Троицкий Александр Витальевич

Подписано цифровой подписью: Троицкий Александр Витальевич
Дата: 2023.06.30 16:40:23 +03'00'

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

ПРИНЯТО
Решением Ученого совета ФГБОУ ВО «Технологический университет»
Протокол №__9__
«__11__» __апреля__2023 г.

УТВЕРЖДАЮ
и.о. проректора ФГБОУ ВО «Технологический университет»
А.В. Троицкий

ОСНОВНАЯ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ВЫСШЕГО ОБРАЗОВАНИЯ

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Год набора 2023

Королев
2023

Руководитель ОПОП: к.в.н., доцент Сухотерин А.И. Основная профессиональная образовательная программа высшего образования 10.03.01 Информационная безопасность, профиль: «Организация и технологии защиты информации» - Королев МО: Технологический университет, 2023.

Основная профессиональная образовательная программа высшего образования 10.03.01 Информационная безопасность, профиль: «Организация и технология защиты информации» 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 № 09 от 11.04.2023 года.

Основная профессиональная образовательная программа рассмотрена и одобрена на заседании кафедры «Информационной безопасности» протокол № 08 от 29.03.2023 года.

Основная профессиональная образовательная программа рекомендована на заседании УМС протокол № 5 от 11.04.2023 года.

Рецензия

на основную профессиональную
образовательную программу высшего образования
квалификации выпускника «Бакалавр»
по направлению подготовки 10.03.01 «Информационная безопасность»,
профиль «Организация и технология защиты информации», 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 «17» ноября 2020 года №1427 (Зарегистрировано в Минюсте России 18 февраля 2021 года № 62548) (далее ФГОС), с учетом потребностей рынка труда; Приказом Минобрнауки России от 6 апреля 2021 г. № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»; Приказом Министерства науки и высшего образования Российской Федерации, Министерства просвещения от 05.08.2020 №885/390 «О практической подготовке обучающихся» (Зарегистрировано в минюсте РФ 11.09.2020 №59778).

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 «Организация и технологии защиты информации)».

Генеральный Директор подпись И.Н. Землячев.

(печать)

Дата «апреля» «02» 2023г.

Рецензия
на образовательную программу высшего образования бакалавр по направлению подготовки 10.03.01 «Информационная безопасность», профиль «Организация и технологии защиты информации», разработанную ФГБОУ ВО «Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова»

Рецензируемая основная профессиональная образовательная программа высшего образования (далее – ОПОП ВО) представляет собой систему документов, разработанную на основе Федерального государственного образовательного стандарта высшего образования (далее – ФГОС ВО) – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденный приказом Министерства образования и науки Российской Федерации от «17» ноября 2020 г. № 1427 (Зарегистрировано в Минюсте России 18 февраля 2021 года № 62548).

Общая характеристика образовательной программы представлена на официальном сайте университета и содержит следующую информацию: уровень высшего образования, форма и срок обучения, вступительные экзамены, выпускающая кафедра (контакты); дана краткая характеристика направления и характеристика профессиональной деятельности выпускников; приведен полный перечень универсальных, общепрофессиональных и профессиональных компетенций, которыми должен обладать выпускник в результате освоения образовательной программы, а также область профессиональной деятельности и типы задач, к решению которых готов выпускник.

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, условия реализации практической и воспитательной подготовки, а также другие материалы, обеспечивающие качество подготовки обучающихся. В программу включены все виды практик, предусмотренные учебным планом и методические

материалы, обеспечивающие реализацию соответствующих образовательных технологий, в том числе и дистанционных.

Образовательная программа реализует также систему воспитательной работы, направленную на создание условий для активной жизнедеятельности обучающихся, их гражданского самоопределения, профессионального становления и индивидуально-личностной самореализации в созидательной деятельности для удовлетворения потребностей в нравственном, культурном, интеллектуальном, социальном и профессиональном развитии.

Объем ОПОП ВО (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 ВО и ее составных частей используется зачетная единица. Объем ОПОП ВО, ее составных частей выражен целым числом зачетных единиц. Общая трудоемкость программы составляет 240 зачетных единиц (1 зачетная единица равна 36 академическим часам).

В рамках ОПОП ВО выделяются обязательная часть программы бакалавриата, обеспечивающая формирование универсальных и общепрофессиональных компетенций, и часть, формируемая участниками образовательных отношений, направленная на расширение и углубление компетенций, установленных ФГОС ВО, и освоение профессиональных компетенций, сформированных на основании профессионального стандарта

06.033 «Специалист по защите информации в автоматизированных системах», 06.030 «Специалист по защите в телекоммуникационных системах и сетях», потребностей рынка труда и с учетом зарубежного опыта. Содержательная часть отражает направленность образовательной программы.

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

Рабочие программы дисциплин 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 и лабораторные занятия), но и интерактивными формами обучения.

В каждой рабочей программе обязательной части и части, формируемой участниками образовательных отношений, а также практик разработан фонд оценочных средств для проведения текущего контроля и промежуточной

аттестации. Учебно-методический комплекс, составляющий образовательную программу разработан профильными кафедрами и высококвалифицированными специалистами в соответствии с формируемыми компетенциями и полностью соответствует видам учебной и практической деятельности обучающихся.

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

Ресурсное обеспечение ОПОП ВО по направлению подготовки 10.03.01 «Информационная безопасность» соответствует всем требованиям ФГОС ВО, а указанная среда Университета в полной мере обеспечивает гармоничное развитие личности выпускника.

Нормативно-методическое обеспечение ОПОП ВО 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;
- привлечение для реализации ОПОП ВО опытного профессорско-преподавательского состава, а также представителей работодателей;
- учет требований работодателей при формировании дисциплин учебного плана;
- углубленное изучение отдельных областей знаний;
- практико-ориентированность.

