

Проректор по учебно-методической работе

Начальник учебно-методического управления

Директор института

Зам. кафедры

 В.В. Бабина Н.В./
 Т.В. Трахтина Т.В./
 В.Г. Бочаренко В.Г./
 В.Н. Соловьев В.Н./



 Т.Е. Смирнова Т.Е.



Государственное бюджетное образовательное учреждение высшего образования
Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ

Б2.В.01 (У) Практика по получению первичных профессиональных умений и навыков

Б2.В.02 (У) Технологическая практика.

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: «Безопасность телекоммуникационных систем (в аэрокосмической сфере)»

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Год набора: 2020

Королев
2020

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ УЧЕБНОЙ ПРАКТИКИ

Учебная практика - является важнейшей составной частью учебного процесса по подготовке специалистов в соответствии с основной профессиональной образовательной программой высшего образования (далее – ОПОП ВО), реализуемой Государственным бюджетным образовательным учреждением высшего образования Московской области «Технологический университет» (далее – Университет) по направлению подготовки 10.03.01 «Информационная безопасность» и обеспечивают системно - деятельностный подход в подготовке бакалавров в области организации и технологии защиты информации, нарушениям в области информационной безопасности.

Учебная практика подразделяется на следующие типы:

- практика по получению первичных профессиональных умений и навыков;
- технологическая практика.

Целями учебной практики являются:

- систематизация, закрепление и углубление теоретических знаний, полученных в процессе обучения в Университете;
- приобретение необходимых практических умений и навыков работы в соответствии с выбранным направлением профессиональной подготовки;
- развитие и накопление специальных практических навыков для решения профессиональных задач;
- развитие профессионального мышления;
- приобретение первоначальных профессиональных умений в области организации и технологии защиты информации.

Задачи учебной практики:

- ознакомление с управленческой структурой предприятия или организации, функциональными обязанностями работников отдела, занимающихся внешнеэкономической деятельностью;
- ознакомление с управленческой структурой таможенного органа, функциональными обязанностями сотрудников таможенной службы;
- сбор, обобщение и анализ материалов в соответствии с программой практики и индивидуальным заданием, определяемых конкретным местом прохождения практики;
- овладение первичными навыками на конкретном рабочем месте.

Учебная практика проводится на базе академических кафедр и лабораторий. По форме проведения учебная практика является камеральной, не требует командирования студентов и проводится на базе Университета. Для прохождения практики, как правило, формируются группы студентов.

Перечень планируемых результатов обучения при прохождении практики

В процессе прохождения учебной практики студент приобретает и совершенствует следующие компетенции:

Б2.В.01 (У) Практика по получению первичных профессиональных умений и навыков:

ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности;

ПК-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

ПК-11: способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;

ПСК-1: способность проводить совместный анализ функционального процесса защиты ТКС и ее информационных составляющих с целью определения возможных источников угроз, их вероятных целей;

ПСК-4: способность организовать реализацию принятых мер по управлению защитой информационных потоков на пакетном уровне с комплексной оценкой информационной безопасности ТКС.

Б2.В.02 (У) Технологическая практика:

ОК-1: способностью использовать основы философских знаний для формирования мировоззренческой позиции;

ОПК-2: способностью применять соответствующий математический аппарат для решения профессиональных задач;

ОПК-4: способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-5: способностью использовать нормативные правовые акты в профессиональной деятельности

ОПК-6: способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности;

ПК-2: способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

ПК-6: способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты

информации;

ПК-7: способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;

ПК-9: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

ПК-10: способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;

ПК-11: способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;

ПК-13: способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;

ПК-14: способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности;

ПК-15: способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ПСК-1: способность проводить совместный анализ функционального процесса защиты ТКС и ее информационных составляющих с целью определения возможных источников угроз, их вероятных целей;

ПСК-4: способность организовать реализацию принятых мер по управлению защитой информационных потоков на пакетном уровне с комплексной оценкой информационной безопасности ТКС.

Итогом проведения учебной практики является овладение студентами навыков использования контрольно-проверочной аппаратуры, программных продуктов, применяемых в таможенных органах, заполнения таможенной документации.

2. Место учебной практики в структуре ОПОП ВО

Учебная практика относится к обязательному разделу ОПОП ВО по направлению подготовки 10.03.01 «Информационная безопасность» и базируется на ранее изученных дисциплинах:

- Философия;
- История;
- Иностранный язык;
- Безопасность жизнедеятельности;

- Экономика предприятия и организация производства;
- Основы права;
- Основы управленческой деятельности;
- Документоведение;
- Линейная алгебра и аналитическая геометрия;
- Математический анализ;
- Теория графов;
- Теория информации;
- Теория вероятностей и математическая статистика;
- Дискретная математика;
- Физика;
- Информатика;
- Языки программирования;
- Основы информационной безопасности;
- Математическая логика и теория алгоритмов;
- Информационные процессы (системы) и их безопасность;
- Психология;
- Введение в профессию;
- Русский язык и культура речи;
- Пакеты прикладных программ;
- Операционные системы, среды и оболочки;
- Пакеты прикладных математических программ;
- Социально-психологические основы управленческой деятельности.

Знания и компетенции, полученные при освоении учебной практики, являются базовыми при изучении ряда последующих дисциплин и выполнении выпускной квалификационной работы бакалавра.

3. Объем практики в зачетных единицах и ее продолжительность

Общая трудоёмкость учебной практики составляет 216 часов, 6 зачетных единиц.

Трудоёмкость учебной практики по получению первичных профессиональных умений и навыков составляет 108 часов, 3 зачетные единицы. Проводится после первого курса во 2 семестре, продолжительностью 2 недели для очной формы обучения.

Трудоёмкость технологической практики составляет 108 часов, 3 зачетные единицы. Проводится после второго курса в 4 семестре, продолжительностью 2 недели для очной формы обучения.

4. Содержание учебной практики

В процессе прохождения практики активно используется обучение на основе опыта, применяется исследовательский метод, в рамках которого предполагается самостоятельный поиск материала, по заданиям, которые указаны в программе практики.

В процессе прохождения учебной практики студент может обращаться за консультациями и помощью в решении отдельных вопросов, связанных с прохождением учебной и производственной практик к преподавателю кафедры Информационной безопасности, назначенному руководителем учебной и производственной практиками студентов, осуществляющему текущее руководство практикой.

Сроки сдачи и защиты отчетов по учебной практике устанавливает руководителем учебной практикой студентов. Содержание учебной практики определяется выпускающей кафедрой Информационной безопасности в соответствии с учебным планом и программой, с учетом специфики деятельности организации, которую изучают студенты в рамках учебной и производственной практик.

Основные виды работ на практике, включая самостоятельную работу студентов, представлены в Таблице 1. Во время учебной практики студенты также выполняют индивидуальное задание, в соответствии со списком предлагаемых направлений. В отчете данная часть отражается в виде описания личных функциональных обязанностей, реализуемых студентом или практических результатов, достигнутых в ходе прохождения практики.

Программой учебной практики при разработке индивидуальных заданий предусматривается соблюдение следующих требований:

- учет уровня теоретической подготовки студента по дисциплинам гуманитарного, социально-экономического цикла, математического и естественнонаучного цикла и профессионального цикла к моменту проведения практики;
- доступность и практическая возможность сбора исходной информации, как в организации, так и с использованием иных источников информации, в том числе сети интернет.

По результатам прохождения практики студентами составляется отчет по учебной практике. Содержание данного отчета определяется спецификой выбранной темы ВКР; объем – не более 10 страниц в отдельном разделе общего отчета. Отчет по индивидуальному занятию визируется руководителем работы. Качество выполнения программы практики учитывается при вынесении общей оценки практики.

Наиболее интересные результаты работ докладываются на конференциях студентов, молодых ученых и аспирантов, организуемых МГОТУ, ИТФ или кафедрой Информационной безопасности. Материалы из лучших отчетов могут быть рекомендованы для представления на открытый конкурс научных работ среди студентов вузов России.

Таблица 1

| № п/п | Виды работ (график) на учебной практике, включая самостоятельную работу студентов в аудиториях Университета | Трудоемкость (в часах) |
|-------|---|------------------------|
| 1 | 2 | 3 |
| 1 | Прохождение вводного инструктажа по организации и проведению практики, выдача индивидуальных заданий. | 1 |

| | | |
|---|--|-----|
| 2 | Прохождение первичного инструктажа по охране труда на рабочем месте ознакомление с современными средствами вычислительной техники, коммуникаций и связи, используемых в процессе обучения. | 1 |
| 3 | Краткая характеристика используемых методов по защите информации и программных продуктов, используемых при отработке практических заданий (таблица №2) | 2 |
| 4 | Выполнение практических заданий по десяти упражнениям учебно-технологической практики в рамках индивидуального задания | 98 |
| 5 | Подготовка и оформление отчета по учебно-технологической практике | 4 |
| 6 | Представление отчета по учебно-технологической практике руководителю и защита результатов работы студентами | 2 |
| | Итого: в часах (у/п) | 108 |

Таблица 2

Отработка упражнений по защите информации на ПК и в сетях в качестве индивидуального пользователя

| № п/п | Наименование упражнений на учебной практике, включая самостоятельную работу студентов в аудиториях Университета | Трудоемкость (в часах) |
|--------------|--|-------------------------------|
| 1 | 2 | 3 |
| 1 | Упражнение №1. Восстановление зараженных макровирусами файлов. | 9 |
| 2 | Упражнение №2. Профилактика проникновения «Троянских программ» в операционную систему ПК. | 9 |
| 3 | Упражнение №3. Настройка безопасности почтового клиента при передаче и получении сообщений по электронной почте. | 9 |
| 4 | Упражнение №4. Настройка параметров аутентификации пользователей в операционной системе ПК. | 9 |
| 5 | Упражнение №5. Применение шифрующей файловой системы и управление сертификатами в операционной системе ПК. | 9 |
| 6 | Упражнение №6. Назначение прав пользователей при произвольном управлении доступом в операционной системе ПК. | 9 |
| 7 | Упражнение №7. Настройка параметров регистрации и аудита в операционной системе ПК. | 9 |
| 8 | Упражнение №8. Управление шаблонами безопасности в операционной системе ПК. | 9 |
| 9 | Упражнение №9. Настройка и использование межсетевых | 18 |

| | | |
|----|--|-----|
| | экрана | |
| 10 | Упражнение №10.Создание виртуального подключения средствами операционной системы ПК. | 18 |
| | Итого: в часах (у/п) | 108 |

Методические рекомендации для самостоятельной работы по индивидуальным заданиям

Учебная практика студентов проводится в форме самостоятельной практической работы под руководством преподавателя. Учебная практика студентов строится с учетом специфики объекта практики (информационного объекта), в соответствии с тематическим планом, примерное содержание которого соответствует списку тем индивидуальных заданий:

1. Разработка системы защиты персональных данных в АС ГУП Моссоцрегистр. (общая характеристика ГУП Моссоцрегистр, как объекта ИБ, состав и структура АС ГУП Моссоцрегистр, как объекта ИБ, требования к системе защиты персональных данных в АС ГУП Моссоцрегистр).

2. Разработка подсистемы программно-аппаратной защиты информации для КСЗИ ЛВС малого коммерческого предприятия»

3. Проект по совершенствованию системы защищенного электронного документооборота в ЗАО «КЛИО» при использовании «облачных» технологий.

4. Совершенствование методики управления инцидентами в проектных решениях, вырабатываемых в ЗАО «ТехЗИ.

5. Совершенствование методики управления информационными рисками при реализации проектных решений в ЗАО «КЛИО».

6. Разработка проекта системы ЗИ для распределенной вычислительной сети в учреждении здравоохранения.

7. Разработка усовершенствованной подсистемы СКУД типового предприятия (описание объекта, проектирование системы контроля и управления доступом, структурно – функциональная схема усовершенствованной СКУД, технология установки).

8. Проектирование системы ИТЗИ кабинета руководителя среднего госпредприятия.

9. Анализ существующей системы ИТЗИ кабинета руководителя госпредприятия

10. Организационно-технические мероприятия по закрытию выявленных технических каналов утечки информации

11. Оценка эффективности предлагаемой системы инженерно-технической защиты кабинета руководителя госпредприятия.

12. Разработка системы информационной безопасности ЗАО «Электротехнический завод»

13. Разработка автоматизированной системы аудита защиты персональных данных высшего учебного учреждения (на примере

Университета).

14. Разработка облика целесообразной подсистемы аудита защиты персональных данных высшего учебного учреждения.

15. Разработать перечень мероприятий по устранению выявленных недостатков подсистемы компьютерной безопасности.

16. Разработка автоматизированной подсистемы управления защитой персональных данных в ВУЗе.

17. Разработать перечень мероприятий по устранению и ограничению недостатков системы защиты информации предприятия, выработать предложения о возможности внедрения дополнительных мер.

18. Разработка подсистемы компьютерной безопасности для малого коммерческого предприятия.

19. Разработка проекта подсистемы защиты персональных данных в информационной системе высшего учебного заведения (на примере ГОУ ВО МО МГОТУ).

20. Разработка основ методологии выявления и оценки деструктивных воздействий в подсистеме энергоинформационной безопасности типового предприятия.

21. Организация защиты персональных данных на объектах информатизации Министерства финансов Правительства Московской области.

22. Организация защиты конфиденциальной информации в организации и обеспечение безопасности информации в современных условиях

23. Организация работы и основные изделия предприятия ЗАО «ВИНГС-М.

24. Разработка политики информационной безопасности в условиях автоматизации деятельности конструкторского бюро на предприятии «Метровагонмаш».

25. Разработка на базе ОАО «Бубер» коммерческого продукта – системы защиты авторского права для учреждений.

26. Проект по совершенствованию системы программно-аппаратной защиты информации автоматизированного рабочего места сотрудника ЗАО «ТехЗИ».

27. Проектирование системы защиты конфиденциальной информации «НИИ КС им. А. А. Максимова» при использовании «облачных» технологий.

28. Проект по совершенствованию системы физической защиты информационных объектов торгового предприятия В2С («Суши Шоп».

29. Разработка на базе ОАО «Бубер» коммерческого продукта анализа открытых персональных данных в сети Интернет.

30. Разработка методики организации тестового режима работы видеосистем стандарта DVI при проведении контроля защищённости информации от утечки по каналам ПЭМИН.

31. Разработка проекта подсистемы сетевого аудита информационной безопасности основных компонентов ЛВС крупного промышленного

предприятия.

32. Совершенствование подсистемы инженерно-технической защиты информации технических средств связи выделенного помещения типового предприятия.

33. Создание подсистемы физической защиты информации для типового Высшего Учебного Заведения.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по учебной практике

В соответствии с требованиями ФГОС ВО - бакалавриата по направлению подготовки 10.03.01 «Информационная безопасность» разработан фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся, который в полном объеме представлен на выпускающей кафедре, а также на сайте Университета.

Завершающим этапом практики является подведение ее итогов, которое предусматривает выявление степени выполнения студентом программы практики. По результатам аттестации выставляется дифференцированная оценка.

При оценке итогов работы студента на практике, учитываются содержание и правильность оформления студентом дневника, отзыв руководителя практики от организации - места прохождения практики и кафедры, качество ответов на вопросы в ходе защиты.

Критерии дифференцированной оценки по итогам учебной практики:

– **оценка «отлично»** - выставляется студенту, если он своевременно в установленные сроки представил на кафедру оформленные в соответствии с требованиями отзыв от руководителя практики, дневник; имеет отличную характеристику (отзыв) от руководителя предприятия; во время защиты правильно ответил на все вопросы руководителя практики от академии.

– **оценка «хорошо»** - выставляется студенту, если он своевременно в установленные сроки представил на кафедру Информационной безопасности отзыв от руководителя практики с предприятия, дневник; имеет отличную характеристику (отзыв) от руководителя предприятия; но получил незначительные замечания по оформлению отчетных документов по практике или во время защиты ответил не на все вопросы руководителя практики от университета;

– **оценка «удовлетворительно»** - выставляется студенту, если он своевременно в установленные сроки представил на кафедру отзыв, дневник; но получил существенные замечания по оформлению отчетных документов по практике; или во время защиты ответил не на все вопросы руководителя практики от университета;

– **оценка «неудовлетворительно»** - выставляется студенту, отсутствующему на закрепленном рабочем месте практики или не выполнившему программу практики, или получившему отрицательный отзыв о работе, или ответившему неверно на вопросы преподавателя при защите.