Рецензируемая образовательная программа соответствует требованиям представителей профессионального сообщества.

Образовательная программа одобрена на заседании учебно-методического совета, утверждена *протоколом № 5 от 11 апреля 2023 г.* и рекомендуется к использованию для осуществления образовательной деятельности по направлению подготовки 10.03.01 «Информационная безопасность».

Председатель учебно-методического совета Н.В. Бабина

Секретарь учебно-методического совета Е.Г. Попова

1. Общие положения

Основная профессиональная образовательная программа высшего образования (далее – ОПОП ВО), реализуемая Федеральным государственным бюджетным образовательным учреждением высшего образования «Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова» (далее – Университет) по направлению подготовки 10.03.01 «Информационная безопасность», 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 - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденный приказом Министерства образования и науки Российской Федерации от «17» ноября 2020 г. № 1427 редакция с изменениями № 1456 от 26.11.2020 г. (Зарегистрировано в Минюсте России 18 февраля 2021 года № 62548) (далее- ФГОС ВО);
- Приказ Министерства науки и высшего образования РФ от 19 июля 2022 г. № 662 «О внесении изменений в федеральные государственные образовательные стандарты высшего образования» (Зарегистрировано в Минюсте России 07 октября 2022 №70414);
- Приказ Министерства науки и высшего образования РФ от 27 февраля 2023 г. № 208 «О внесении изменений в федеральные государственные образовательные стандарты высшего образования» (Зарегистрировано в Минюсте России 31 марта 2023 №72833);
- Профессиональный стандарт 06.033 «Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 г. №525н (зарегистрирован Министерством юстиций Российской Федерации 14 октября 2022 г., регистрационный №70543);
- Профессиональный стандарт 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях» утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 г. №536н (зарегистрирован Министерством юстиций Российской Федерации 18 октября 2022 г., регистрационный №70596);
- Приказом Минобрнауки России от 6 апреля 2021 г. № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования –

программам бакалавриата, программам специалитета, программам магистратуры»;

- 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 науки и высшего образования Российской Федерации, Министерства просвещения Российской Федерации от 05.08.2020 № 885/390 «О практической подготовке обучающихся» (Зарегистрировано в Минюсте России 11.09.2020 № 59778);
- Приказ Министерства труда и социальной защиты Российской Федерации от 12 апреля 2013 г № 148н «Об утверждении уровней квалификации в целях разработки проектов профессиональных стандартов»;
- 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»;
- Требованиями к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети «Интернет» и формату представления информации, утвержденными приказом Рособрнадзора от 14.08.2020 № 831;
- Иные нормативные и методические документы Министерства науки и высшего образования, Национального совета при Президенте Российской Федерации по профессиональным квалификациям, 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. Объем программы бакалавриата, реализуемый за один учебный год, составляет не более 70 з.е. вне зависимости от формы обучения.

Контактная работа включает в себя:

занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками Университета и (или) лицами,

привлекаемыми Университетом к реализации образовательной программы на иных условиях, обучающимся), и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с педагогическими работниками Университета и (или) лицами, привлекаемыми Университетом к реализации образовательной программы на иных условиях (в том числе индивидуальные консультации);

по решению Университета иные занятия, предусматривающие групповую или индивидуальную работу обучающихся с педагогическими работниками Университета и (или) лицами, привлекаемыми Университетом к реализации образовательной программы на иных условиях, определяемую организацией самостоятельно;

иные формы взаимодействия обучающихся с педагогическими работниками Университета и (или) лицами, привлекаемыми Университетом к реализации образовательной программы на иных условиях, определяемые Университетом самостоятельно, в том числе при проведении практики, промежуточной аттестации обучающихся, итоговой (государственной итоговой) аттестации обучающихся.

Объем контактной работы обучающихся с педагогическими работниками Организации при проведении учебных занятий по программе бакалавриата должен составлять в очной форме обучения - не менее 50 процентов, в очно-заочной форме обучения - не менее 25 процентов объема программы бакалавриата, отводимого на реализацию дисциплин (модулей).

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»

Области профессиональной деятельности и (или) сферы профессиональной деятельности, в которых выпускники, освоившие программу бакалавриата, могут осуществлять профессиональную деятельность:

06 Связь, информационные и коммуникационные технологии

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 рубеж, логистических фирмах, складах или терминалах различного назначения, торговых сетях, транспортно-экспедиционных компаниях.

К основным **типам задач профессиональной деятельности выпускников относятся:**

- эксплуатационный;
- проектно-технологический;
- экспериментально-исследовательский;
- организационно-управленческий.

Перечень основных объектов (или областей знания) профессиональной деятельности выпускников:

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.

В соответствии с направленностью (профилем) «Организация и технологии защиты информации»: 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.

Перечень профессиональных стандартов, соотнесенных с ФГОС

Требования к профессиональной деятельности выпускника программы бакалавриата по направлению подготовки 10.03.01 «Информационная безопасность», согласованы с представителями рынка труда в виде обобщённых трудовых функций и трудовых функций.

ОТФ	ТФ
Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации	Диагностика систем защиты информации автоматизированных систем
	Администрирование систем защиты информации автоматизированных систем
	Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций
	Мониторинг защищенности информации в автоматизированных системах
	Аудит защищенности информации в автоматизированных системах
Внедрение систем защиты информации автоматизированных систем	Установка и настройка средств защиты информации в автоматизированных системах
	Разработка организационно-распорядительных документов по защите информации в автоматизированных системах
	Анализ уязвимостей внедряемой системы защиты информации
	Внедрение организационных мер по защите информации в автоматизированных системах

Перечень основных задач профессиональной деятельности выпускников:

Область профессионально	Типы задач профессиональной	Задачи профессиональной деятельности

й деятельности (по Реестру Минтруда)	**деятельности**	
06 Связь, информационные и коммуникационные технологии	*экспериментально-исследовательский*	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;
	организационно-управленческий	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.
	эксплуатационный	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;
	проектно-технологический	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

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

Требования к планируемым результатам освоения образовательной программы, обеспечиваемым дисциплинами (модулями) и практиками обязательной части.