7. Формы отчетности по учебной практике

Результаты практики студент обобщает в виде письменного отчета. Отчет по практике является основным документом студента, отражающим, выполненную им работу во время практики, полученные им организационные и технические навыки и знания.

Отчет составляется в соответствии с программой практики и включает материалы, отражающие общие сведения об организации, выполненную работу по изучению организационной структуры управления организацией, задач и функций различных отделов, динамики основных технико-экономических показателей и т.д.

Отчет должен быть оформлен и полностью завершен к моменту окончания практики. Основой отчета являются самостоятельно выполняемые работы студентом в соответствии с программой практики.

В отчете описывается методика проведения исследований, отражаются результаты выполнения индивидуального задания. В заключение отчета приводятся краткие выводы о результатах практики, предлагаются рекомендации по улучшению эффективности деятельности организации.

Изложение в отчете должно быть сжатым, ясным и сопровождаться цифровыми данными, схемами, графиками и диаграммами. Цифровой материал необходимо оформлять в виде таблиц. Сложные отчетные и плановые формы и расчеты могут быть оформлены как приложения к отчету с обязательной ссылкой на них в тексте.

Отчет должен состоять из двух частей.

В первой части необходимо теоретическое рассмотрение по предлагаемой тематике упражнений тем индивидуальных заданий.

Во второй части методика выполнения упражнений.

Материал в отчете представляется в следующей последовательности и объеме:

- титульный лист;
- содержание отчета;
- введение (1-2 стр.);
- глава 1 (7-10стр.);
- глава 2 (5-10стр.);
- заключение (1-2 стр.);
- список используемых источников;
- приложения.

Изложение материалов в отчете должно быть последовательно, лаконично, логически связано. Отчет выполняется на компьютере одной стороне листа А-4. Таблицы и схемы могут быть выполнены на листах иного формата, но должны быть аккуратно сложены по формату А-4.

Отчет может состоять из двух частей: основной и приложений. Объем отчета должен быть не менее 10-15 страниц текста. Вторая часть представляет собой приложения к отчету и может включать схемы, графики, таблицы, документацию организации и т.д.

Основная часть и приложения к отчету нумеруются сплошной нумерацией. Титульный лист не нумеруется.

На последнем листе отчета студент ставит свою подпись и дату окончания работы над отчетом. Титульный лист отчета оформляется по единой форме.

Допускается использование цветных рисунков, схем и диаграмм.

Текст оформляется в соответствии с требованиями делопроизводства, печатается через 1,5 интервала. Сверху страницы делается отступ 20 мм, слева – 25 мм, справа 15 мм, снизу 20 мм. Абзацные отступы должны быть равны 1,25 см.

Нумерация страниц должна быть сквозной. Номер проставляется арабскими цифрами в верхнем правом углу страницы.

Текст должен быть разделен главы. Номер помещается перед названием, после каждой группы цифр ставится точка. В конце заголовка точка не ставится.

Заголовки одного уровня оформляются одинаково по всему тексту. Каждую главу следует начинать с новой страницы. Переносы в заголовках не допускаются.

При компьютерном наборе основной текст следует набирать шрифтом Times New Roman 14 размером.

Все рисунки, таблицы, формулы нумеруются. Нумерация рисунков, таблиц и формул должна быть сквозной по всему тексту, например «Таблица 7». Номер формулы располагается справа от нее в скобках.

Каждый рисунок должен иметь название, состоящее из слова «Рисунок», номера рисунка и через дефис текстовой части. Название таблицы состоит из слова «Таблица», номера таблицы и через дефис текстовой части.

Название рисунка располагается под рисунком по центру. Название таблицы располагается над таблицей справа. Все названия должны располагаться без отрыва от соответствующего объекта.

Если рисунок или таблица продолжается на нескольких страницах, каждая, начиная со второй, часть снабжается названием вида «Таблица 1.2. Продолжение». На последней части вместо слова «Продолжение» рекомендуется записывать «Окончание».

Приложения идентифицируются номерами или буквами, например «Приложение 1» или «Приложение А». На следующей строке, при необходимости, помещается название приложения, которое оформляется как заголовок 1-го уровня без нумерации.

8. Перечень основной и дополнительной литературы, необходимых для прохождения практики

Основная литература:

1. Малюк А.А. и др. Введение в информационную безопасность. Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2011.
2. Белов Е.Б. Основы информационной безопасности. Учебное пособие для вузов.– М.: Горячая линия-Телеком, 2011.
3. Малюк А.А. Теория защиты информации. Научное издание.- М.: Горячая линия-телеком, 2013.- 184 с.
4. Галатенко В.Н. Основы информационной безопасности. Учебное пособие – М.: БИНОМ, 2008.
5. Анисимов А.А. Менеджмент в сфере информационной безопасности: Учеб. пособие. – М.: Интернет-Университет Информационных Технологий, 2012.

Электронные издания:

1. А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др. Технические средства и методы защиты информации. Учебное пособие для вузов.: -4-е издание исправленное и дополненное - –М. Горячая линия – Телеком, 2012.
<http://biblioclub.ru/index.php?page=book&id=253208&sr=1>
2. А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др. Технические средства и методы защиты информации. Учебное пособие для вузов.: -4-е издание исправленное и дополненное - –М. Горячая линия – Телеком, 2012.
<http://biblioclub.ru/index.php?page=book&id=253208&sr=1>
3. Иванов М.А., Чугунов И.В. криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие/ под редакцией М.А. Иванова .М.: НИЯУ МИФИ,2012.
http://biblioclub.ru/index.php?page=book_view&book_id=231673
4. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: учебное пособие для вузов. –М. Горячая линия – Телеком,- 2-е изд., стер. 2012.
http://eknigi.org/nauka_i_ucheba/57446-kriptograficheskie-metody-zashhity-informacii.html
5. Введение в информационно-аналитические системы.
[e-biblio.ru>book/bib/01_informatika/IAS/Book.html](http://e-biblio.ru/book/bib/01_informatika/IAS/Book.html)
6. Ющук Е.Л. Интернет и компьютеры как инструменты конкурентной разведки, электронный ресурс:
http://cirazvedka.ru/Themes/Pages/Internet_and_computers_as_CI_tools.html
7. Титов В.В Конкурентная разведка в современных условиях, электронный ресурс: <http://www.bre.ru/security/22722.html>
8. Баяндин Н. И. Противодействие промышленному шпионажу. Информационно-аналитическая работа, электронный ресурс:
<http://www.mbs-seminar.ru/seminars/seminar.php?seminar=4258>
9. Ющук Е.Л. Презентация «Что такое Конкурентная Разведка и чем она занимается (видео со звуком)», сайт «Сообщества Практиков Конкурентной разведки», электронный ресурс:

<http://www.youtube.com/watch?v=MyQ33slbtFI>

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для прохождения практики (модуля)

1. Электронно-библиотечная система ЭБС Университетская библиотека онлайн <http://www.biblioclub.ru>
2. Электронно-библиотечная система ЭБС ZNANIUM.COM <http://www.znanium.com>
3. Официальный сайт Федеральной таможенной службы <http://customs.ru/>
4. Официальный сайт Евразийской Экономической комиссии <http://eurasiancommission.org/>

10. Методические указания по прохождению практики

Руководство практикой

Основными нормативно-методическими документами, регламентирующими работу студентов на практике, являются программа практики и учебный план.

Утверждение базовых для прохождения практики учреждений и организаций (или конкретных подразделений) осуществляется на основе заявлений студентов и соответствующего приказа, договора с организацией или иных нормативных документов.

Руководство кафедры и деканат факультета обеспечивают выполнение подготовительной и текущей работы по организации и проведению практики, осуществляют контроль ее проведения. Также организуют разработку и согласование программы практики с учреждениями-базами практики; назначают из числа опытных преподавателей кафедры руководителей практики; готовят и проводят совместно с ответственным за практику преподавателем организационные собрания студентов перед началом практики; организуют на кафедре хранение отчетов и дневников студентов по практике.

Отчетные документы и оценка результатов практики

Отчетными документами по практике являются:

1. Дневник по практике, включающий в себя отчет. По окончании практики студент представляет на кафедру дневник по практике, подписанный руководителем практики об организации и от ВУЗа.

Отчет о практике должен содержать сведения о конкретно выполненной студентом работе в период практики.

Отчеты студентов рассматриваются руководителями практики от учебного заведения и организации базы практик.

Дневник практики оформляется на стандартных листах формата А4.

По окончании практики студенты должны сдать документацию не позднее 3-х дней с момента окончания практики, а также защитить отчет (дневник по практике).

Защита практики представляет собой устный публичный отчет студента-практиканта, на который ему отводится 7–8 минут и ответы на вопросы руководителей практики. Устный отчет студента включает: раскрытие целей и задач практики, общую характеристику места практики, описание выполненной работы, выводы и предложения по содержанию и организации практики, совершенствованию программы практики.

К защите практики допускаются студенты, своевременно и в полном объеме выполнившие программу практики и предоставившие в указанные сроки всю отчетную документацию.

2. Отчет руководителя учебной практикой от предприятия / ВУЗа

Руководители практики представляют письменный отчет, в котором описывают содержание работы каждого студента на практике.

Форма дневника по практике и отчета по практике представлены ниже.

Памятка практиканту

До начала практики необходимо выяснить на кафедре место и время прохождения практики, получить дневник практики.

Во время прохождения практики необходимо строго соблюдать правила внутреннего распорядка, установленного в организации; полностью выполнять программу (план) практики; нести ответственность за выполняемую работу и ее результаты наравне со штатными работниками; вести научные исследования в интересах организации; вести дневник практики и по окончании практики предоставить его на подпись руководителям от ВУЗа / организации.

Дневник с отчетом предоставляются руководителям практики для оценки.

Потеря дневника равноценна невыполнению программы практики и получению неудовлетворительной оценки. Дневники хранятся на кафедре весь период обучения студента.

Права и обязанности студентов во время прохождения практики

Студент во время прохождения практики обязан:

1. Посещать все консультации и методические совещания, посвященные организации практики.

2. Знать и соблюдать правила охраны труда, выполнять действующие в организации правила внутреннего трудового распорядка.

3. В случае пропуска, опоздания сообщить руководителю заранее, объяснить причину отсутствия или опоздания, предоставить необходимые документы (справка о болезни, повестка и др.).

4. Выполнять задания, предусмотренные программой практики, требования руководителей практики.

5. Оформлять в ходе практики дневник по практике и предоставлять его непосредственным руководителям практики для проверки.

6. По завершении практики в точно указанные сроки подготовить отчет о результатах проделанной работы и защитить его с положительной оценкой.

Студент во время прохождения практики имеет право:

1. Обращаться к руководителям ВУЗа, руководству факультета и выпускающей кафедры по всем вопросам, возникающим в процессе практики.

2. Вносить предложения по совершенствованию процесса организации практики.

3. Пользоваться фондами библиотеки, кабинетами с выделенными линиями Интернета.

Памятка руководителю практики

Руководитель практики обязан: осуществлять непосредственное руководство практикой студентов на предприятии, в учреждении, организации; обеспечивать высокое качество прохождения практики студентами и строгое соответствие ее учебным планам и программам; участвовать в организованных мероприятиях перед выходом студентов на практику (установочные конференции, инструктаж по технике безопасности и охране труда и т.д.); распределять студентов по местам прохождения практики; осуществлять контроль за соблюдением нормальных условий труда и быта студентов, находящихся на практике, контролировать выполнение практикантами правил внутреннего трудового распорядка; собирать и анализировать документацию, подготовленную студентами по итогам практики, составлять отчет по итогам практики и предоставлять его на кафедру; принимать участие в мероприятиях по защите отчета (дневника по практике), оценивать работу студентов-практикантов и оформлять ведомость и зачетные книжки.

Руководитель составляет отчет о результатах прохождения учебной практики студентами, обучающимися по направлению подготовки 10.03.01 «Информационная безопасность».

Отчет включает в себя: сроки практики, цели, тематику работы, указание организации, в которой проходила практика, список студентов-практикантов с описанием выполняемой ими работы и оценкой за защиту результатов практики.

12. Перечень информационных технологий, используемых при проведении практики

Перечень программного обеспечения: Microsoft Office Power Point, Microsoft Office Word, Microsoft Office Excel.

Информационные справочные системы:

Электронные ресурсы образовательной среды Университета:

- www.biblioclub.ru
- www.rucont.ru
- znanium.com
- e.lanbook.com

Информационно-справочные системы:

- Консультант+
- Гарант

13. Описание материально-технической базы, необходимой для проведения практики

Материально-техническое обеспечение учебной практики включает в себя: мультимедийную аудиторию для защиты отчетов, подготовленных с использованием MicrosoftOfficePowerPoint, MicrosoftOfficeWord, MicrosoftOfficeExcel для выполнения и оформления отчетов студентов по учебной практике, а также доступный для студента выход в Интернет с целью поиска современной информации по информационной безопасности (защите информации).



Государственное бюджетное образовательное учреждение высшего образования
Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Б2.В.03 (II) Проектно-технологическая практика

Б2.В.04 (II) Преддипломная

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: «Безопасность телекоммуникационных систем (в аэрокосмической сфере)»

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Год набора: 2020

Королев
2020

1. Перечень планируемых результатов производственной практики

Производственная практика - является важнейшей составной частью учебного процесса по подготовке специалистов в соответствии с основной профессиональной образовательной программой высшего образования (далее – ОПОП ВО), реализуемой Государственным бюджетным образовательным учреждением высшего образования Московской области «Технологический университет» (далее – Университет) по направлению подготовки 10.03.01 «Информационная безопасность» и обеспечивают системно-деятельностный подход в подготовке бакалавров в области организации и технологии защиты информации, нарушениям в области информационной безопасности.

Производственная практика подразделяется на следующие типы:

- проектно-технологическая практика;
- преддипломная практика.

Целями производственной практики являются:

- систематизация, закрепление и углубление теоретических знаний, полученных в процессе обучения в Университете;
- приобретение необходимых практических умений и навыков работы в соответствии с выбранным направлением профессиональной подготовки;
- развитие и накопление специальных практических навыков для решения профессиональных задач;
- развитие профессионального мышления;
- приобретение первоначальных профессиональных умений в области организации и технологии защиты информации.

Задачи производственной практики:

- ознакомление с управленческой структурой предприятия или организации, функциональными обязанностями работников отдела, занимающихся внешнеэкономической деятельностью;
- ознакомление с управленческой структурой таможенного органа, функциональными обязанностями сотрудников таможенной службы;
- сбор, обобщение и анализ материалов в соответствии с программой практики и индивидуальным заданием, определяемых конкретным местом прохождения практики;
- овладение первичными навыками на конкретном рабочем месте.

Производственная практика проводится на базе кафедры информационной безопасности и ее лабораторий: на базе ЗАО «Клио», «НИИ КС им. А. А. Максимова» - филиала ФГУП «ГКНПЦ им М. В. Хруничева», 18 ЦНИИ МО, кафедры «Информационной безопасности», лабораторий кафедры «Информационной безопасности»: Аудитория 2210: Лаборатория управления информационной безопасности; Аудитория 2210а: Лаборатория защищенных технических средств и систем; Аудитория 2206: Лаборатория технологий обеспечения информационной безопасности.

По форме проведения производственная практика является камеральной, не требует командирования студентов и проводится в профильных учреждениях, расположенных в г. Москве и Московской области. Для прохождения практики, как правило, формируются группы студентов. Среди организаций, которые будут изучаться студентами могут быть следующие:

НИИ КС; 18 ЦНИИ МО; ООО «ТехЗИ»; ЗАО «КЛИО»; ООО НОВО», НТЦ «ЗАРЯ», подразделения предприятий различных сфер деятельности (службы (отделы) информационной безопасности, защиты информации, подразделения занимающиеся информационной безопасностью кредитно-финансовых организаций; отделения ГОСТЕХНАДЗОРА; иные организации, связанные в будущем с профессиональной деятельностью выпускников направления подготовки 10.03.01 «Информационная безопасность» могут также выступать в качестве объекта исследования, но только при согласовании с руководителем практики от кафедры Информационная безопасность.