3.1 Универсальные компетенции выпускников и индикаторы их достижения.

Категория (группа) универсальных компетенций	**Код и наименование универсальной компетенции**	**Код и наименование индикатора достижения универсальной компетенции**

Системное и критическое мышление	УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. Описание сути проблемной ситуации УК-1.2. Выявление составляющих проблемной ситуации и связей между ними УК-1.3. Сбор и систематизация информации по проблеме УК-1.4. Оценка адекватности и достоверности информации о проблемной ситуации УК-1.5. Выбор методов критического анализа, адекватных проблемной ситуации УК-1.6. Разработка и обоснование плана действий по решению проблемной ситуации УК-1.7. Выбор способа обоснования решения (индукция, дедукция, по аналогии) проблемной ситуации
Разработка и реализация проектов	УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1. Формулирование цели, задач, значимости, ожидаемых результатов проекта УК-2.2. Определение потребности в ресурсах для реализации проекта УК-2.3. Разработка плана реализации проекта УК-2.4. Контроль реализации проекта УК-2.5. Оценка эффективности реализации проекта и разработка плана действий по его корректировке
Командная работа и лидерство	УК-3. Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	УК-3.1. Разработка целей команды в соответствии с целями проекта (организации) УК-3.2. Формирование состава команды, определение функциональных и ролевых критериев отбора участников УК-3.3. Разработка и корректировка плана работы команды УК-3.4. Выбор правил командной работы как основы межличностного взаимодействия УК-3.5. Выбор способов мотивации членов команды с учетом организационных возможностей и личностных особенностей членов команды, в т.ч. лиц с ограниченными возможностями здоровья УК-3.6. Выбор стиля управления работой команды в соответствии с ситуацией УК-3.7. Презентация результатов собственной и командной деятельности УК-3.8. Оценка эффективности работы команды по достигнутому результату
Коммуникация	УК-4. Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	УК-4.1. Поиск источников информации на русском и иностранном языках УК-4.2. Использование информационно-коммуникационных технологий для поиска, обработки и представления информации УК-4.3. Составление и корректный перевод академических и профессиональных текстов с иностранного языка на государственный язык РФ и с государственного языка РФ на иностранный УК-4.4. Выбор психологических способов оказания влияния и противодействия влиянию в процессе академического и профессионального взаимодействия

		УК-4.5. Представление результатов академической и профессиональной деятельности на публичных мероприятиях УК-4.6. Ведение академической и профессиональной дискуссии на государственном языке РФ и/или иностранном языке УК-4.7. Выбор стиля делового общения применительно к ситуации взаимодействия, ведение деловой переписки
Межкультурное взаимодействие	УК-5. Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах	УК-5.1. Определение целей и задач межкультурного профессионального взаимодействия в условиях различных этнических, религиозных ценностных систем, выявление возможных проблемных ситуаций УК-5.2. Выбор способов интеграции работников, принадлежащих к разным культурам, в производственную команду УК-5.3. Выбор способа преодоления коммуникативных, образовательных, этнических, конфессиональных барьеров для межкультурного взаимодействия при решении профессиональных задач УК-5.4. Выбор способа поведения в поликультурном коллективе при конфликтной ситуации
Самоорганизация и саморазвитие (в том числе здоровье-сбережение)	УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни	УК-6.1. Определение уровня самооценки и уровня притязаний как основы для выбора приоритетов собственной деятельности УК-6.2. Определение приоритетов собственной деятельности, личностного развития и профессионального роста УК-6.3. Выбор технологий целеполагания и целедостижения для постановки целей личностного развития и профессионального роста УК-6.4. Оценка собственных (личностных, ситуативных, временных) ресурсов, выбор способов преодоления личностных ограничений на пути достижения целей УК-6.5. Оценка требований рынка труда и образовательных услуг для выстраивания траектории собственного профессионального роста УК-6.6. Оценка собственного ресурсного состояния, выбор средств коррекции ресурсного состояния УК-6.7. Оценка индивидуального личностного потенциала, выбор техник самоорганизации и самоконтроля для реализации собственной деятельности
	УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	УК-7.1. Выбирает здоровье - сберегающие технологии для поддержания здорового образа жизни с учетом физиологических особенностей организма УК-7.2. Планирует свое рабочее и свободное время для оптимального сочетания физической и умственной нагрузки и обеспечения работоспособности УК-7.3. Соблюдает и пропагандирует нормы здорового образа жизни в различных жизненных ситуациях и в профессиональной деятельности

Безопасность жизнедеятельности	УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении черезвычайных ситуаций и военных конфликтов	УК-8.1. Анализирует факторы вредного влияния на жизнедеятельность элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений); УК-8.2. Идентифицирует опасные и вредные факторы в рамках осуществляемой деятельности; УК-8.3. Выявляет проблемы, связанные с нарушениями техники безопасности на рабочем месте; предлагает мероприятиях по предотвращению чрезвычайных ситуаций; УК-8.4. Разъясняет правила поведения при возникновении чрезвычайных ситуаций природного и техногенного происхождения; оказывает первую помощь, описывает способы участия в восстановительных мероприятиях.
Экономическая культура, в том числе финансовая грамотность	УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-9.1. Понимает базовые принципы функционирования экономики и экономического развития, цели формы участия государства в экономике; УК-9.2. Применяет методы личного экономического и финансового планирования для достижения текущих и долгосрочных финансовых целей, использует финансовые инструменты для управления личными финансами (личным бюджетом), контролирует собственные экономические и финансовые риски УК-9.3. Умеет разрабатывать основные показатели технико-экономического обоснования соответствующих проектных решений; УК-9.4. Умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите.
Гражданская позиция	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	УК-10.1 Анализирует действующие правовые нормы, обеспечивающие борьбу с экстремизмом, терроризмом и коррупцией в различных областях жизнедеятельности, а также способы профилактики коррупции и формирования нетерпимого отношения к ней УК-10.2. Планирует, организует и проводит мероприятия, обеспечивающие формирование гражданской позиции и предотвращение экстремизма, терроризма и коррупции в обществе УК-10.3 Соблюдает правила общественного взаимодействия на основе нетерпимого отношения к экстремизму, терроризму и коррупции

3.2 Общепрофессиональные компетенции выпускников и индикаторы их достижения.