Перечень планируемых результатов обучения при прохождении практики

В процессе прохождения производственной практики студент приобретает и совершенствует следующие компетенции:

Б2.В.03 (II) Проектно-технологическая практика

ОК-1: способностью использовать основы философских знаний для формирования мировоззренческой позиции;

ОК-6: способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия;

ОК-8: способность к самоорганизации и самообразованию;

ОПК-2: способностью применять соответствующий математический аппарат для решения профессиональных задач;

ОПК-3: способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач;

ОПК-4: способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-5: способностью использовать нормативные правовые акты в профессиональной деятельности;

ОПК-6: способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности;

ОПК-7: способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их

реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

ПК-2: способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

ПК-5: способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;

ПК-6: способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

ПК-7: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;

ПК-8: способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

ПК-9: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

ПК-10: способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;

ПК-11: способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;

ПК-12: способность принимать участие в проведении экспериментальных исследований системы защиты информации;

ПК-13: способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;

ПК-14: способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности;

ПК-15: способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ПСК-1: способность проводить совместный анализ функционального процесса защиты ТКС и ее информационных составляющих с целью определения возможных источников угроз, их вероятных целей;

ПСК-2: способность формировать предложения по оптимизации функционального процесса и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов;

ПСК-3: способность организовывать контроль и анализ защищенности объектов ТКС в соответствии с нормативными документами;

ПСК-4: способность организовать реализацию принятых мер по управлению защитой информационных потоков на пакетном уровне с комплексной оценкой информационной безопасности ТКС.

Б2.В.04 (II) Преддипломная практика

ОК-1: способностью использовать основы философских знаний для формирования мировоззренческой позиции;

ОК-2: способностью использовать основы экономических знаний в различных сферах деятельности;

ОК-3: способностью анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма;

ОК-4: способностью использовать основы правовых знаний в различных сферах деятельности;

ОК-5: способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;

ОК-6: способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия;

ОК-7: способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности;

ОК-8: способность к самоорганизации и самообразованию;

ОК-9: способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности;

ОПК-1: способностью анализировать физические явления и процессы для решения профессиональных задач;

ОПК-2: способностью применять соответствующий математический аппарат для решения профессиональных задач;

ОПК-3: способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач;

ОПК-4: способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-5: способностью использовать нормативные правовые акты в профессиональной деятельности;

ОПК-6: способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности;

ОПК-7: способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

ПК-2: способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

ПК-3: способность администрировать подсистемы информационной безопасности объекта защиты;

ПК-4: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

ПК-5: способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;

ПК-6: способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

ПК-7: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;

ПК-8: способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

ПК-9: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

ПК-10: способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;

ПК-11: способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;

ПК-12: способность принимать участие в проведении экспериментальных исследований системы защиты информации;

ПК-13: способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;

ПК-14: способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности;

ПК-15: способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ПСК-1: способность проводить совместный анализ функционального процесса защиты ТКС и ее информационных составляющих с целью определения возможных источников угроз, их вероятных целей;

ПСК-2: способность формировать предложения по оптимизации функционального процесса и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов;

ПСК-3: способность организовывать контроль и анализ защищенности объектов ТКС в соответствии с нормативными документами;

ПСК-4: способность организовать реализацию принятых мер по управлению защитой информационных потоков на пакетном уровне с комплексной оценкой информационной безопасности ТКС.

Итогом проведения производственной практики является овладение студентами навыков использования контрольно-проверочной аппаратуры, программных продуктов, применяемых на предприятиях (организациях), заполнения документации подразделений организации.

2. Место производственной практики в структуре ОПОП ВО

Производственная практика относится к обязательному разделу ОПОП ВО по направлению подготовки 10.03.01. «Информационная безопасность» и базируется на ранее изученных дисциплинах:

Блок 1. Дисциплины (модули)

Базовая часть

Б1.Б.01 Философия

Б1.Б.02 История

Б1.Б.03 Иностранный язык

Б1.Б.04 Безопасность жизнедеятельности

Б1.Б.05 Русский язык и культура речи

Б1.Б.06 Основы управленческой деятельности

Б1.Б.07 Документоведение

Б1.Б.08 Экономика предприятия и организация производства

Б1.Б.09 Группа учебных дисциплин (модулей) "Математические основы обеспечения информационной безопасности":

Б1.Б.09.01 Линейная алгебра и аналитическая геометрия

Б1.Б.09.02 Математический анализ

Б1.Б.09.03 Теория графов

Б1.Б.09.04 Теория информации

Б1.Б.09.05 Теория вероятностей и математическая статистика

Б1.Б.09.06 Дискретная математика

Б1.Б.10 Группа учебных дисциплин (модулей) "Физико-технические основы обеспечения информационной безопасности":

Б1.Б.10.01 Физика

Б1.Б.10.02 Электротехника

Б1.Б.10.03 Электроника и схемотехника

Б1.Б.11 Группа учебных дисциплин (модулей) "Информационные технологии":

Б1.Б.11.01 Информатика

Б1.Б.11.02 Языки программирования

Б1.Б.11.03 Технологии и методы программирования

Б1.Б.11.04 Аппаратные средства вычислительной техники

Б1.Б.11.05 Сети и системы передачи информации

Б1.Б.11.06 Информационные технологии

Б1.Б.12 Группа учебных дисциплин (модулей) "Методы и средства обеспечения информационной безопасности":

Б1.Б.12.01 Основы информационной безопасности

Б1.Б.12.02 Организационное и правовое обеспечение информационной безопасности

Б1.Б.12.03 Основы управления информационной безопасностью

Б1.Б.12.04 Техническая защита информации

Б1.Б.12.05 Криптографические методы защиты информации

Б1.Б.12.06 Программно-аппаратные средства защиты информации

Б1.Б.12.07 Комплексное обеспечение защиты информации объекта информатизации (предприятия)

Б1.Б.13 Дисциплины (модули) профиля: "Информационная безопасность телекоммуникационных систем (по отрасли или в сфере профессиональной деятельности)":

Б1.Б.13.01 Устройства формирования и передачи сигналов в ТКС

Б1.Б.13.02 Устройства приема и обработки сигналов в ТКС

Б1.Б.13.03 Сетевые технологии

Б1.Б.13.04 Защита информации в ТКС

Б1.Б.13.05 Системы аэрокосмической и наземной подвижной связи

Б1.Б.13.06 Беспроводные системы связи и их безопасность

Б1.Б.13.07 Проектирование элементов защищенных ТКС

Б1.Б.13.08 Математическое моделирование защищенных систем ТКС

Б1.Б.13.09 Физические основы волоконно-оптических линий связи (ВОЛС)
Б1.Б.14 Физическая культура

Вариативная часть

Б1.В.01 Дисциплины (модули) образовательной организации:

Б1.В.01.01 Основы исследований информационной безопасности

Б1.В.01.02 Основы социального государства и гражданского общества

Б1.В.01.03 Пакеты прикладных программ

Б1.В.01.04 Социально-психологические основы управленческой деятельности

Б1.В.01.05 Основы проектной деятельности

Б1.В.01.06 История защиты информации в РФ

Б1.В.01.07 Информационная безопасность автоматизированных систем

Б1.В.02 Основы права

Б1.В.03 Гуманитарные аспекты (профессиональная этика) информационной безопасности

Б1.В.04 Безопасность информационных технологий

Б1.В.05 Элективные курсы по физической культуре и спорту

Б1.В.ДВ.01 Дисциплины по выбору Блок 1.В.ДВ.1

Б.В.ДВ.01.01 Операционные системы, среды и оболочки

Б.В.ДВ.01.02 Базы данных, системы управления базами данных

Б1.В.ДВ.02 Дисциплины по выбору Блок 1.В.ДВ.2

Б1.В.ДВ.02.01 Основы алгоритмизации и программирования

Б1.В.ДВ.02.02 Пакеты прикладных математических программ

Б1.В.ДВ.03 Дисциплины по выбору Блок 1.В.ДВ.3

Б1.В.ДВ.03.01 Информационная безопасность кредитно-финансовых операций

Б1.В.ДВ.03.02 Защищенные электронные технологии банка

Б1.В.ДВ.03.03 Технические каналы утечки конфиденциальной информации (ОАО «НОВО»)

Б1.В.ДВ.04 Дисциплины по выбору Блок 1.В.ДВ.4

Б1.В.ДВ.04.01 Информационно-психологическая безопасность персонала предприятия

Б1.В.ДВ.04.02 Защита общества от информации, запрещенной к распространению

Б1.В.ДВ.04.03 Организация защиты конфиденциальной информации от несанкционированного доступа (ОАО «НОВО»)

Б1.В.ДВ.05 Дисциплины по выбору Блок 1.В.ДВ.5

Б1.В.ДВ.05.01 Разработка политики информационной безопасности в организациях

Б1.В.ДВ.05.02 Разработка политики информационной безопасности в Интернет - системах

Б1.В.ДВ.05.03 Оценка защищённости конфиденциальной информации по техническим каналам и от несанкционированного доступа (ОАО «НОВО»)

Б1.В.ДВ.06 Дисциплины по выбору Блок 1.В.ДВ.6

Б1.В.ДВ.06.01 Организация защиты персональных данных на предприятии
Б1.В.ДВ.06.02 Правовая охрана результатов интеллектуальной деятельности
Б1.В.ДВ.06.03 Методы и средства защиты информации от утечки по техническим каналам (ОАО «НОВО»)

Б1.В.ДВ.07 Дисциплины по выбору Блок 1.В.ДВ.7

Б1.В.ДВ.07.01 Защита профессиональной тайны в различных сферах деятельности

Б1.В.ДВ.07.02 Информационная безопасность операционных систем и баз данных

Б1.В.ДВ.07.03 Подготовка объекта информатизации к аттестации по требованиям безопасности информации (ОАО «НОВО»)

Б1.В.ДВ.08 Дисциплины по выбору Блок 1.В.ДВ.8

Б1.В.ДВ.08.01 Лицензирование и сертификация в области защиты информации

Б1.В.ДВ.08.02 Аттестация в области защиты информации

Б1.В.ДВ.08.03 Разработка объекта информатизации в защищённом исполнении (ОАО «НОВО»)

Б1.В.ДВ.09 Дисциплины по выбору Блок 1.В.ДВ.9

Б1.В.ДВ.09.01 Радиоэлектронные системы и средства как объекты информационной безопасности

Б1.В.ДВ.09.02 Основы радиоэлектронной разведки (РЭР)

Б1.В.ДВ.09.03 Методы и средства защиты информации от несанкционированного доступа (ОАО «НОВО»)

Б1.В.ДВ.10 Дисциплины по выбору Блок 1.В.ДВ.10

Б1.В.ДВ.10.01 Социотехносферная безопасность объектов информационной защиты

Б1.В.ДВ.10.02 Эффективность защищённых информационных систем

Б1.В.ДВ.10.03 Методы и средства выявления демаскирующих признаков закладочных устройств в защищаемых помещениях (ОАО «НОВО»)

Б1.В.ДВ.11 Дисциплины по выбору Блок 1.В.ДВ.11

Б1.В.ДВ.11.01 Введение в профессию

Б1.В.ДВ.11.02 Профессиональные адаптации инвалидов и лиц с ОВЗ

Б1.В.ДВ.12 Дисциплины по выбору Блок 1.В.ДВ.12

Б1.В.ДВ.13 Дисциплины по выбору Блок 1.В.ДВ.13

Блок 2. Практики

Вариативная часть

Б2.В.01(У) Практика по получению первичных профессиональных умений и навыков

Б2.В.02(У) Технологическая практика

Б2.В.03(У) Проектно-технологическая практика

Б2.В.04(У) Преддипломная практика

Блок 3. Государственная итоговая аттестация

Базовая часть

ФТД Факультативы

Вариативная часть

ФТД.В. 01 Техничко-экономическое обоснование проекта;

ФТД В 02. Разработка и реализация проекта

Знания и компетенции, полученные при освоении учебной и производственной практик, являются базовыми при изучении ряда последующих изучаемых дисциплин и выполнении выпускной квалификационной работы бакалавра.

3. Объем практики в зачетных единицах и ее продолжительность

Общая трудоёмкость производственной практики составляет 432 часов, 12 зачетных единиц. Проводится производственная практика (проектно-технологическая практика) после третьего курса продолжительностью 2 недели, (шестой семестр) и после четвертого курса производственная практика (преддипломная практика) (восьмой семестр), продолжительностью 6 недель для очной формы обучения.

Общая трудоёмкость производственной практики составляет 432 часа, 12 зачетных единиц.

Трудоёмкость производственной проектно-технологической практики составляет 108 часов, 3 зачетные единицы. Проводится после третьего курса в 6 семестре, продолжительностью 2 недели для очной формы обучения.

Трудоёмкость производственной преддипломной практики составляет 324 часа, 9 зачетных единиц. Проводится в 8 семестре для очной формы обучения продолжительностью 6 недель.

4. Содержание производственной практики

В процессе прохождения практики активно используется обучение на основе опыта, применяется исследовательский метод, в рамках которого предполагается самостоятельный поиск материала, по заданиям, которые указаны в программе практики.

В процессе прохождения производственной практики студент может обращаться за консультациями и помощью в решении отдельных вопросов, связанных с прохождением производственной практики к преподавателю кафедры Информационной безопасности, назначенному руководителем производственной практиками студентов, осуществляющему текущее руководство практикой.

Сроки сдачи и защиты отчетов по производственной практике устанавливает руководитель производственной практикой студентов. Содержание производственной практики определяется выпускающей кафедрой Информационной безопасности в соответствии с учебным планом и программой, с учетом специфики деятельности организации, которую изучают студенты в рамках производственной практик.

Основные виды работ на практике, включая самостоятельную работу студентов, представлены в Таблице 1,2. Во время производственной практики студенты также выполняют индивидуальное задание, в соответствии со списком предлагаемых направлений. В отчете данная часть отражается в виде описания личных функциональных обязанностей, реализуемых студентом или практических результатов, достигнутых в ходе прохождения практики.

Программой производственной практики при разработке индивидуальных заданий предусматривается соблюдение следующих требований:

- учет уровня теоретической подготовки студента по дисциплинам гуманитарного, социально-экономического цикла, математического и естественнонаучного цикла и профессионального цикла к моменту проведения практики;
- доступность и практическая возможность сбора исходной информации, как в организации, так и с использованием иных источников информации, в том числе сети интернет.

По результатам прохождения практики студентами составляется отчет по производственной практике. Содержание данного отчета определяется спецификой выбранной темы ВКР; объем – не более 10 страниц в отдельном разделе общего отчета. Отчет по индивидуальному занятию визируется руководителем работы. Качество выполнения программы практики учитывается при вынесении общей оценки практики.

Наиболее интересные результаты работ докладываются на конференциях студентов, молодых ученых и аспирантов, организуемых МГОТУ, ИТФ или кафедрой Информационной безопасности. Материалы из лучших отчетов могут быть рекомендованы для представления на открытый конкурс научных работ среди студентов вузов России.

Таблица 1

| № п/п | Виды работ на производственной практике, включая самостоятельную работу студентов | Трудоемкость (в часах) |
|-------|---|------------------------|
| 1 | 2 | 3 |
| 1 | Ознакомление с деятельностью организации. Написание раздела отчета. | 1 |
| 2 | Ознакомление с миссией, целями, задачами, сферой деятельности, историей развития организации, видами деятельности. Написание раздела отчета. | 1 |
| 3 | Характеристика предприятия: полное название; форма собственности; месторасположение, правовой статус, учредительные документы предприятия, документация по лицензированию. Написание раздела отчета. | 1 |
| 4 | Описание организационной структуры предприятия: схема, | 1 |

| | | |
|----|---|------------|
| | количество отделов и их название, их функции, подчиненность, взаимодействие. Написание раздела отчета. | |
| 5 | Управление кадрами. Информация о кадровом составе организации: должности, численность персонала, структура персонала. Описание основных подразделений по кадрам, взаимосвязь их с другими отделами. Написание раздела отчета. | 1 |
| 6 | Ознакомление с ЕКС руководителей, специалистов и служащих и ЕТКС работ и профессий рабочих. Сравнение должностных и рабочих обязанностей в должностных инструкциях и в данных справочниках (необходимо рассмотреть 3 должностные инструкции). Написание раздела отчета. | 1 |
| 7 | Изучение функционально-должностных инструкций специалистов низшего звена на предприятии. Написание раздела отчета. | 1 |
| 8 | Анализ методов контроля, используемых в организации. Написание раздела отчета. | 1 |
| 9 | Анализ и характеристика деятельности организации/отдела. Написание раздела отчета. | 1 |
| 10 | Анализ и описание сильных и слабых сторон организации; выводы и предложения по итогам практики. Написание раздела отчета. | 1 |
| 11 | Выполнение индивидуального задания. Написание раздела отчета. | 97 |
| 12 | Согласование отчета по практике с руководителем практики от кафедры. Завершение и оформление отчета по учебной практике. | 1 |
| | Итого: в часах (у/п) | 108 |

Таблица 2

| № п/п | Виды работ (график) на производственной практике, включая самостоятельную работу студентов в аудиториях Университета | Трудоемкость (в часах) |
|--------------|--|-------------------------------|
| 1 | 2 | 3 |
| 1 | Прохождение вводного инструктажа по организации и проведению практики, выдача индивидуальных заданий. | 1 |
| 2 | Прохождение первичного инструктажа по охране труда на рабочем месте ознакомление с современными средствами вычислительной техники, коммуникаций и связи, используемых в процессе обучения. | 1 |
| 3 | Краткая характеристика используемых методов по защите | 2 |

| | | |
|---|---|------------|
| | информации и программных продуктов, используемых при отработке практических заданий | |
| 4 | Выполнение практических заданий по тематике индивидуальных заданий производственной практики в рамках индивидуального задания | 314 |
| 5 | Подготовка и оформление отчета по производственной практике | 4 |
| 6 | Представление отчета по производственной практике руководителю и защита результатов работы студентами | 2 |
| | Итого: в часах (у/п) | 324 |

Методические рекомендации для самостоятельной работы по индивидуальным заданиям

Производственная практика студентов проводится в форме самостоятельной практической работы под руководством преподавателя. Производственная практика студентов строится с учетом специфики объекта практики (информационного объекта), в соответствии с тематическим планом, примерное содержание которого соответствует списку тем индивидуальных заданий:

1. Разработка системы защиты персональных данных в АС ГУП Моссоцрегистр. (общая характеристика ГУП Моссоцрегистр, как объекта ИБ, состав и структура АС ГУП Моссоцрегистр, как объекта ИБ, требования к системе защиты персональных данных в АС ГУП Моссоцрегистр).

2. Разработка подсистемы программно-аппаратной защиты информации для КСЗИ ЛВС малого коммерческого предприятия»

3. Проект по совершенствованию системы защищенного электронного документооборота в ЗАО «КЛИО» при использовании «облачных» технологий.

4. Совершенствование методики управления инцидентами в проектных решениях, вырабатываемых в ЗАО «ТехЗИ.

5. Совершенствование методики управления информационными рисками при реализации проектных решений в ЗАО «КЛИО».

6. Тема дипломного проекта «Разработка проекта системы ЗИ для распределенной вычислительной сети в учреждении здравоохранения»

7. Разработка усовершенствованной подсистемы СКУД типового предприятия (описание объекта, проектирование системы контроля и управления доступом, структурно –функциональная схема усовершенствованной СКУД, технология установки).

8. Проектирование системы ИТЗИ кабинета руководителя среднего госпредприятия.

9. Анализ существующей системы ИТЗИ кабинета руководителя госпредприятия

10. Организационно-технические мероприятия по закрытию выявленных технических каналов утечки информации

11. Оценка эффективности предлагаемой системы инженерно-

технической защиты кабинета руководителя госпредприятия.

12. Разработка системы информационной безопасности ЗАО «Электротехнический завод»

13. Разработка автоматизированной системы аудита защиты персональных данных высшего учебного учреждения (на примере Университета).

14. Разработка облика целесообразной подсистемы аудита защиты персональных данных высшего учебного учреждения.

15. Разработать перечень мероприятий по устранению выявленных недостатков подсистемы компьютерной безопасности.

16. Разработка автоматизированной подсистемы управления защитой персональных данных в ВУЗе.

17. Разработать перечень мероприятий по устранению и ограничению недостатков системы защиты информации предприятия, выработать предложения о возможности внедрения дополнительных мер.

18. Разработка подсистемы компьютерной безопасности для малого коммерческого предприятия.

19. Разработка проекта подсистемы защиты персональных данных в информационной системе высшего учебного заведения (на примере ГОУ ВПО МО Технологический Университет).

20. Разработка основ методологии выявления и оценки деструктивных воздействий в подсистеме энергоинформационной безопасности типового предприятия.

21. Организация защиты персональных данных на объектах информатизации Министерства финансов Правительства Московской области.

22. Организация защиты конфиденциальной информации в организации и обеспечение безопасности информации в современных условиях

23. Организация работы и основные изделия предприятия ЗАО «ВИНГС-М.

24. Разработка политики информационной безопасности в условиях автоматизации деятельности конструкторского бюро на предприятии «Метровагонмаш».

25. Разработка на базе ОАО «Бубер» коммерческого продукта – системы защиты авторского права для учреждений.

26. Проект по совершенствованию системы программно-аппаратной защиты информации автоматизированного рабочего места сотрудника ЗАО «ТехЗИ».

27. Проектирование системы защиты конфиденциальной информации «НИИ КС им. А. А. Максимова» при использовании «облачных» технологий.

28. Проект по совершенствованию системы физической защиты информационных объектов торгового предприятия В2С («Суши Шоп».

29. Разработка на базе ОАО «Бубер» коммерческого продукта анализа открытых персональных данных в сети Интернет.

30. Разработка методики организации тестового режима работы видеосистем стандарта DVI при проведении контроля защищённости информации от утечки по каналам ПЭМИН.

31. Разработка проекта подсистемы сетевого аудита информационной безопасности основных компонентов ЛВС крупного промышленного предприятия.

32. Совершенствование подсистемы инженерно-технической защиты информации технических средств связи выделенного помещения типового предприятия.

33. Создание подсистемы физической защиты информации для типового Высшего Учебного Заведения.

5. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по производственной практике

В соответствии с требованиями ФГОС ВО - бакалавриата по направлению подготовки 10.03.01 «Информационная безопасность» разработан фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся, который в полном объеме представлен на выпускающей кафедре, а также на сайте Университета.

Завершающим этапом практики является подведение ее итогов, которое предусматривает выявление степени выполнения студентом программы практики. По результатам аттестации выставляется дифференцированная оценка.

При оценке итогов работы студента на практике, учитываются содержание и правильность оформления студентом дневника, отзыв руководителя практики от организации - места прохождения практики и кафедры, качество ответов на вопросы в ходе защиты.

Критерии дифференцированной оценки по итогам производственной практики:

– оценка «отлично» - выставляется студенту, если он своевременно в установленные сроки представил на кафедру оформленные в соответствии с требованиями отзыв от руководителя практики, дневник; имеет отличную характеристику (отзыв) от руководителя предприятия; во время защиты правильно ответил на все вопросы руководителя практики от академии.

– оценка «хорошо» - выставляется студенту, если он своевременно в установленные сроки представил на кафедру ГСД отзыв от руководителя практики с предприятия, дневник; имеет отличную характеристику (отзыв) от руководителя предприятия; но получил незначительные замечания по оформлению отчетных документов по практике или во время защиты ответил не на все вопросы руководителя практики от университета;

– оценка «удовлетворительно» - выставляется студенту, если он своевременно в установленные сроки представил на кафедру отзыв, дневник; но получил существенные замечания по оформлению отчетных документов по практике; или во время защиты ответил не на все вопросы руководителя практики от университета;

– оценка «неудовлетворительно» - выставляется студенту, отсутствующему на закрепленном рабочем месте практики или не выполнившему программу практики, или получившему отрицательный отзыв о работе, или ответившему неверно на вопросы преподавателя при защите.

6. Формы отчетности по производственной практике

Результаты практики студент обобщает в виде письменного отчета. Отчет по практике является основным документом студента, отражающим, выполненную им работу во время практики, полученные им организационные и технические навыки и знания.

Отчет составляется в соответствии с программой практики и включает материалы, отражающие общие сведения об организации, выполненную работу по изучению организационной структуры управления организацией, задач и функций различных отделов, динамики основных технико-экономических показателей и т.д.

Отчет должен быть оформлен и полностью завершен к моменту окончания практики. Основой отчета являются самостоятельно выполняемые работы студентом в соответствии с программой практики.

В отчете описывается методика проведения исследований, отражаются результаты выполнения индивидуального задания. В заключение отчета приводятся краткие выводы о результатах практики, предлагаются рекомендации по улучшению эффективности деятельности организации.

Изложение в отчете должно быть сжатым, ясным и сопровождаться цифровыми данными, схемами, графиками и диаграммами. Цифровой материал необходимо оформлять в виде таблиц. Сложные отчетные и плановые формы и расчеты могут быть оформлены как приложения к отчету с обязательной ссылкой на них в тексте.

Отчет должен состоять из двух глав.

В первой главе должно быть отражено:

- миссия, цели, задачи, сфера деятельности, история развития организации, виды деятельности;
- характеристика организации (полное название; форма собственности; месторасположение, правовой статус, учредительные документы (устав), документация по лицензированию);
- описание организационной структуры предприятия: схема, количество отделов и их название, их функции, подчиненность, взаимодействие;
- вопросы управления кадрами (информация о кадровом составе организации: должности, численность персонала, структура персонала; описание основных подразделений по кадрам, взаимосвязь их с другими отделами);
- исследование ЕКС руководителей, специалистов и служащих и ЕТКС работ и профессий рабочих и сравнение должностных и рабочих

обязанностей в должностных инструкциях и в данных справочниках (не менее 3-х должностных инструкций);

- функционально-должностные инструкции менеджеров низшего звена в организации;

- анализ методов контроля, используемых в организации;

- анализ и характеристика деятельности организации/отдела, связанной с внешней торговлей, либо контроля за перемещением товаров и транспортных средств через таможенную границу Таможенного союза;

- анализ и описание сильных и слабых сторон организации.

Во второй главе необходимо теоретическое рассмотрение по одной из тем индивидуальных заданий с практическими рекомендациями для их применения.

Материал в отчете представляется в следующей последовательности и объеме:

титульный лист;

содержание отчета;

введение (1-2 стр.)

глава 1 (7-10стр.);

глава 2 (5-10стр.);

заключение (1-2 стр.);

список используемых источников;

приложения.

Изложение материалов в отчете должно быть последовательно, лаконично, логически связано. Отчет выполняется на компьютере одной стороне листа А-4. Таблицы и схемы могут быть выполнены на листах иного формата, но должны быть аккуратно сложены по формату А-4.

Отчет может состоять из двух частей: основной и приложений. Объем отчета должен быть не менее 20 страниц текста. Вторая часть представляет собой приложения к отчету и может включать схемы, графики, таблицы, документацию организации и т.д.

Основная часть и приложения к отчету нумеруются сплошной нумерацией. Титульный лист не нумеруется.

На последнем листе отчета студент ставит свою подпись и дату окончания работы над отчетом. Титульный лист отчета оформляется по единой форме.

Допускается использование цветных рисунков, схем и диаграмм.

Текст оформляется в соответствии с требованиями делопроизводства, печатается через 1,5 интервала. Сверху страницы делается отступ 20 мм, слева – 25 мм, справа 15 мм, снизу 20 мм. Абзацные отступы должны быть равны 1,25 см.

Нумерация страниц должна быть сквозной. Номер проставляется арабскими цифрами в верхнем правом углу страницы.

Текст должен быть разделен главы. Номер помещается перед названием, после каждой группы цифр ставится точка. В конце заголовка точка не ставится.

Заголовки одного уровня оформляются одинаково по всему тексту. Каждую главу следует начинать с новой страницы. Переносы в заголовках не допускаются.

При компьютерном наборе основной текст следует набирать шрифтом Times New Roman 14 размером.

Все рисунки, таблицы, формулы нумеруются. Нумерация рисунков, таблиц и формул должна быть сквозной по всему тексту, например «Таблица 7». Номер формулы располагается справа от нее в скобках.

Каждый рисунок должен иметь название, состоящее из слова «Рисунок», номера рисунка и через дефис текстовой части. Название таблицы состоит из слова «Таблица», номера таблицы и через дефис текстовой части.

Название рисунка располагается под рисунком по центру. Название таблицы располагается над таблицей справа. Все названия должны располагаться без отрыва от соответствующего объекта.

Если рисунок или таблица продолжается на нескольких страницах, каждая, начиная со второй, часть снабжается названием вида «Таблица 1.2. Продолжение». На последней части вместо слова «Продолжение» рекомендуется записывать «Окончание».

Приложения идентифицируются номерами или буквами, например «Приложение 1» или «Приложение А». На следующей строке, при необходимости, помещается название приложения, которое оформляется как заголовок 1-го уровня без нумерации.

7. Перечень учебной литературы и ресурсов «Интернет», необходимых для проведения практики

Основная литература:

1. Малюк А.А. и др. Введение в информационную безопасность. Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2011.
2. Белов Е.Б. Основы информационной безопасности. Учебное пособие для вузов.– М.: Горячая линия-Телеком, 2011.
3. Малюк А.А. Теория защиты информации. Научное издание.- М.: Горячая линия-телеком, 2013.- 184 с.
4. Галатенко В.Н. Основы информационной безопасности. Учебное пособие – М.: БИНОМ, 2008.
5. Анисимов А.А. Менеджмент в сфере информационной безопасности: Учеб. пособие. – М.: Интернет-Университет Информационных Технологий, 2012.

Электронные издания:

1. А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др. Технические средства и методы защиты информации. Учебное пособие для вузов: -4-е издание исправленное и дополненное - –М. Горячая линия – Телеком, 2012.

<http://biblioclub.ru/index.php?page=book&id=253208&sr=1>

2. А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др. Технические средства и методы защиты информации. Учебное пособие для вузов.: -4-е издание исправленное и дополненное - –М. Горячая линия – Телеком, 2012.

<http://biblioclub.ru/index.php?page=book&id=253208&sr=1>

3. Иванов М.А., Чугунов И.В. криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие/ под редакцией М.А. Иванова .М.: НИЯУ МИФИ,2012.

http://biblioclub.ru/index.php?page=book_view&book_id=231673

4. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: учебное пособие для вузов. –М. Горячая линия – Телеком,- 2-е изд., стер. 2012.

http://eknigi.org/nauka_i_ucheba/57446-kriptograficheskie-metody-zashhity-informacii.html

5. Введение в информационно-аналитические системы.

[e-biblio.ru>book/bib/01_informatika/IAS/Book.html](http://e-biblio.ru/book/bib/01_informatika/IAS/Book.html)

6. Ющук Е.Л. Интернет и компьютеры как инструменты конкурентной разведки, электронный ресурс:

http://cirazvedka.ru/Themes/Pages/Internet_and_computers_as_CI_tools.html

7. Титов В.В. Конкурентная разведка в современных условиях, электронный ресурс:

<http://www.bre.ru/security/22722.html>

8. Баяндин Н. И. Противодействие промышленному шпионажу. Информационно-аналитическая работа, электронный ресурс:

<http://www.mbs-seminar.ru/seminars/seminar.php?seminar=4258>

9. Ющук Е.Л. Презентация «Что такое Конкурентная Разведка и чем она занимается (видео со звуком)», сайт «Сообщества Практиков Конкурентной разведки», электронный ресурс:

<http://www.youtube.com/watch?v=MyO33slbtFI>

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для прохождения практики (модуля)

1. Электронно-библиотечная система ЭБС Университетская библиотека онлайн <http://www.biblioclub.ru>

2. Электронно-библиотечная система ЭБС ZNANIUM.COM <http://www.znanium.com>

3. Официальный сайт Федеральной таможенной службы <http://customs.ru/>

4. Официальный сайт Евразийской Экономической комиссии <http://eurasiancommission.org/>

9. Методические указания по прохождению практики

Руководство практикой

Основными нормативно-методическими документами, регламентирующими работу студентов на практике, являются программа

практики и учебный план.

Утверждение базовых для прохождения практики учреждений и организаций осуществляется на основе заявлений студентов и соответствующего приказа, договора с организацией или иных нормативных документов.

Руководство кафедры и деканат факультета обеспечивают выполнение подготовительной и текущей работы по организации и проведению практики, осуществляют контроль ее проведения. Также организуют разработку и согласование программы практики с учреждениями-базами практики; назначают из числа опытных преподавателей кафедры руководителей практики; готовят и проводят совместно с ответственным за практику преподавателем организационные собрания студентов перед началом практики; организуют на кафедре хранение отчетов и дневников студентов по практике.