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ОПК-1. Способен оценивать роль информации, информационных	ОПК-1.1.1 знает понятия информации и информационной безопасности;

технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1.2 знает место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики; ОПК-1.1.3 знает источники и классификацию угроз информационной безопасности; ОПК-1.2.1 умеет классифицировать и оценивать угрозы информационной безопасности. ОПК-1.1.4 знает основные понятия, связанные с обеспечением информационно-психологической безопасности личности, общества и государства, понятия информационного противоборства, информационной войны и формы их проявлений в современном мире;
ОПК-2. Способен применять информационно – коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.1.1 знает классификацию современных компьютерных систем и программного обеспечения, типовые структуры и принципы организации компьютерных сетей; назначение, функции и обобщённую структуру операционных систем; назначение и основные компоненты систем баз данных; ОПК-2.2.1 умеет применять типовые программные средства сервисного назначения и пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети интернет; ОПК-2.2.2 умеет составлять SQL запросы и осуществлять удалённый доступ к базам данных; ОПК-2.3.1 владеет навыками поиска информации в глобальной информационной сети Интернет; ОПК-2.3.2 владеет навыками подготовки документов в среде типовых офисных пакетов; ОПК-2.1.2 знает классификацию современных компьютерных систем и архитектуру их основных типов; ОПК-2.1.3 знает состав, назначение функциональных компонентов и программного обеспечения персонального компьютера; ОПК-2.1.4 знает структуру и принципы работы современных и перспективных микропроцессоров ОПК-2.2.2 умеет определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств; ОПК-2.3.3 владеет навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности;

ОПК-3. Способен использовать совокупность необходимых математических методов для решения задач профессиональной деятельности	ОПК-3.1.1 знает основные понятия теории пределов и непрерывности функций одной и нескольких действительных переменных; ОПК-3.1.2 знает основные методы дифференциального исчисления функций одной и нескольких действительных переменных; ОПК-3.1.3 знает основные методы интегрального исчисления функций одной и нескольких действительных переменных; ОПК-3.1.4 знает основные методы исследования числовых и функциональных рядов; ОПК-3.1.5 знает основные задачи теории функций комплексного переменного; ОПК-3.1.6 знает основные типы обыкновенных дифференциальных уравнений и методы их решения; ОПК-3.2.1 умеет исследовать функциональные зависимости, возникающие при решении стандартных прикладных задач; ОПК-3.2.2 умеет использовать типовые модели и методы математического анализа при решении стандартных прикладных задач; ОПК-3.3.1 владеет навыками типовых расчетов с использованием основных формул дифференциального и интегрального исчисления; ОПК-3.3.2 владеет навыками использования справочных материалов по математическому анализу. ОПК-3.1.7 знает основные понятия теории вероятностей, числовые и функциональные характеристики распределений случайных величин и их основные свойства; ОПК-3.1.8 знает классические предельные теоремы теории вероятностей; ОПК-3.1.9 знает основные понятия теории случайных процессов; ОПК-3.1.10 знает постановку задач и основные понятия математической статистики; ОПК-3.1.11 знает стандартные методы получения точечных и интервальных оценок параметров вероятностных распределений; ОПК-3.1.12 знает стандартные методы проверки статистических гипотез; ОПК-3.2.3 умеет применять стандартные вероятностные и статистические модели к решению типовых прикладных задач; ОПК-3.3.3 владеет навыками использования расчетных формул и таблиц при решении стандартных вероятностно-статистических задач; ОПК-3.1.13 знает возможности координатного метода для исследования различных

	геометрических объектов, ОПК-3.1.14 знает основные задачи векторной алгебры и аналитической геометрии; ОПК-3.1.15 знает основные виды уравнений простейших геометрических объектов; ОПК-3.1.16 знает основы линейной алгебры над произвольными полями и свойства векторных пространств; ОПК-3.2.4 умеет исследовать простейшие геометрические объекты по их уравнениям в различных системах координат ОПК-3.2.5 умеет оперировать с числовыми и конечными полями, многочленами, матрицами ОПК-3.2.6 умеет решать основные задачи линейной алгебры, в частности системы линейных уравнений над полями ОПК-3.3.4 владеет навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике ОПК-3.3.5 владеет стандартными методами линейной алгебры ОПК-3.1.17 знает основные понятия и методы математической логики и теории алгоритмов ОПК-3.1.18 знает основные понятия, составляющие предмет дискретной математики ОПК-3.1.19 знает основные методы решения задач профессиональной области с применением дискретных моделей ОПК-3.2.7 умеет строить математические модели задач профессиональной области ОПК-3.2.8 умеет применять стандартные методы дискретной математики к решению типовых задач ОПК-3.3.6 владеет навыками самостоятельного решения комбинаторных задач ОПК-3.3.7 владеет навыками нахождения различных параметров и представлений булевых функций ОПК-3.3.8 владеет навыками вычисления параметров графов ОПК-3.1.20 знает основные понятия теории информации (энтропия, взаимная информация, источники сообщений, каналы связи, коды) ОПК-3.1.21 знает понятие пропускной способности канала связи, прямую и обратную теоремы кодирования (без доказательства) ОПК-3.1.22 знает основные методы оптимального кодирования источников информации (код Хаффмана) и помехоустойчивого кодирования каналов связи (линейные коды, циклические коды, код Хэмминга)