Отчетные документы и оценка результатов практики

Отчетными документами по практике являются:

1. Дневник по практике, включающий в себя отчет. По окончании практики студент представляет на кафедру дневник по практике, подписанный руководителем практики об организации и от ВУЗа.

Отчет о практике должен содержать сведения о конкретно выполненной студентом работе в период практики.

Отчеты студентов рассматриваются руководителями практики от учебного заведения и организации базы практик.

Дневник практики оформляется на стандартных листах формата А4.

По окончании практики студенты должны сдать документацию не позднее 3-х дней с момента окончания практики, а также защитить отчет (дневник по практике).

Защита практики представляет собой устный публичный отчет студента-практиканта, на который ему отводится 7–8 минут и ответы на вопросы руководителей практики. Устный отчет студента включает: раскрытие целей и задач практики, общую характеристику места практики, описание выполненной работы, выводы и предложения по содержанию и организации практики, совершенствованию программы практики.

К защите практики допускаются студенты, своевременно и в полном объеме выполнившие программу практики и предоставившие в указанные сроки всю отчетную документацию.

2. Отчет руководителя производственной практикой от предприятия / ВУЗа

Руководители практики представляют письменный отчет, в котором описывают содержание работы каждого студента на практике.

Форма дневника по практике и отчета по практике представлены ниже.

Памятка практиканту

До начала практики необходимо выяснить на кафедре место и время прохождения практики, получить дневник практики.

Во время прохождения практики необходимо строго соблюдать правила внутреннего распорядка, установленного в организации; полностью выполнять программу (план) практики; нести ответственность за выполняемую работу и ее результаты наравне со штатными работниками; вести научные исследования в интересах организации; вести дневник практики и по окончании практики предоставить его на подпись руководителям от ВУЗа / организации.

Дневник с отчетом предоставляются руководителям практики для оценки.

Потеря дневника равноценна не выполнению программы практики и получению неудовлетворительной оценки. Дневники хранятся на кафедре весь период обучения студента.

Права и обязанности студентов во время прохождения практики

Студент во время прохождения практики обязан:

1. Посещать все консультации и методические совещания, посвященные организации практики.
2. Знать и соблюдать правила охраны труда, выполнять действующие в организации правила внутреннего трудового распорядка.
3. В случае пропуска, опоздания сообщить руководителю заранее, объяснить причину отсутствия или опоздания, предоставить необходимые документы (справка о болезни, повестка и др.).
4. Выполнять задания, предусмотренные программой практики, требования руководителей практики.
5. Оформлять в ходе практики дневник по практике и предоставлять его непосредственным руководителям практики для проверки.
6. По завершении практики в точно указанные сроки подготовить отчет о результатах проделанной работы и защитить его с положительной оценкой.

Студент во время прохождения практики имеет право:

1. Обращаться к руководителям ВУЗа, руководству факультета и выпускающей кафедры по всем вопросам, возникающим в процессе практики.
2. Вносить предложения по совершенствованию процесса организации практики.
3. Пользоваться фондами библиотеки, кабинетами с выделенными линиями Интернета.

Памятка руководителю практики

Руководитель практики обязан: осуществлять непосредственное руководство практикой студентов на предприятии, в учреждении,

организации; обеспечивать высокое качество прохождения практики студентами и строгое соответствие ее учебным планам и программам; участвовать в организованных мероприятиях перед выходом студентов на практику (установочные конференции, инструктаж по технике безопасности и охране труда и т.д.); распределять студентов по местам прохождения практики; осуществлять контроль за соблюдением нормальных условий труда и быта студентов, находящихся на практике, контролировать выполнение практикантами правил внутреннего трудового распорядка; собирать и анализировать документацию, подготовленную студентами по итогам практики, составлять отчет по итогам практики и предоставлять его на кафедру; принимать участие в мероприятиях по защите отчета (дневника по практике), оценивать работу студентов-практикантов и оформлять ведомость и зачетные книжки.

Руководитель составляет отчет о результатах прохождения производственной практики студентами, обучающимися по направлению подготовки 10.03.01 «Информационная безопасность».

Отчет включает в себя: сроки практики, цели, тематику работы, указание организации, в которой проходила практика, список студентов-практикантов с описанием выполняемой ими работы и оценкой за защиту результатов практики.

10. Перечень информационных технологий, используемых при проведении практики

Перечень программного обеспечения: Microsoft Office Power Point, Microsoft Office Word, Microsoft Office Excel.

Информационные справочные системы:

Электронные ресурсы образовательной среды Университета:

- www.biblioclub.ru
- www.rucont.ru
- znanium.com
- e.lanbook.com

Информационно-справочные системы:

- Консультант+
- Гарант

11. Описание материально-технической базы, необходимой для проведения практики

Материально-техническое обеспечение производственной практики включает в себя: мультимедийную аудиторию для защиты отчетов, подготовленных с использованием MicrosoftOfficePowerPoint, MicrosoftOfficeWord, MicrosoftOfficeExcel для выполнения и оформления отчетов студентов по производственной практике, а также доступный для студента выход в Интернет с целью поиска современной информации по информационной безопасности (защите информации).



Государственное бюджетное образовательное учреждение высшего образования
Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

БЛОК 3. ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ

Вариативная часть

БЗ.Б.01(Д) Подготовка и защита ВКР

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО НАПИСАНИЮ
ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ**

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Год набора: 2020

Королев
2020

1. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО НАПИСАНИЮ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

1.1. Общие положения

Государственная итоговая аттестация направлена на установление соответствия уровня профессиональной подготовки выпускников требованиям федерального образовательного стандарта.

Основу выпускной квалификационной работы могут составлять стартапы в рамках регионального компонента образования с учетом основных направлений российских и коммуникационных технологий подготовки кадров для цифровой экономики (по ИТ-технологиям и предпринимательству) учитывая требования работодателей к качеству подготовки специалистов. Разработка стартапов является непрерывным многоступенчатым процессом и выполняется обучающимися на протяжении нескольких семестров.

Выполнение ВКР направлено на реализацию следующих компетенций:

способностью использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1);

способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2);

способностью анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3);

способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);

способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);

способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);

способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7);

способностью к самоорганизации и самообразованию (ОК-8);

способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9).

способностью анализировать физические явления и процессы для решения профессиональных задач (ОПК-1);

способностью применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2);

способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач (ОПК-3);

способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4);

способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5);

способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности (ОПК-6);

способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7).

способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);

способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);

способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3);

способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);

способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5);

способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6);

способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7);

способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8);

способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9);

способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области

информационной безопасности (ПК-10);

способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов (ПК-11);

способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12);

способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13);

способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14);

способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15);

способностью проводить совместный анализ функционального процесса защиты ТКС и ее информационных составляющих с целью определения возможных источников угроз, их вероятных целей (ПСК-1);

способностью формировать предложения по оптимизации функционального процесса и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов (ПСК-2);

способность организовывать контроль и анализ защищенности объектов ТКС в соответствии с нормативными документами (ПСК-3);

способность организовать реализацию принятых мер по управлению защитой информационных потоков на пакетном уровне с комплексной оценкой информационной безопасности ТКС (ПСК-4).

Государственная итоговая аттестация включает защиту выпускной квалификационной работы.

Требования к содержанию, объёму и структуре выпускной квалификационной работы (проекта) определяются высшим учебным заведением.

Выпускная квалификационная работа (ВКР) – это завершённая научно-практическая работа академического абитуриента по определенной проблеме, систематизирующая, закрепляющая и расширяющая, теоретические знания и практические навыки академического абитуриента при решении конкретной задачи, демонстрирующая умение самостоятельно решать профессиональные задачи и характеризующая итоговый уровень его квалификации, подтверждающая его готовность к профессиональной деятельности.

Выпускная квалификационная работа в соответствии с программой подготовки бакалавров выполняется в виде дипломной работы в период обучения студентов и прохождения практики и представляет собой самостоятельную и логически завершённую выпускную квалификационную

работу, связанную с решением задач того вида или видов деятельности, к которым готовится бакалавр.

Тематика выпускных квалификационных работ должна быть направлена на решение профессиональных задач в соответствии с п. 4.4 данного ФГОС.

При выполнении выпускной квалификационной работы обучающиеся должны показать свою способность и умение, опираясь на полученные углубленные знания, умения и сформированные универсальные и профессиональные компетенции, самостоятельно решать на современном уровне задачи своей профессиональной деятельности, профессионально излагать специальную информацию, научно аргументировать и защищать свою точку зрения.

Выпускная квалификационная работа (ВКР) – это самостоятельная (под руководством научного руководителя) научно-исследовательская работа, которая выполняет квалификационную функцию. Основная задача её автора – продемонстрировать уровень своей научной квалификации, умение самостоятельно вести научный поиск и решать конкретные научно-практические задачи.

ВКР должна отражать уровень фундаментальной и специальной подготовки в соответствии с требованиями Государственного образовательного стандарта высшего профессионального образования различных направлений подготовки бакалавров, а также умение применять приобретённые знания в научной и практической деятельности.

Бакалавр – квалификация (степень), присваиваемая выпускнику высшего учебного заведения, успешно прошедшему итоговую аттестацию и защитившему выпускную квалификационную работу.

Бакалавр должен обладать достаточной эрудицией, фундаментальной научной базой, владеть методологией научного познания, современными информационными технологиями, методами получения, обработки, хранения и использования научной информации, быть способен к плодотворной профессиональной деятельности.

Для выполнения ВКР студенту назначается научный руководитель. Взаимодействие студента с научным руководителем может осуществляться как контактно, так и по электронной почте, что позволяет оперативно взаимодействовать с профессорско-преподавательским составом (ППС) Университета.

При подготовке к написанию ВКР студенты могут воспользоваться современными информационными средствами (Internet, электронной библиотекой Университета и т.д.), предоставляемыми Университетом. Это даёт возможность в индивидуальном режиме активно вести поиск ответов на возникающие вопросы по выбору темы, поиску литературы, современного состояния научных и практических достижений в области выбранного направления исследования.

Студенту необходимо помнить, что он лично отвечает за качество и оформление выпускной работы.

Совокупность полученных в ВКР результатов должна свидетельствовать о наличии у её автора достаточных первоначальных навыков самостоятельной научной работы в избранной области профессиональной деятельности. Обязательным признаком успешного выполнения ВКР является демонстрация такого уровня научной квалификации, который позволяет самостоятельно вести научный поиск, анализировать исследуемые проблемы, формулировать их в виде конкретных задач, умело использовать научную литературу и знание методов и приёмов для их грамотного решения; при необходимости, моделировать исследуемые процессы и получать экспериментальные результаты, делать правильные выводы, обосновывать и предлагать практическую реализацию исследуемых задач и выдвинутых решений.

Задачи, поставленные в ВКР, должны быть выполнены на современном уровне развития науки и техники по выбранному направлению.

Защита ВКР проводится в соответствии с действующим порядком проведения итоговой аттестации, утвержденным решением Ученого совета Университета.

ТРЕБОВАНИЯ К СОДЕРЖАНИЮ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ БАКАЛАВРА

1.1. Выбор темы, требования к названию

Выбор темы для выпускной квалификационной работы (ВКР) имеет исключительно большое значение. Практика показывает, что правильно выбрать тему – значит наполовину обеспечить успешное её выполнение. Под темой ВКР принято понимать то главное, чему она посвящена.

Тематика выпускных квалификационных работ должна быть направлена на решение профессиональных задач в соответствии с п. 4.4 данного ФГОС.

При выборе темы студент, с помощью научного руководителя, должен уяснить, в чем заключаются содержание ВКР, сущность положенных в её основу идей, их новизну, актуальность и практическую ценность. Кроме того необходимо уяснить входящие в тему задачи и предполагаемые пути их решения, предполагаемые результаты и объём работы, оценить значимость темы для формирования бакалавра как специалиста высокой квалификации.

Выбор темы студентом совместно с научным руководителем исходит из накопленных знаний, опыта, практики прошлой работы, близких ему проблем, актуальных в избранной области исследования.

Научный руководитель направляет работу студента, помогая ему оценить возможные варианты решений. Но выбор окончательного решения – задача самого студента. Он как автор выполняемой работы отвечает за верный её выбор, за правильность полученных результатов и их фактическую точность.

Тема ВКР определяется и утверждается в установленном порядке в конце обучения бакалавра. Студент может выбрать тему из рекомендуемого кафедрой ИБ перечня тем ВКР, но может предложить и свою тему, предварительно обосновав целесообразность её разработки.

Тематика ВКР по направлению подготовки: 10.03.01 «Информационная безопасность» должна быть направлена на решение следующих профессиональных задач:

- анализ и моделирование предметной области с использованием современных информационных технологий;
- анализ показателей и технико-экономическое обоснование проекта по информационной безопасности;
- исследование и разработка информационно-программных продуктов для решения прикладных задач информационной безопасности;
- исследование бизнес-процессов прикладной области и проведение реинжиниринга;
- проектирование современных систем защиты информации и её компонентов в прикладной области в соответствии с профессиональным профилем;
- исследование и разработка эффективных методов управления информационной безопасностью предприятий, фирм и организаций;
- разработка нормативных методических и производственных документов в процессе проектирования и реализации систем информационной безопасности.

Заявление на ВКР бакалавра приведено в приложении 1. Образец титульного листа ВКР приведен в приложении 2. Задание на ВКР и сроки её выполнения фиксируются на бланке (приложение 3), что является фактическим её утверждением.

Свобода выбора тем ВКР позволяет реализовать индивидуальные научные интересы будущего бакалавра, его основные подходы к изучению и решению проблемы.

1.2. Разработка рабочего плана

При выполнении ВКР, обучающиеся должны показать свою способность и умение, опираясь на полученные углубленные знания, умения и сформированные универсальные и профессиональные компетенции, самостоятельно решать на современном уровне задачи своей профессиональной деятельности, профессионально излагать специальную информацию, научно аргументировать и защищать свою точку зрения.

Для разработки рабочего плана ВКР студент должен чётко представлять её структуру.

Содержание ВКР включает в себя: введение; обзор и анализ литературы, нормативной базы; теоретическую часть; практическую часть (научно-экспериментальную); выводы и заключение с рекомендациями

относительно возможностей применения полученных результатов; список использованных источников; глоссарий; приложения.

Общий объём выпускной квалификационной работы (без приложений) составляет для бакалавров 80-100 страниц выровненного по ширине компьютерного текста. Требования, предъявляемые к объёму и оформлению ВКР, приведены в приложении 4.

Основная часть ВКР, как правило, состоит из трёх глав, каждая из которых в свою очередь делится на 3-5 параграфов. В первой главе, посвященной обзору и анализу литературы, связанной с темой ВКР, приводятся различные точки зрения по исследуемому направлению, определяется круг нерешённых проблем, задач, которые могли бы стать основой анализа в ВКР.

Так, обзор литературы может включать описание концепций по теоретическим основам направления исследования, и в этом случае студент может провести анализ позитивных, спорных и негативных сторон той или иной концепции, что уже составит элемент научной новизны ВКР. Аналогичным образом может быть проведен анализ методологических, методических основ и подходов к исследованию выбранной темы.

Во второй главе представляется проблема исследования, которая может относиться как к научной, так и к практической составляющей ВКР и иметь либо качественную направленность, либо формальную возможность представления, например, в виде экономико-математической модели, либо сводиться к практической задаче. Здесь же обосновывается методика исследования, описываются источники информации, их достоверность и репрезентативность, проводится анализ экспериментальных данных.

В третьей главе как основной части в зависимости от поставленных задач ВКР излагается обоснование разработанной методологии, применяется выбранная или разработанная методика к решению, описывается и анализируется алгоритм решения, конкретизируются и аргументируются научные и практические положения полученных результатов исследования, предлагаются дальнейшие пути развития анализируемых проблем и т.п. Параграфы обзорной и практической части определяются в зависимости от профиля подготовки бакалавров и темы ВКР.

ВКР, выполняя квалификационные функции, является самостоятельной научно-исследовательской работой, а любая научная работа предполагает наличие плана её осуществления. Планирование работы начинается с составления рабочего плана, представляющего собой своеобразную наглядную схему предпринимаемого исследования.

Правильно составленный план позволяет продуктивно организовать исследовательскую работу по избранной теме и представить её в установленные сроки. Рабочий план подготовки ВКР составляется параллельно с предварительным изучением и отбором литературы, согласовывается с научным руководителем.

Рабочий план имеет произвольную форму и «подвижный» характер, позволяющий включать в него новые аспекты, появляющиеся в процессе разработки темы.

Научный руководитель оказывает помощь в подборе необходимой литературы, нормативных, справочных, статистических и архивных материалов и других источников по теме.

1.3. Библиографический поиск, сбор, анализ и обобщение литературных источников

Знакомство с опубликованной по теме ВКР литературой начинается с разработки идеи, т.е. замысла предполагаемого научного исследования, который находит своё выражение в теме и рабочем плане выполняемой работы. Такая постановка вопроса позволяет более целеустремленно искать литературные источники по выбранной теме, глубже осмысливать тот материал, который содержится в опубликованных в печати работах других учёных, ибо основные положения и проблемы почти всегда изложены в более ранних исследованиях.

Далее следует продумать порядок поиска и приступить к составлению списка литературных источников по теме. Хорошо составленный список даже при беглом обзоре заглавий источников позволяет охватить тему в целом. На её основе возможно уже в начале исследования уточнить цели.

Целесообразно просмотреть все виды источников, содержание которых связано с темой исследования. К ним относятся материалы, опубликованные в различных отечественных и зарубежных изданиях, а так же непубликуемые документы и другие официальные материалы.

Сбор литературы по теме исследования (в том числе нормативной, первоисточников, научной и учебной) начинается с подготовки библиографического списка, который должен всесторонне охватывать исследуемую тему.

Источниками для формирования библиографического списка могут быть:

- список обязательной и рекомендованной литературы по теме ВКР;
- Internet;
- библиографические списки и сноски в учебниках и научных изданиях (монографиях, научных статьях) последних лет или диссертациях по данной тематике;
- рекомендации научного руководителя в том числе через систему IP;
- каталоги электронной библиотеки и библиотек, к которым библиотека Университета предоставляет доступ в режиме виртуального читального зала.

В первую очередь следует подбирать литературу за последние 3-5 лет, поскольку в ней отражены наиболее актуальные научные достижения по данной проблеме, современное законодательство и актуальная практическая деятельность. Использование литературных и иных источников 10-ти, 20-ти

или даже 30-ти летней давности должно быть скорректировано применительно к современным концепциям учёных и специалистов.

Указание на литературные источники по исследуемой теме можно встретить в сносках и списке литературы уже изданных работ. Поиск статей в научных журналах следует начинать с последнего номера соответствующего издания за определённый год, так как в нём, как правило, помещается указатель всех статей, опубликованных за год.

Полезно просматривать профессиональные и специализированные периодические издания (журналы, газеты, сборники научных трудов).

Для подготовки ВКР каждый студент имеет уникальную возможность работать с литературой по теме, используя электронную библиотеку МГОТУ. Электронная библиотека предоставляет доступ в режиме виртуального читального зала к ресурсам удалённого доступа электронных библиотек:

– Библиотека электронных диссертаций Российской государственной библиотеки (ЭБД РГБ).

– Научная электронная библиотека (НЭБ);

– Открытая русская электронная библиотека;

– Единое окно доступа к образовательным ресурсам;

– База электронных диссертаций «Proquest digital dissertations»;

– Коллекция электронных журналов «Sage journals online»;

– База журналов открытого доступа «Directory of open access journals» и др.

др.

При написании ВКР (научно-исследовательской работы) большой интерес представляет «Единое окно доступа к образовательным ресурсам». В электронной библиотеке Единого окна размещены образовательные информационные ресурсы, разработанные ведущими российскими Вузами: учебники, тексты лекций, методические указания и др.

Работа с научной книгой начинается с изучения титульного листа, где приводятся данные об авторе и выходные сведения (год и место издания), а также оглавления. Год издания книги позволяет соотнести информацию, содержащуюся в ней, с существующими знаниями по данной проблеме на современном этапе. В оглавлении книги раскрываются ключевые моменты её содержания, логика и последовательность изложения материала.

После этого надо ознакомиться с введением, где, как правило, формулируется актуальность темы, кратко излагается содержание книги и её направленность, раскрываются источники и способы исследования, степень разработанности проблемы.

Ознакомление можно завершить постраничным просмотром, обратив внимание на научный аппарат, частично расположенный в сносках, на определения ключевых понятий, полноту изложения заявленных в оглавлении вопросов.

При изучении специальной (научной) литературы полезно обращаться к различным словарям, энциклопедиям и справочникам в целях выяснения смысла специальных понятий и терминов, конспектируя те из них, которые в

дальнейшем будут использованы в тексте работы и при составлении глоссария.

Фонд справочных, нормативных и официальных изданий Университета содержит энциклопедии (отраслевые и универсальные); словари и различные справочники.

Изучение нормативных документов – законов, подзаконных актов, постановлений – является обязательным, так как знание этих документов и умение работать с ними – залог успешной научно-исследовательской и профессиональной деятельности.

Университет, являясь так же пользователем справочно-информационных систем «Гарант» и «Консультант Плюс», предоставляет возможность каждому обучающемуся быть в курсе последних изменений в законодательстве, получать свежие материалы по правовой и финансовой информации.

В ходе анализа собранного по теме исследования материала студент выбирает наиболее обоснованные и аргументированные конспективные записи, выписки, цитаты и систематизирует их по ключевым вопросам исследования. На основе обобщённых данных уточняется структура исследования по ВКР, его содержание и объём.

Если структура работы первоначально определяется на стадии планирования ВКР, то в ходе её написания могут возникнуть новые идеи и соображения. Поэтому не рекомендуется окончательно структурировать работу сразу же после сбора и анализа материалов.

1.4. Основные части работы

Каждая структурная часть ВКР имеет своё назначение. Оформляя работу, студент должен помнить, что каждая структурная часть (содержание, введение, основная часть, заключение, глоссарий, библиография) начинается с новой страницы.

Содержание (или оглавление) включает в себя заголовки всех разделов (глав, параграфов и т.д.), содержащихся в работе. Обязательное требование – дословное повторение в заголовках содержания (или оглавления) названий разделов, представленных в тексте, в той же последовательности и соподчиненности.

Во введении кратко характеризуется проблема, решению которой посвящена исследовательская работа. (Проблема – это теоретический или практический вопрос, ответ на который пока неизвестен, и на который нужно ответить.)

Проблема может быть обобщённым множеством сформулированных научных вопросов как области будущих исследований и соответствует постановке и решению крупных задач теоретического и прикладного характера, требующих получения новых знаний. Именно на разрешение проблемы или её части (противоречия) направляется работа.

Во введении обычно обосновываются актуальность выбранной темы, цель исследований и содержание поставленных задач, формулируются объект и предмет исследования, указывается избранный метод (или методы) исследования, сообщается, в чем заключаются теоретическая значимость и прикладная ценность полученных результатов.

Актуальность – обязательное требование к любой научно-исследовательской работе. В применении к ВКР понятие «актуальность» имеет одну особенность. Поскольку ВКР является квалификационной работой, и то, как её автор умеет выбрать тему и насколько правильно он эту тему понимает и оценивает с точки зрения современности и социальной значимости, характеризует его научную зрелость и профессиональную подготовленность.

Освещение актуальности темы должно быть немногословным. Начинать её описание издалека нет особой необходимости. Достаточно в пределах 1-2 страниц текста показать главное – суть проблемы, из чего и будет видна актуальность темы. Наиболее эффективной работа бакалавра окажется в том случае, если рассмотрение выбранной проблемы будет связано с профилем той области знания, в которой он специализируется.

Таким образом, введение – очень ответственная часть ВКР, поскольку оно не только ориентирует автора на дальнейшее раскрытие темы, но и содержит все её необходимые квалификационные характеристики.

Степень разработанности проблемы. Краткий обзор литературных источников позволяет автору сделать вывод, что именно данная тема не полностью раскрыта (или раскрыта лишь частично или не в том аспекте) и требует дальнейшей разработки. Во введении необходимо показать недостаточность разработанности выбранной темы исследования на современном этапе развития общества, необходимость изучения проблемы в новых социально-экономических, юридических (правовых), политических и иных условиях и т.п.

Обзор литературы по теме должен показать основательное знакомство студента со специальной литературой, его умение систематизировать источники, критически их рассматривать, выделять существенные моменты, оценивать ранее сделанные другими исследователями открытия, определять главное в современном состоянии изученности темы, а также критически оценивать, сопоставлять разные концепции, научные направления, методологические подходы, связанные с темой исследования, аргументированно вырабатывать собственную точку зрения.

От формулировки научной проблемы и доказательства того, что та часть этой проблемы, которая является темой данной ВКР, еще не получила своей разработки и освещения в специальной литературе, уместно перейти к формулировке цели предпринимаемого исследования, а также указать на конкретные задачи, которые предстоит решить в связи с этим. Обычно это делается в форме перечисления (изучить..., описать..., установить..., выявить..., вывести формулу... и т.п.).

Цель исследования – это мысленное предвосхищение (прогнозирование) результата, определение оптимальных путей решения задач в условиях выбора методов и приёмов исследования в процессе проведения ВКР.

Задачи исследования определяются поставленной целью и представляют собой конкретные последовательные этапы (пути) решения проблемы исследования по достижению основной цели.

Объект и предмет исследования. Обязательным элементом введения является формулировка объекта и предмета исследования. Объект – это процесс или явление, порождающее проблемную ситуацию, которое автор избрал для исследования. Предмет – это то, что находится в границах объекта.

Нередко объект исследования определить достаточно сложно из-за множественности понятий, предметов, связей в различных видах деятельности. Определение же предмета исследования – это, прежде всего, уточнение «места и времени» действия. Объект отражает проблемную ситуацию, рассматривает предмет (аспект) исследования во всех его взаимосвязях. Проще говоря, это определённая область реальной действительности либо сфера общественной жизни (социально-экономической, политической, организационной, правовой и т.д.).

Объект исследования всегда шире, чем его предмет. Если объект – это область деятельности, то предмет – это изучаемый процесс в рамках этой области.

Именно на предмет исследования направлено основное внимание автора, именно предмет определяет тему работы. Для его исследования (предмета) формулируются цель и задачи.

Часто конкретное исследование начинается с гипотезы.

Гипотеза – научное предположение, выдвигаемое для объяснения каких-либо явлений; это мысленное представление обобщённых положений, основных идей, к которым может привести исследование. Студент после предварительного изучения фактов, характерных черт и условий по выбранной теме формулирует предположение о результатах исследования. Рассуждение при этом идёт от следствия к причине.

Гипотеза должна быть обоснованной и внутренне непротиворечивой.

Представляются методы исследования, которые будут использованы в процессе выполнения работы и послужат инструментом в добывании необходимого фактического материала.

Любой метод – это совокупность приёмов, шагов для достижения цели.

Например, при исследовании возможно использовать следующие методы:

- анализ научной литературы;
- обобщение отечественной и зарубежной практики;
- моделирование, сравнение, аналогия, синтез, интервьюирование и т.п.

Практическая значимость. Практическая значимость заключается в возможности использования результатов исследования в практической

деятельности, независимо от того – является данная ВКР теоретической или практической разработкой.

Необходимо отметить важное правило – введение, как и заключение, рекомендуется писать после полного завершения основной части. До того, как будет создана основная часть работы, реально невозможно написать хорошее введение, так как автор ещё не вполне овладел материалами по теме.

Объём введения для ВКР составляет 3-5 страниц выровненного по ширине машинописного текста.

Основная часть. Основная часть исследования должна соотноситься с поставленными задачами. Она обычно делится на 3 главы.

Главы основной части должны быть соразмерны друг другу по объёму. Каждую главу целесообразно разделить на 2 - 4 параграфа. Предварительная структура основной части работы (главы, параграфы) определяется ещё на стадии планирования. Однако в ходе написания могут возникнуть новые идеи и соображения, которые побуждают не только изменить и уточнить структуру, но и обогатить содержание работы или увеличить её объём.

Обязательным атрибутом исследования является краткий обзор привлечённых источников и литературы. Обзор литературы приводится в основной части исследования. При этом разделяют обзор первоисточников и обзор собственно литературы. Под первыми понимают тексты, которые являются объектом исследования. К ним относятся исторические документы, законодательные и иные нормативные документы. Под вторыми – литературные источники, которые используются, но при этом не являются предметом исследования. Умение различать эти две группы источников чрезвычайно важно.

В главах основной части ВКР подробно анализируется литература по теме, рассматривается методика и техника исследования, обобщаются результаты. Содержание глав основной части должно точно соответствовать теме ВКР, полностью её раскрывать. Эти главы призваны показать умение студента сжато, логично и аргументировано излагать материал.

Содержанием основной части ВКР является обзор и анализ литературы по теме, сопоставление различных точек зрения на концептуальное развитие научного направления, в рамках которого проходит исследование, на методологию изучения проблемы.

В содержании приводится обоснование или разработка собственных алгоритмов решения поставленных в ВКР задач, обоснование достоверности и репрезентативности используемой информации. Другими словами, в основной части приводится теоретическое осмысление проблемы, даётся изложение эмпирического и фактического материала. Последовательность изложения того и другого может быть различной.

Чаще всего вначале излагаются основные теоретические положения по исследуемой теме, а затем конкретный практический материал, который аргументированно подтверждает изложенную теорию.

Но возможна и другая последовательность, когда вначале анализируется конкретный материал, а затем на основе этого анализа делаются теоретические обобщения и выводы.

В конце каждой главы должны быть сформулированы краткие выводы.

Объём основной части выпускной квалификационной работы для бакалавров – 60-80 страниц.

Заключение. ВКР заканчивается заключительной частью. Как и всякое заключение, эта часть выполняет роль концовки, обусловленной логикой проведения исследования, которая носит форму синтеза накопленной в основной части научной и практической информации.

Заключение содержит краткую формулировку результатов, полученных в ходе работы. В заключении, как правило, автор исследования суммирует результаты осмысления темы, выводы, обобщения и рекомендации, которые вытекают из его работы, подчеркивает элементы научной новизны, их практическую значимость, а также определяет основные направления для дальнейшего исследования в этой области знаний.

Заключение может включать в себя научные и практические предложения, что повышает ценность ВКР. Но такие предложения должны обязательно исходить из круга работ, проведенных лично автором и внедрённых на практике.

Заключительная часть ВКР представляет собой не простой перечень полученных результатов проведённого исследования, а формулирование того нового, что внесено её автором в изучение и решение проблемы.

Необходимо иметь в виду, что введение и заключение никогда не делятся на части.

Объём заключения примерно равен 2-3 страницы.

Глоссарий. В научном мире при выполнении учебно-научных работ предусмотрено составление глоссария, он является обязательным компонентом ВКР.

Глоссарий – толковый (объясняющий) словарь понятий и терминов.

Автор, используя в тексте ВКР термины, которые правильно раскрывают их содержание, показывает степень включённости в сферу профессии и готовность к научной деятельности.

В глоссарий, как правило, включаются основные профессиональные термины (а также их английские либо латинские аналоги, в необходимых случаях аналоги и на других языках), факты, персоналии, важнейшие даты. Формулировка понятий глоссария должна соответствовать формулировкам в различных словарях, энциклопедиях, справочниках и в документах законодательного характера.

Количественное и качественное наполнение глоссария учитывается при оценивании как учебно-научных, так и научно-исследовательских работ обучающихся.

Список использованных источников. Список использованных источников является обязательным атрибутом любой учебно-

исследовательской работы. Этот список составляет одну из существенных частей ВКР и отражает самостоятельную творческую работу студента.

Данный список включает библиографические описания всех использованных, цитированных или упоминаемых в работе документов, а также прочитанную литературу по теме, которая оказала существенное влияние на содержание работы.

Список сокращений, если он окажется необходимым в ВКР, должен включать в себя расшифровку наиболее часто упоминаемых в работе сокращенных наименований документов, научно-исследовательских институтов, предприятий, акционерных обществ, понятий, слов и т.д. Но, как правило, в тексте ВКР следует избегать сокращений слов, за исключением общепринятых. Считается, что чем меньше сокращений слов и словосочетаний употребляется в научной работе, тем грамотнее она оформлена.