	ОПК-3.2.9 умеет вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность) ОПК-3.2.10 умеет решать типовые задачи кодирования и декодирования
ОПК-4. Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности;	ОПК-4.1.1 знает основополагающие принципы механики; ОПК-4.1.2 знает основополагающие принципы термодинамики и молекулярной физики; ОПК-4.1.3 знает основные положения электричества и магнетизма; ОПК-4.1.4 знает основные положения колебаний и оптики; знает основные положения теории колебаний и волн, оптики; ОПК-4.1.5 знает основополагающие принципы квантовой физики; ОПК-4.2.1 умеет решать базовые прикладные физические задачи; ОПК-4.2.2 умеет делать выводы и формулировать их в виде отчета о проделанной исследовательской работе; ОПК-4.1.6 знает основополагающие принципы работы элементов и функциональных узлов электронной аппаратуры средств защиты информации; ОПК-4.1.7 знает основные законы электротехники, элементы электрических цепей; ОПК-4.1.8 знает дифференциальные уравнения простых электрических цепей ОПК-4.1.9 знает методы анализа и расчета линейных и нелинейных электрических цепей постоянного и переменного тока, переходных процессов и установившихся режимах в частотной и временной областях; ОПК-4.2.3 умеет измерять параметры электрической цепи; ОПК-4.2.4 умеет анализировать процессы, протекающие в линейных и нелинейных электрических цепях; ОПК-4.3.1 владеет методами расчета простых линейных и нелинейных электрических цепей
ОПК-5.Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	ОПК-5.1.1 знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; ОПК-5.1.2 знает основные понятия и характеристику основных отраслей права, применяемых в профессиональной деятельности организации; ОПК-5.1.3 знает основы законодательства

	Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации; ОПК-5.1.4 знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности; ОПК-5.2.1 умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав; ОПК-5.2.2 умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; ОПК-5.2.3 умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; ОПК-5.2.4 умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации;
ОПК-6. Способен при решении задач профессиональной деятельности организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.1.1 знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; ОПК-6.1.2 знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях; ОПК-6.1.3 знает систему организационных мер, направленных на защиту информации ограниченного доступа ОПК-6.1.4 знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа ОПК-6.1.5 знает основные угрозы

	безопасности информации и модели нарушителя объекта информатизации ОПК-6.2.1 умеет разрабатывать модели угроз и модели нарушителя объекта информатизации ОПК-6.2.2 умеет разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации ОПК-6.2.3 умеет определить политику контроля доступа работников к информации ограниченного доступа ОПК-6.2.4 умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации
ОПК-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности;	ОПК-7.1.1 знает основные принципы построения компьютера, формы и способы представления данных в персональном компьютере ОПК-7.1.2 знает области и особенности применения языков программирования высокого уровня ОПК-7.1.3 знает язык программирования высокого уровня (структурное, объектно-ориентированное программирование) ОПК-7.2.1 умеет работать с интегрированной средой разработки программного обеспечения ОПК-7.2.2 умеет разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач ОПК-7.2.3 умеет разрабатывать программы для работы с файлами как с источником данных ОПК-7.3.1 владеет навыками разработки, документирования, тестирования и отладки программ ОПК-7.1.4 знает базовые структуры данных ОПК-7.1.5 знает основные алгоритмы сортировки и поиска данных ОПК-7.1.6 знает основные комбинаторные и теоретико-графовые алгоритмы ОПК-7.1.7 знает общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения ОПК-7.2.4 умеет применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач; ОПК-7.3.2 владеет навыками разработки алгоритмов решения типовых профессиональных задач;

ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	ОПК-8.1.1 знает принципы и порядок работы информационно-справочных систем ОПК-8.1.2 знает способы поиска и обработки информации, методы работы с научной информацией, принципы и правила построения суждений и оценок ОПК-8.2.1 умеет обобщать, анализировать и систематизировать научную информацию в области информационной безопасности ОПК-8.2.2 умеет различать факты, интерпретации, оценки и аргументированно отстаивать свою позицию в процессе коммуникации ОПК-8.2.3 умеет пользоваться информационно-справочными системами ОПК-8.3.1 владеет навыком составления и оформления реферата по результатам обзора научно-технической литературы, нормативных и методических документов
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ОПК-9.1.1 знает принципы построения систем и сетей электросвязи; ОПК-9.1.2 знает современные виды информационного взаимодействия и обслуживания телекоммуникационных сетей и систем; ОПК-9.2.1 умеет проводить анализ показателей эффективности сетей и систем телекоммуникаций и качества предоставляемых услуг; ОПК-9.1.3 знает основные понятия и задачи криптографии, математические модели криптографических систем ОПК-9.1.4 знает основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и криптографические протоколы ОПК-9.1.5 знает национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения ОПК-9.2.2 умеет применять математические модели для оценки стойкости СКЗИ ОПК-9.2.3 умеет использовать СКЗИ в автоматизированных системах ОПК-9.1.6 знает классификацию и количественные характеристики технических каналов утечки информации; ОПК-9.1.7 знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;