Приложения являются необязательным компонентом выпускной квалификационной работы. В приложениях, как правило, следует приводить различные вспомогательные материалы (таблицы, схемы, графики, диаграммы, иллюстрации, копии постановлений, договоров, инструкции, вспомогательные расчеты и т.п.). С одной стороны, они призваны дополнять и иллюстрировать основной текст, с другой, – разгружать его от второстепенной информации. Все материалы, помещенные в приложениях, должны быть обязательно связаны с основным текстом, в котором делаются ссылки на соответствующие приложения.

Приложения не засчитываются в заданный объем работы.

1.5. Оформление работы

Этап оформления ВКР является не менее важным, чем остальные, так как на этом этапе автор должен не только свести все материалы по работе в единый документ, но и оформить в соответствии с требованиями.

При оформлении глоссария автор проверяет соответствие понятий, данных в тексте, с понятиями, приведенными в глоссарии. Количество понятий, приведенных в глоссарии, должно полностью соответствовать количеству понятий, используемых в тексте. Следует приводить четкие определения понятий, терминов, а не пояснения к ним.

Не допускается включать в глоссарий понятия, выраженные несколькими различными терминами, например, «сырьё и основные материалы». Комментарий должен быть конкретным, научным и достоверным.

Глоссарий составляется по алфавиту в табличной форме, предусматривающей три графы (столбца). Лексические единицы в глоссарии систематизируются в алфавитном порядке. Образец оформления глоссария представлен в приложении 5.5.

К оформлению чистового варианта ВКР приступают, когда все материалы собраны, сделаны необходимые обобщения, которые получили

одобрение научного руководителя. Затем начинается детальная шлифовка текста рукописи. Проверяются и критически оцениваются каждый вывод, формула, таблица, каждое предложение, каждое отдельное слово.

После подготовки чистового варианта необходимо ещё раз отредактировать текст, устранить все опечатки. Далее следует проверить логику работы - насколько точен смысл абзацев и отдельных предложений, соответствует ли содержание глав их заголовкам.

Далее следует проверить, нет ли в работе пробелов в изложении материала и аргументации, устранить стилистические погрешности, обязательно проверить точность цитат и ссылок, правильность оформления, обратить особое внимание на написание числительных и т.д.

Целенаправленная завершающая работа с текстом характеризует ответственность автора за представляемый материал, его уважение к руководителю, рецензенту и членам аттестационной комиссии, оценивающим работу.

Лишь после такой корректуры следует сделать окончательный вариант работы для проведения нормоконтроля.

Правила оформления научных работ являются общими для всех направлений исследовательской деятельности и регламентируются действующими государственными стандартами.

Оформленная работа должна быть сброшюрована в следующей последовательности:

Титульный лист (приложение 5.2);

Задание на выполнение выпускной квалификационной работы (приложение 5.3);

Результаты нормоконтроля ВКР (приложение 5.6);

Содержание (оглавление) работы;

Введение;

Основная часть;

Заключение;

Глоссарий (образец оформления, приложение 5.5);

Список использованных источников;

Список сокращений (если используются при написании);

Приложения (по мере необходимости).

Подготовленная к защите ВКР, предварительно прошедшая нормоконтроль, сдаётся научному руководителю.

Научный руководитель анализирует содержание ВКР на соответствие заявленной теме, оценивает уровень разработанности проблемы, степень использования привлекаемых материалов, правильность структурирования материала, грамотность изложения, достоверность и обоснованность полученных результатов, аргументированность выводов.

Научный руководитель даёт письменное заключение (отзыв) (приложение 5.7) о степени соответствия работы требованиям, предъявляемым к выпускной квалификационной работе бакалавра.

Отзыв – это оценка не только качества работы выпускника, но и оценка его работы над выбранной темой, его активности, системности мышления, уровня знаний, умения искать и находить нужную информацию, качества материала, самостоятельности в исследованиях и пр. Научный руководитель оформляет допуск к защите выпускной квалификационной работы на титульном листе (приложение 5.2).

При выявлении серьезных недоработок, касающихся содержания или оформления, ВКР не допускается к защите и возвращается выпускнику на доработку с указанием срока повторного представления.

В случае если ВКР не представлена в установленный срок или не допущена к защите, выпускник отчисляется из МГОТУ как не прошедший итогового аттестационного испытания.

Вместе с оформленной и сброшюрованной выпускной квалификационной работой выпускник представляет научному руководителю (и в дальнейшем на защиту) тщательно оформленные демонстрационные плакаты или сброшюрованный «раздаточный материал», экземпляры которого передаются каждому члену аттестационной комиссии. Титульный лист демонстрационных материалов к выпускной квалификационной работе (приложение 5.8) должен быть подписан выпускником и его научным руководителем.

Назначение демонстрационного («раздаточного материала») – акцентировать внимание членов аттестационной комиссии на результатах, полученных выпускником при выполнении ВКР. На нём отражаются схемы, графики, диаграммы, таблицы и другие данные, характеризующие результаты выполненной научно-исследовательской работы. При этом содержание демонстрационного и раздаточного материала должно быть органически связано с содержанием доклада.

Все выносимые выпускником на защиту демонстрационные материалы обязательно должны присутствовать (дублироваться) в соответствующих разделах ВКР.

Не допускается представление на защиту выпускной квалификационной работы, демонстрационных и раздаточных материалов, по своему содержанию не связанных непосредственно с текстом доклада, а как бы оживляющих и украшающих доклад или свидетельствующих о широте кругозора студента.

Также не допускается представление на защиту демонстрационных и раздаточных материалов, на которые не делается ссылок в докладе. В большинстве случаев для иллюстрации результатов ВКР достаточно 4 - 6 электронных слайдов или компьютерных распечаток в «раздаточном материале».

В приложении 5.9 даётся примерный перечень информации, которую рекомендуется размещать на демонстрационных слайдах или в «раздаточном материале».

1.6. Подготовка к защите выпускной квалификационной работы бакалавра

Подготовка к защите ВКР – ответственный процесс. Важно не только написать высококачественную работу, но и уметь квалифицированно её защитить.

Студент, получив положительный отзыв на ВКР от научного руководителя, внешнюю рецензию и допуск к защите, должен подготовить доклад (до 10 -12 минут), в котором чётко и кратко излагаются основные положения ВКР.

Для успешной защиты необходимо хорошо выучить доклад. Текст выступления должен быть максимально приближен к тексту ВКР, поэтому основу выступления составляют введение и заключение, которые используются в выступлении практически полностью. Также практически полностью используются выводы в конце каждой из глав.

Доклад следует начинать с описания научной проблемы и обоснования актуальности избранной темы, обзора других научных работ по избранной проблеме, формулировки цели и задач работы.

Надо указать, какие методы были использованы при исследовании рассматриваемой проблемы, а далее, по главам раскрывать основное содержание работы, обращая особое внимание на наиболее важные разделы и интересные результаты, критические сопоставления и оценки.

Заключительная часть доклада строится по тексту заключения ВКР. В ней перечисляются общие выводы по работе без повторения частных обобщений, сделанных при характеристике глав основной части, собираются воедино основные рекомендации.

Доклад не должен быть перегружен цифровыми данными, которые приводятся лишь в случае необходимости для доказательства или иллюстрации того или иного вывода.

Рекомендации к структуре доклада на защите ВКР приведены в приложении 5.10.

1.7. Рекомендации по составлению компьютерной презентации ВКР с помощью пакета Microsoft PowerPoint

Компьютерная (электронная) презентация (КП) даёт ряд преимуществ перед обычной – плакатной.

В широком смысле слова презентация – это выступление, доклад, защита законченного или перспективного проекта, представление на обсуждение рабочего проекта, результатов исследования и т.п.

Использование КП позволяет значительно повысить информативность и эффективность доклада при защите ВКР, способствует увеличению динамизма и выразительности излагаемого материала.

Написание презентации к защите всегда ответственная, кропотливая, но полезная работа. Полезная, так как приводит в порядок мысли студента, классифицирует материал, позволяет вскрыть «узкие» места.

Презентация – суть всего перечисленного, поскольку весь отобранный и подготовленный выпускником материал наглядно отображается на экране в концентрированном, сжатом виде, и все огрехи здесь становятся достаточно рельефными. Поэтому один из главных положительных моментов при создании электронных презентаций – максимальная собранность выпускника. Работая с мультимедийными презентационными технологиями, он показывает умение представлять итоги своего труда с привлечением современных средств редактирования, выполнять требования, предъявляемые к уровню подготовки бакалавра, изложенные в Государственном образовательном стандарте для различных направлений.

Презентация позволяет членам аттестационной комиссии одновременно изучать выпускную квалификационную работу и контролировать выступление выпускника. Поэтому желательно сопровождать выступление презентацией с использованием 10-12 слайдов.

Основными принципами при составлении подобной презентации являются лаконичность, ясность, уместность, сдержанность, наглядность (подчеркивание ключевых моментов), запоминаемость (разумное использование ярких эффектов).

Необходимо начать КП с заголовочного слайда и завершить итоговым. В заголовке приводится тема исследования (название) и её автор (Ф.И.О.).

Сделайте нумерацию слайдов и напишите, сколько всего их в презентации. В итоговом слайде уместно поблагодарить руководителя и всех, кто давал ценные консультации и рекомендации.

Основное требование – каждый слайд должен иметь заголовок и номер по порядку, количество слов в слайде не должно превышать - 40.

Для оформления профессиональной КП можно использовать дизайн шаблонов (Формат – Применить оформление). Не следует увлекаться яркими шаблонами, так как информация на слайде должна быть контрастна фону, а фон не должен затенять содержимое слайда, если яркость проецирующего оборудования будет недостаточной.

Не следует злоупотреблять эффектами анимации. Оптимальной настройкой эффектов анимации является появление в первую очередь заголовка слайда, а затем – текста по абзацам. При этом если несколько слайдов имеют одинаковое название, то заголовок слайда должен постоянно оставаться на экране.

Динамическая анимация эффективна тогда, когда в процессе выступления происходит логическая трансформация существующей структуры в новую структуру, предлагаемую Вами. Настройка анимации, при которой происходит появление текста по буквам или словам, может вызвать негативную реакцию со стороны членов комиссии, которые одновременно должны выполнять 3 различных дела: слушать выступление, бегло изучать текст работы и вникать в тонкости визуального преподнесения

материала исследования. Практически визуальное восприятие слайда презентации занимает от 2 до 5 секунд времени, в то время как продолжительность некоторых видов анимации может превышать 20 секунд.

Для настройки временного режима презентации используется меню - Показ слайдов - Режим настройки времени. Предварительно надо определить, сколько минут требуется на каждый слайд.

Очень важно не торопиться при докладе и чётко произносить слова. Презентация, конечно, поможет Вам провести доклад, но она не должна его заменить. Желательно подготовить к каждому слайду заметки по докладу (Вид - страницы заметок). Можно распечатать некоторые ключевые слайды в качестве раздаточного материала.

2. ПРИНЦИПЫ ОЦЕНИВАНИЯ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ БАКАЛАВРА

В соответствии с Государственными образовательными стандартами высшего профессионального образования, другими нормативными документами Минобразования и науки России выпускные квалификационные работы бакалавров подлежат обязательному рецензированию.

В числе рецензентов могут быть работники министерств, ведомств, предприятий (организаций, фирм), преподаватели и научные сотрудники Университета и других вузов, исследовательских учреждений, предприниматели без образования юридического лица и иные специалисты. Основные требования для назначения рецензентом – наличие у предполагаемого эксперта высшего профессионального образования и достаточно высокая компетенция в той сфере деятельности, по которой выполнена выпускная квалификационная работа.

Для экспертизы ВКР рекомендуется привлекать также внешних рецензентов.

При оценке выпускной квалификационной работы студента исходят из того, что он должен уметь:

- формулировать цель и задачу исследования;
- составлять план исследования;
- вести библиографический поиск с применением современных информационных технологий;
- использовать современные методы научного исследования, модифицировать имеющиеся методы, исходя из задач конкретного исследования;
- обрабатывать полученные данные, анализировать и синтезировать их на базе известных литературных источников;
- использовать и правильно истолковывать профессиональные термины и понятия;
- оформлять результаты исследований соответственно современным требованиям.

С целью унификации внутренних и внешних рецензий, поступающих на выпускные работы бакалавров, рекомендуется использовать единую форму рецензии (образец рецензии представлен в приложении 5.11).

2.1. Справка о внедрении рекомендаций выпускной квалификационной работы бакалавра

Справка о внедрении рекомендаций выпускной квалификационной работы (ВКР) не является обязательным документом для её защиты на заседании аттестационной комиссии. Однако наличие такой справки характеризует высокий уровень выполнения ВКР и готовность будущего бакалавра квалифицированно решать профессиональные задачи.

Поэтому в МГОТУ поощряется представление на защиту справки о внедрении тех или иных рекомендаций ВКР в практику работы конкретного предприятия (организации, фирмы и т.п.). В первую очередь это относится к предприятию, на примере которого выполнялась ВКР.

Справка пишется в произвольной форме, но с обязательным указанием конкретных рекомендаций студента, которые использованы на предприятии (организации, фирме и т.п.), а также конкретного места (участка, цеха, подразделения, службы, отдела и т.п.), где эти рекомендации были применены.

Справка прилагается к ВКР и представляется в аттестационную комиссию.

Образец справки о внедрении приводится в приложении 5.11.

2.2. Процедура публичной защиты выпускной квалификационной работы бакалавра

До начала заседания Государственной аттестационной комиссии* ВКР должны быть сданы секретарю для контроля правильности оформления и сверки фамилии, имени, отчества выпускника, темы ВКР, фамилии, имени, отчества научного руководителя ВКР, номера приказа о допуске к защите с соответствующими документами. Необходимый комплект документов, который перед защитой должен иметь выпускник, перечислен в приложении 5.12.

Защита ВКР проходит в торжественной обстановке, публично, на открытом заседании аттестационной комиссии. Идентификация выпускников на итоговых аттестационных испытаниях проводится традиционно: визуально и по паспортам.

* Государственная экзаменационная комиссия по аккредитованному направлению подготовки (специальности) включает в себя Государственные экзаменационные комиссии по приему итоговых государственных экзаменов и Государственные экзаменационные комиссии по защите выпускных квалификационных работ (ГЭК).

Экзаменационная комиссия по не аккредитованному направлению подготовки (специальности) включает в себя Экзаменационные комиссии по приему итоговых экзаменов и Экзаменационные комиссии по защите выпускных квалификационных работ (ЭК).

В начале работы комиссии председатель представляет выпускникам и другим присутствующим всех членов комиссии с указанием фамилии, имени и отчества, ученой степени и звания, должности.

Объявляя защиту каждой ВКР, председатель называет фамилию, имя и (обязательно) отчество выпускника, тему его научно-исследовательской работы, а также время, отводимое на доклад. Члены комиссии, задавая вопросы, также обращаются к выпускнику по имени и отчеству.

Продолжительность защиты не должна превышать 20 минут.

Схематично процедура защиты включает следующие стадии.

Доклад выпускника по теме ВКР – 10-12 минут. В докладе с использованием демонстрационных слайдов кратко излагаются актуальность, цель и задачи работы, освещаются научная и практическая значимость полученных результатов, формулируются рекомендации и выводы.

Ответы на вопросы председателя, членов комиссии и других присутствующих.

Оглашение рецензии специалиста на ВКР и справки о внедрении её результатов на предприятии, организации, фирме (если имеется).

Ответы выпускника на замечания рецензента.

Выступление научного руководителя ВКР и других лиц, присутствующих на защите, если они просят слово.

Ответы выпускника на критические замечания научного руководителя и других лиц, принявших участие в обсуждении ВКР.

После публичного заслушивания всех ВКР, представленных на защиту, проводится закрытое (для посторонних) заседание аттестационной комиссии. На закрытом заседании комиссии обсуждаются результаты прошедших защит, выносится согласованная оценка по каждой ВКР: «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно». Оценка выносится простым большинством голосов членов комиссии, участвующих в заседании (при равенстве голосов, решающим является голос председателя).

Выносится решение о выдаче диплома с отличием. Такое решение принимается на основании оценок, вносимых в приложение к диплому, включающих оценки по дисциплинам, курсовым работам, практикам и итоговой аттестации. По результатам итоговой аттестации выпускник должен иметь только оценки «отлично». При этом оценок «отлично», включая оценки по итоговой аттестации, должно быть не менее 75%, остальные оценки – «хорошо». Зачёты в процентный подсчет не входят.

Одновременно принимаются рекомендации о практическом использовании полученных в ВКР результатов.