	ОПК-9.1.8 знает организацию защиты информации от утечки по техническим каналам на объектах информатизации; ОПК-9.2.9 умеет пользоваться нормативными документами в области технической защиты информации; ОПК-9.2.4 умеет анализировать и оценивать угрозы информационной безопасности объекта информатизации; ОПК-9.3.1 владеет методами и средствами технической защиты информации.
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;	ОПК-10.1.1 знает программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях ОПК-10.2.1 умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности ОПК-10.1.2 знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности ОПК-10.1.3 знает принципы формирования политики информационной безопасности организации
ОПК-11. Способен проводить эксперименты по заданной методике и обработку их результатов;	ОПК-11.1.1 знает теоретические основы теории погрешностей; ОПК-11.2.1 умеет проводить физический эксперимент, обрабатывать его результаты ОПК-11.2.2 умеет использовать стандартные вероятностно-статистические методы анализа экспериментальных данных; ОПК-11.2.3 умеет строить стандартные процедуры принятия решений на основе имеющихся экспериментальных данных;
ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем и средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.1.1 знает принципы формирования политики информационной безопасности в информационных системах; ОПК-12.1.2 знает принципы организации информационных систем в соответствии с требованиями по защите информации; ОПК-12.1.3 знает требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации; ОПК-12.1.4 знает основные этапы процесса проектирования и общие требования к содержанию проекта; ОПК-12.2.1 умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; ОПК-12.2.2 умеет анализировать показатели

	качества и критерии оценки систем и отдельных методов и средств защиты информации; ОПК-12.2.3 умеет формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения; ОПК-12.2.4 умеет оценивать информационные риски в автоматизированных системах; ОПК-12.2.5 умеет разрабатывать основные показатели технико-экономического обоснования соответствующих проектных решений;
ОПК-13. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире, в том числе для формирования гражданской позиции и развития патриотизма.	ОПК-13.1.1 знает основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире; ОПК-13.1.2 знает ключевые события истории России и мира, выдающихся деятелей России; ОПК-13.2.1 умеет соотносить общие исторические процессы и отдельные факты, выявлять существенные черты исторических процессов, явлений и событий; ОПК-13.2.2 умеет формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории;

В соответствии с профилем №2 «Организация и технологии защиты информации» обучающиеся осваивают следующие общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ДОПК-2.1. Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	ДОПК-2.1.1.1знает технологии обеспечения информационной безопасности, способы их организации и оптимизации ДОПК-2.1.1.2знает технологии проектирования и построения информационных систем ДОПК-2.1.2.1умеет классифицировать информационные системы по назначению, структуре, типу ДОПК-2.1.3.1владеет навыками выявления и устранения угроз информационной безопасности ДОПК-2.1.1.3знает стратегии обеспечения информационной безопасности, способы их организации и оптимизации ДОПК-2.1.1.4знает определения рисков информационной безопасности применительно к объекту информатизации с заданными характеристиками ДОПК-2.1.1.5знает методы и подходы к реализации системы управления безопасностью автоматизированных информационных систем

	ДОПК-2.1.2.2умеет обосновывать решения по обеспечению информационной безопасности объектов в профессиональной сфере деятельности ДОПК-2.1.3.2владеет навыками реализации политики информационной безопасности ДОПК-2.1.1.6знает методы анализа процессов для определения актуальных угроз ДОПК-2.1.1.7знает особенности работы решений по защите информации в информационных процессах и системах ДОПК-2.1.2.3умеет представлять процессы в формализованном виде на языках моделирования ДОПК-2.1.3.3владеет навыками применения современных программно-аппаратных средств моделирования информационных процессов и систем ЗИ ДОПК-2.1.3.4владеет навыками оценки адекватности моделей и анализа результатов моделирования ДОПК-2.1.1.8знает принципы обеспечения информационной безопасности объекта информатизации ДОПК-2.1.1.9знает методы хранения, обработки и передачи и получения информации из открытых информационных систем ДОПК-2.1.2.4умеет делать выводы по результатам проведённого анализа, выявляя потенциальные угрозы ИБ ДОПК-2.1.3.5владеет навыками применения автоматизированных средств сбора и анализа информации, основанных на технологиях OSINT и data mining ДОПК-2.1.3.6владеет навыками анализа надежности защиты информационных систем ДОПК-2.1.1.10 знает основные категории требований к программным и программно-аппаратным средствам защиты информации ДОПК-2.1.1.11 знает требования по защите автоматизированных систем от НСД ДОПК-2.1.2.5умеет делать обоснованный выбор существующих средств защиты информации для нейтрализации определенного вида угроз ДОПК-2.1.2.7владеет навыками выбора и применения современных аппаратных и программных средств технической защиты информации ДОПК-2.1.3.8владеет навыками эффективного использования средств автоматического контроля и обнаружения возможных каналов утечки сведений, представляющих государственную, военную, служебную и коммерческую тайну

	ДОПК-2.1.1.12 знает основы администрирования вычислительных сетей ДОПК-2.1.1.13 знает основы организации систем управления БД ДОПК-2.1.1.14 знает принципы организации операционных систем в защищённом исполнении ДОПК-2.1.2.6умеет настраивать политики безопасности наиболее распространенных операционных систем ДОПК-2.1.2.7умеет выявлять и устранять сбои в работе ос, систем электронного документооборота и основных СУБД ДОПК-2.1.3.8владеет навыками установки и администрирования основных операционных систем и систем электронного документооборота
ДОПК-2.2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;	ДОПК-2.2.1.1 знает подходы к построению подсистем фиксации и реагирования на инциденты информационной безопасности ДОПК-2.2.1.2 знает принципы разработки организационных и технических мер по сбору, анализу и мониторингу событий безопасности ДОПК-2.2.2.1 умеет анализировать эффективность применения мер по обеспечению ЗИ и разрабатывать предложения по совершенствованию структуры мер и повышению эффективности. ДОПК-2.2.2.2 умеет реагировать на инциденты информационной безопасности ДОПК-2.2.3.1 владеет навыками классификации информационных систем и средств вычислительной техники по требованиям регуляторов ИБ ДОПК-2.2.1.3 знает как проводится анализ журналов событий средств защиты информации ДОПК-2.2.1.4 знает основные этапы расследования компьютерных преступлений в соответствии с нормативными требованиями ДОПК-2.2.2.3 умеет сопоставлять основные структурно-функциональные характеристики информационных систем с требованиями руководящих документов ДОПК-2.2.3.2 владеет навыками сравнения и анализа существующих средств защиты информации ДОПК-2.2.3.3 владеет навыками нахождения наиболее подходящего решения применительно к заданным характеристикам информационной системы ДОПК-2.2.1.5 знает руководящие документы в области классификации современных информационных систем и средств вычислительной и техники

	ДОПК-2.2.1.6 знает основы нормативно-правовых актов в области защиты информации конфиденциального характера ДОПК-2.2.1.7 знает как формируется организационно-распорядительная и эксплуатационная документация по обеспечению безопасности информационных систем ДОПК-2.2.2.4 умеет классифицировать информацию и автоматизированные системы, определять основные требования к ее защите ДОПК-2.2.3.4владеет навыками работы с нормативно-правовыми актами, навыками ориентации в них и поиска необходимой информации
ДОПК-2.3. Способен разработать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;	ДОПК-2.3.1.1знает государственные нормативные документы в области организации проведения и сопровождения аттестации объекта информатизации ДОПК-2.3.1.2знает отечественные и зарубежные стандарты в области информационной безопасности ДОПК-2.3.1.3знает как разрабатывать технические задания на создание подсистем информационной безопасности открытых информационных систем ДОПК-2.3.2.1умеет организовывать проведение и сопровождать аттестацию объекта информатизации в соответствии с требованиями нормативных документов ДОПК-2.3.3.1владеет навыками внедрения и контроля исполнения требования локальных нормативных документов по обеспечению ИБ ДОПК-2.3.1.4знает правовые нормы, инструкции и стандарты в области организации документооборота ДОПК-2.3.1.5знает правовые основы организации защиты государственной тайны и конфиденциальной информации ДОПК-2.3.2.2умеет разрабатывать инструкции по организации защищённого документооборота и контролировать их исполнение ДОПК-2.3.3.2владеет навыками установки, настройки и использования современных систем электронного документооборота в защищённом исполнении ДОПК-2.3.1.6знает как разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации ДОПК-2.3.1.7знает актуальные нормативно-правовые акты и методические документы в области обеспечения информационной безопасности персональных данных

	ДОПК-2.3.1.8знает правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны в соответствии с доктриной ИБ РФ ДОПК-2.3.2.3умеет формировать требования к системам защиты информации в информационных системах персональных данных с учетом специфики их эксплуатации в различных сферах жизнедеятельности ДОПК-2.3.3.3владеет навыками проведения лицензирования в области защиты информации ДОПК-2.3.3.4владеет навыками работы с нормативно-правовыми актами
ДОПК-2.4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами	ДОПК-2.4.1.1 знает стандарты и критерии в области аудита ИБ ДОПК-2.4.1.2 знает требования законодательства по обеспечению безопасности персональных данных ДОПК-2.4.1.3 знает как составляются политики информационной безопасности в информационной системе персональных данных ДОПК-2.4.2.1 умеет определять объекты аудита, критерии и область их действия ДОПК-2.4.3.1 владеет навыками составления отчётов по результатам выполненного аудита ДОПК-2.4.1.4 знает принципы организации процесса аудита ДОПК-2.4.1.5 знает теоретическую базу разработки политик безопасности ДОПК-2.4.2.2 умеет применять инструментальные средства мониторинга и аудита безопасности ДОПК-2.4.2.3 умеет составлять программу аудита ИБ ДОПК-2.4.3.2 владеет навыками проведения аудита ИБ со сбором данных ДОПК-2.4.1.6 знает теоретическую базу и средства для проведения мониторинга защищенности информационной системы ДОПК-2.4.1.7 знает принципы администрирования подсистем информационной безопасности ДОПК-2.4.2.4 умеет разрабатывать методики анализа рисков ДОПК-2.4.2.5 умеет собирать и анализировать свидетельства аудита ДОПК-2.4.3.3 владеет навыками по формулированию выводов и заключения по полученным результатам ДОПК-2.4.1.8 знает порядок аттестации

	объектов информатизации ДОПК-2.4.1.9 знает порядок проведения сертификационных испытаний средств защиты информации ДОПК-2.4.2.6 умеет формализовать задачи анализа безопасности информационных систем ДОПК-2.4.3.4владеет навыками выбора и обоснования критериев оценки защищенности открытых информационных систем

3.3 Профессиональные компетенции выпускников и индикаторы их достижения.

В качестве профессиональных компетенций в программу магитсратуры включены определенные самостоятельно профессиональные компетенции, формируемые на основе анализа требований к профессиональным компетенциям, предъявляемых к выпускникам на рынке труда, обобщения отечественного и зарубежного опыта, проведения консультаций с ведущими работодателями, объединениями работодателей отрасли, в которой востребованы выпускники

Задача ПД	**Код и наименование профессиональной компетенции**	**Код и наименование индикатора достижения профессиональной компетенции**	**Основание (ПС, анализ опыта)**
экспериментально-исследовательский	ПК-1. Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности	ПК-1.1.1 Нормативно-правовые акты и стандарты в области ИБ и принципы проведения диагностики системы ЗИ; ПК-1.2.2 Выявлять и оценивать источники и последствия инцидентов ИБ (ЗИ); ПК-1.3.3. Выполнять обнаружение, идентификацию и устранение инцидентов ИБ (ЗИ);	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях»
экспериментально-исследовательский	ПК-2. Способность принимать участие в проведении экспериментальных исследований системы защиты	ПК-2.1.1 Руководящие и методические документы принципы организации по проведению	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» Профессиональный

	информации	экспериментальной деятельности в области ЗИ; ПК-2.2.2 Применять действующую нормативную базу выбирать целесообразные потребные средства и определять структуру системы ЗИ в ходе проведения экспериментов; ПК-2.3.3 Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;	стандарт «Специалист по защите информации в телекоммуникационных системах и сетях»
организационно-управленческий	ПК-3. Способность осуществлять управление с разработкой организационно-распорядительных документов и реализацию организационных мер по ЗИ в АС	ПК-3.1.1 Основные нормативно-правовые акты, методы управления деятельностью, угрозы ИБ и нарушители систем безопасности информации; ПК-3.2.2 Оценивать информационные риски разрабатывать предложения по совершенствованию СУ (ИБ) и применять средства контроля эффективности ЗИ; ПК-3.3.3 Анализировать воздействие на защищаемую систему информации, оценивать последствия и вырабатывать предложения по ее совершенствованию;	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях»
эксплуатационный	ПК-4. Способность осуществлять диагностику и оценку обеспечения	ПК-4.1.1 Знать нормативно-методические, руководящие и методические	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах»

	работоспособности системы ЗИ при возникновении внештатных ситуаций	документы, организационные меры, критерии оценки защищенности и регламенты обеспечения работоспособности систем ЗИ; ПК-4.2.2 Определять и оценивать источники, причины и последствия возникающих инцидентов выявлять и устранять нарушения в области ИБ (ЗИ); ПК-4.3.3 Принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;	Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях»
проектно-технологическай	ПК-5. Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений	ПК-5.1.1 Документационное обеспечение по разработке проектных решений по ЗИ, принципы и особенности организации проектно-технологической деятельности; ПК-5.2.2 Участвовать в разработке проектных документов на создание подсистемы ИБ с разработкой модели проектируемых систем ЗИ и осуществлять технико-экономическое обоснование; ПК-5.3.3 Анализировать защищенность информационной инфраструктуры с	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах»

		формированием системы требований по ЗИ и участвовать в обосновании критериев эффективности функционирования проектируемых систем ИБ (ЗИ)	

Приобретенные компетенции способствуют формированию профессиональных качеств квалифицированного специалиста, отвечающего требованиям профессиональных стандартов и 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 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)

Обязательная часть

Б1.О.01 «Философия»

Дисциплина «Философия» относится к обязательной 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: отдельных разделах «История России», «Основы права» и компетенциях: УК-1, УК-5, ПК-1.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;

ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;

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 4 зачетные единицы, 144 часа. Преподавание дисциплины ведется на 1 курсе во 2 семестре для очной и в 4 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 экзамена в 2 семестре для очной и в 4 семестре очно-заочной формы обучения.

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

Б1.О.02 «История России»

Дисциплина «История России» относится к обязательной 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: «Основы российской государственности» и компетенциях УК-5.

Дисциплина направлена на формирование следующих компетенций:
УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач
УК-5. Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах;

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 4 зачетных единицы, 144 часов. Преподавание дисциплины ведется на 1 и 2 курсе во 2 и 3 семестре для очной и на 1 и 2 курсе во 2 и 3 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, зачета с оценкой во 2 семестре для очной и очно-зачетной формы обучения и экзамена в 3 семестре для очной и очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: отдельные разделы дисциплины «Философия», «Организация системы обеспечения информационной безопасности (служба ИБ)», «История защиты информации в РФ», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.03 Основы российской государственности

Дисциплина «Основы российской государственности» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений, основной образовательной программы подготовки бакалавров по направлению подготовки 10.03.01 «Информационная безопасность».

Дисциплина базируется на уроках обществознания в среднеобразовательных учебных заведениях, и опирается на коммуникативные компетенции, приобретённые в средней общеобразовательной школе.

В процессе обучения студент приобретает и совершенствует следующие компетенции:

УК-5. Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах;

Содержание дисциплины охватывает круг вопросов, связанных с изучением исторических, географических, институциональных оснований формирования российской цивилизации, помогает обучающимся расставить мировоззренческие акценты, сформировать чувство гражданственности и принадлежности к российскому обществу. Также содержательная часть данного курса способствует созданию духовно-нравственного и культурного фундамента развитой и цельной личности, осознающей особенности исторического пути российского государства и самобытность его политической организации.

Общая трудоемкость дисциплины для студентов очной формы обучения составляет 2 зачетных единицы, 72 часа.

Преподавание дисциплины ведется на 1 курсе во 1 семестре при очной форме обучения и на втором курсе во 2 семестре для очно-заочной формы обучения, 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 и промежуточная аттестация в форме контрольной работы и зачета в 1 семестре при очной и во 2 семестре очно-заочной форме обучения.

Основные положения и знания, полученные при освоении дисциплины должны быть использованы при изучении последующих дисциплин: «Основы управленческой деятельности», «Основы права», «Введение в профессию» и выполнении выпускной квалификационной работы бакалавра.

Б1.О.04 «Иностранный язык» (английский, французский, немецкий языки)

Дисциплина «Иностранный язык» относится к обязательной 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:

УК-4. Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном (ых) языке(ах);
ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач 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 и 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 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 и очно-заочной формы обучения.

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

Б1.О.05 «Безопасность жизнедеятельности»

Дисциплина «Безопасность жизнедеятельности» относится к обязательной 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:

УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности;
УК-8. Способен создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций;

Целью изучения дисциплины является: 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 во 1 семестре для очной и во 2 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 во 1 семестре для очной и во 2 семестре для очно-заочной формы обучения.

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

Б1.О.6 «Физическая культура»

Дисциплина «Физическая культура» относится к обязательной 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:

УК-7. Способен поддерживать должный уровень физической подготовленности 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 в 2 семестре очно-заочной 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 зачета во 2 семестре для очной и очно-заочной 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.

Б1.О.07 «Русский язык и культура речи»

Дисциплина «