Решения комиссии считаются правомочными, если на заседании присутствовало не менее 2/3 её состава.

По окончании закрытого заседания возобновляется публичное открытое заседание комиссии, на которое вместе с выпускниками приглашаются все желающие. Председатель кратко подводит итоги защиты, объявляет оценки по защищённым на данном заседании ВКР и другие результаты, в том числе, о присуждении (не присуждении) каждому

выпускнику искомой степени (квалификации), о выдаче дипломов с отличием и др.

Решения о работе комиссии оформляются протоколами установленной формы, в которых фиксируются заданные каждому выпускнику вопросы, даются оценки выпускным квалификационным работам.

Успешная защита ВКР означает окончание обучения в ВУЗе, при этом выпускнику присуждается степень бакалавра по соответствующему направлению.

Выпускник, получивший неудовлетворительную оценку при защите ВКР, отчисляется из Университета. При восстановлении ему назначается повторное итоговое испытание, но не ранее, чем через три месяца, и не более чем через пять лет после прохождения итоговой аттестации впервые. Повторные итоговые испытания назначаются не более двух раз.

В случае неудовлетворительной оценки, полученной на защите ВКР, государственная экзаменационная комиссия устанавливает, может ли к повторной защите представляться та же работа, но с доработкой, или должна быть разработана новая тема.

Заявление на выпускную квалификационную работу
бакалавра

Заведующему кафедрой _____
(наименование кафедры)

(ученая степень, ученое звание, Ф.И.О.)

Студента(ки) группы _____

_____ формы обучения
(очной, заочной)

(Ф.И.О. студента)

ЗАЯВЛЕНИЕ

Прошу утвердить мне следующую тему выпускной квалификационной работы:

(точное название темы)

и _____ назначить _____ руководителем

(ученая степень, ученое звание, Ф.И.О.)

« _____ » _____ 202__ г.

Подпись студента(ки)

Консультанты _____
(Ф.И.О.)

СОГЛАСОВАНО

Руководитель _____
(ученая степень, ученое звание,
Ф.И.О.) (подпись)

« _____ » _____ 20 _____ г.

УТВЕРЖДАЮ

Зав. _____ кафедрой _____
(ученая степень, ученое звание,
Ф.И.О.) (подпись)

« _____ » _____ 202__ г.

Унифицированные требования к оформлению выпускных
квалификационных работ бакалавра

| № п.п. | Объект унификации | Параметры унификации |
|--------|---|---|
| 1 | Формат листа бумаги | A4 |
| 2 | Размер шрифта | 14 пунктов |
| 3 | Название шрифта | Times New Roman |
| 4 | Междустрочный интервал | Полуторный |
| 5 | Кол-во строк на странице | 28-30 строк (1800 печатных знаков) |
| 6 | Абзац | 1,25 см (5 знаков) |
| 7 | Поля (мм) | Левое, верхнее и нижнее – 20, правое – 10. |
| 8 | Общий объем без приложений | 80-100 страниц машинописного текста |
| 9 | Объем введения | 3-5 стр. машинописного текста |
| 10 | Объем основной части | 60-80 стр. машинописного текста |
| 11 | Объем заключения | 2-3 стр. машинописного текста |
| 12 | Нумерация страниц | Сквозная, в нижней части листа, посередине. На титульном листе номер страницы не проставляется |
| 13 | Последовательность приведения структурных частей работы | Титульный лист. Задание на выполнение выпускной квалификационной работы. Содержание. Введение. Основная часть. Заключение. Глоссарий. Список использованных источников. Список сокращений. Приложения |
| 14 | Оформление структурных частей работы | Каждая структурная часть начинается с новой страницы. Наименования приводятся с абзаца с прописной (заглавной буквы). Точка в конце наименования не ставится. |
| 15 | Структура основной части | 3 главы, соразмерные по объёму |
| 16 | Наличие глоссария | Обязательно. Не менее 10 понятий |
| 17 | Состав библиографического списка | Не менее 10 библиографических описаний документальных и литературных источников |

| | | |
|----|------------------------------------|---|
| 18 | Наличие приложений | По мере необходимости |
| 19 | Оформление содержания (оглавления) | Содержание (оглавление включает в себя заголовки всех разделов, глав, параграфов, глоссария, приложений с указанием страниц начала каждой части |

Образец оформления глоссария

ГЛОССАРИЙ

| № п/п | Новое понятие | Содержание |
|-------|--|--|
| 1 | 2 | 3 |
| 1 | IP-хелпинг | индивидуальная асинхронная консультация через Интернет, во время которой студент задаёт вопросы преподавателю по определенной дисциплине, а ведущий преподаватель готовит ответ на специальном сайте МГОТУ |
| 2 | Академический абитуриент | лицо, успешно завершившее теоретическое и практическое обучение по определенной образовательной программе и приказом допущенное к итоговой аттестации |
| 3 | Бакалавр | квалификация (степень), присваиваемая выпускнику высшего учебного заведения, успешно прошедшему итоговую аттестацию и защитившему выпускную квалификационную работу |
| 4 | Выпускная квалификационная работа | завершённая научно-практическая работа академического абитуриента по определенной проблеме, систематизирующая, закрепляющая и расширяющая теоретические знания и практические навыки академического абитуриента при решении конкретной задачи, демонстрирующая умение самостоятельно решать профессиональные задачи и характеризующая итоговый уровень его квалификации, подтверждающая его готовность к профессиональной деятельности |
| 5 | Глоссарий | толковый (объясняющий) словарь понятий и терминов |
| 6 | Государственный образовательный стандарт | базовый нормативный документ федерального значения, определяющий содержание и уровень подготовки обучающихся по определенной образовательной программе |
| 7 | Диплом | свидетельство об окончании высшего или среднего специального учебного заведения и присвоении соответствующей квалификации; |

| | | |
|----|--|---|
| | | или - о присвоении ученой степени |
| 8 | Информационные ресурсы | совокупность данных, организованных для эффективного получения достоверной информации |
| 9 | Государственная итоговая аттестация | комплексная оценка уровня подготовки выпускника высшего учебного заведения на соответствие требованиям государственного образовательного стандарта |
| 10 | Нормоконтроль | процедура, которая проводится с целью поддержания единообразия в структуре и оформлении курсовых и других квалификационных работ и не касается содержания работ |
| 11 | Презентация от лат. praesento от англ. present | это выступление, доклад, защита законченного или перспективного проекта, представление на обсуждение рабочего проекта, результатов внедрения и т.п. передаю, вручаю представлять |
| 12 | Слайд-тьюторинг (телетьюторинг) | методический и дидактический материал в виде слайд-лекций (телелекций), обеспечивающий подготовку студентов к выполнению курсовых работ, сдаче экзаменов и выполнению выпускной квалификационной работы, а также других видов учебных занятий |
| 13 | Список использованных источников | список, который содержит сведения об источниках, использованных при написании научно-исследовательских работ студентов |
| 14 | Телекоммуникационная двухуровневая библиотека | организованное хранилище изданий учебной, учебно-методической, научной и справочной литературы на электронном (цифровом) носителе, предназначенное для быстрого поиска и доступа к конкретному изданию |

НОРМОКОНТРОЛЬ

выпускной квалификационной работы бакалавра

Нормоконтроль осуществляется с целью установления соответствия выполненной работы действующим методическим указаниям по выполнению и оформлению ВКР. Нормоконтроль проводится на этапе представления выпускником полностью законченной ВКР.

Данный лист нормоконтроля прикладывается к ВКР.

Тема

ВКР: _____

Студент(ка)

фамилия, имя, отчество

Факультет _____ Группа _

Анализ ВКР на соответствие требованиям методических указаний

| № п/п | Объект | Параметры | Соответствует: + Не соответствует: - |
|-------|----------------------------|--|--|
| 1 | Наименование темы работы | Соответствует утверждённой базовым вузом | |
| 2 | Размер шрифта | 14 пунктов | |
| 3 | Название шрифта | Times New Roman | |
| 4 | Междустрочный интервал | Полуторный | |
| 5 | Абзац | 1,25 см | |
| 6 | Поля (мм) | Левое, верхнее и нижнее – 20, правое – 10. | |
| 7 | Общий объём без приложений | 80-100 стр. машинописного текста | |
| 8 | Объём введения | 3-5 стр. машинописного текста | |
| 9 | Объём основной части | 60-80 стр. машинописного текста | |
| 10 | Объём заключения | 2-3 стр. машинописного текста | |
| 11 | Нумерация страниц | Сквозная, в нижней части листа, посередине. На | |

| | | | |
|----|---|--|--|
| | | титულном листе номер страницы не проставляется | |
| 12 | Последовательность приведения структурных частей работы | Титульный лист. Задание на выполнение выпускной квалификационной работы. Содержание. Введение. Основная часть. Заключение. Глоссарий. Список использованных источников. Приложения | |
| 13 | Оформление структурных частей работы | Каждая структурная часть начинается с новой страницы. Наименования приводятся с абзаца с прописной (заглавной буквы). Точка в конце наименования не ставится. | |
| 14 | Структура основной части | 3 главы, соразмерные по объёму | |
| 15 | Наличие глоссария | Обязательно. не менее 10 понятий | |
| 16 | Состав списка использованных источников | Не менее 10 библиографических описаний документальных и литературных источников | |
| 17 | Наличие приложений | По мере необходимости | |
| 18 | Оформление содержания (оглавления) | Содержание (оглавление включает в себя заголовки всех разделов, глав, параграфов, глоссария, приложений с указанием страниц начала каждой части. | |

Выпускная квалификационная работа допускается к защите после устранения выявленных несоответствий.

Нормоконтролёр

подпись

С результатами нормоконтроля ознакомлен:
выпускник

подпись

ОТЗЫВ
на выпускную квалификационную работу

студента(ки) _____

фамилия, имя, отчество

на

тему

1. Актуальность и практическая / теоретическая значимость темы _____

2. Научная новизна

3. Логическая последовательность

4. Умение пользоваться методами научного исследования

5. Аргументированность и конкретность выводов и предложений

6. Использование программных средств*

7. Умение систематизировать информационный материал

8. Широта использования литературных источников _____

* Для ВКР, позволяющих применение специализированных программных средств.

9. Самостоятельность подхода к раскрытию темы ВКР _____

10. Наличие собственной точки зрения

11. Степень обоснованности выводов и рекомендаций _____

12. Качество оформления ВКР, качество иллюстративного материала

13. Недостатки в работе

14. ВКР соответствует/не соответствует требованиям, предъявляемым к ВКР, и может/не может _____
нужное подчеркнуть
нужное подчеркнуть быть рекомендована к защите на заседании Государственной аттестационной комиссии

15. Студент (ка)

_____ фамилия, имя, отчество заслуживает присвоения ему (ей) степени бакалавра по направлению подготовки

Научный руководитель ВКР

фамилия, и., о., ученая степень, звание, место работы, должность

« _____ » _____ 202__ г.

подпись научного руководителя

Демонстрационный материал*
к выпускной квалификационной работе

Демонстрационный материал оформлен в виде:
«Раздаточного материала»/слайдов

Студент(ка) _____
фамилия, имя, отчество
форма обучения _____, факультет _____, группа

очная/заочная
1. _____ Тема

2. Научный руководитель
ВКР _____
фамилия, и.о., ученая степень, звание

3. «Раздаточный материал»/ слайды

количество слайдов

4. Перечень листов

1. _____

2. _____

3. _____

4. _____

5. _____

6. _____

Студент (ка) _____
(подпись)

Научный руководитель ВКР _____ / _____ /
(подпись) (расшифровка подписи)

* «Раздаточный материал» к ВКР оформляется выпускником и утверждается руководителем

ВКР. Представляется выпускником членам ГЭК перед защитой ВКР.

Примерный состав информации,
представляемой на демонстрационных плакатах (в «раздаточном
материале») на защите выпускной квалификационной работы

Цель и задачи выполнения выпускной квалификационной работы, в том числе изображённые в виде дерева целей.

Таблицы, диаграммы и графики, блок-схемы, характеризующие объект исследования.

Методика исследования.

Практические и/или научные результаты, полученные при выполнении выпускной квалификационной работы.

Рекомендации по внедрению в практику деятельности предприятия (организации, фирмы) результатов выпускной квалификационной работы.

Данные из справки о внедрении результатов выпускной квалификационной работы на предприятии (организации, фирме).

Примечание: общее количество демонстрационных слайдов 10-12 штук; общее количество информационных страниц, приводимых в «раздаточном материале», 8-10 страниц.

Рекомендации к докладу по защите выпускной квалификационной работы

Схема доклада по защите ВКР бакалавра

1. Обращение: Уважаемые члены Государственной аттестационной комиссии! Вашему вниманию предлагается выпускная квалификационная работа на тему...

2. В 2-3 предложениях дается характеристика актуальности темы.

3. Приводится краткий обзор научных работ по избранной проблеме (степень разработанности проблемы).

4. Цель выпускной квалификационной работы - указывается цель проделанных исследований.

5. Формулируются задачи, приводятся названия глав. При этом в формулировке должны присутствовать глаголы типа - изучить, рассмотреть, раскрыть, сформулировать, проанализировать, определить и т.п.

6. Из каждой главы используются выводы или формулировки, характеризующие результаты. Здесь можно демонстрировать плакаты (раздаточный материал). При демонстрации плакатов не следует читать текст, изображенный на них. Надо только описать изображение в одной-двух фразах. Если демонстрируются графики, то их надо назвать и констатировать тенденции, просматриваемые на графиках. При демонстрации диаграмм обратить внимание на обозначение сегментов, столбцов и т.п. Графический материал должен быть наглядным и понятным со стороны. Текст, сопровождающий диаграммы и гистограммы, должен отражать лишь конкретные выводы. Объем этой части доклада не должен превышать 2,5-3 стр. печатного текста.

7. В результате проведенного исследования были сделаны следующие выводы: (формулируются основные выводы, вынесенные в заключение).

8. Опираясь на выводы, были сделаны следующие предложения: (перечисляются предложения и рекомендации).

Примечание: Седьмая и восьмая части доклада не должны превышать в сумме 1 стр. печатного текста.

Весь доклад с хронометражем в 12-15 минут (с демонстрационным материалом) укладывается на 4-5 стр. печатного текста с междустрочным интервалом 1,0 и шрифтом (14 пунктов).

Образец справки о внедрении
результатов выпускной квалификационной работы

СПРАВКА

о внедрении рекомендаций, разработанных
в выпускной квалификационной работе Тарасова Александра Ивановича

В процессе выполнения выпускной квалификационной работы на тему:
«Совершенствование оценки инновационной деятельности на предприятии»
(на примере ОАО «Каскад») выпускник Тарасов А.И. принимал участие в
разработке _____ (перечисляются разработанные вопросы)

Полученные им результаты, включающие в себя (перечисляется то, что
конкретно сделано выпускником) _____
нашли отражение в методических разработках по планированию инноваций в
ОАО «Каскад» (либо в докладных, аналитических и прочих записках,
направленных в Совет директоров ОАО «Каскад» (другой руководящий
орган), либо использованы в расчетах эффективности инноваций в ОАО
«Каскад» и т.п.).

В настоящее время указанные методические разработки распоряжением
директора по экономике и финансам ОАО «Каскад» (№ _____ от 5 марта 201
г.) включены в инструктивные материалы, которыми должны
руководствоваться работники отдела новых технологий ОАО.

Генеральный директор
ПЕЧАТЬ

А.В.Степанов

(На крупных предприятиях (организациях, фирмах) справка может быть
также подписана начальником департамента, отдела, цеха или другого
структурного подразделения.

В таких случаях подпись специалиста заверяется руководителем отдела
кадров (канцелярии)
и соответствующей печатью)

Документы, представляемые на защиту

Зачетка

Выпускная квалификационная работа (ВКР), сброшюрованная в следующей последовательности:

- титульный лист;
- задание на выполнение выпускной квалификационной работы;
- результаты нормоконтроля ВКР;
- содержание (оглавление) ВКР;
- введение;
- основная часть;
- заключение;
- глоссарий;
- список использованных источников;
- список сокращений (если используются при написании);
- приложения (если они имеются).

К выпускной квалификационной работе прикладываются:

- отзыв на ВКР;
- рецензия на ВКР (если необходима, согласуется с научным руководителем);
- раздаточный материал (демонстрационные плакаты) / диск либо дискета с материалами компьютерной презентации;
- справка о внедрении рекомендаций ВКР (при наличии таковой).

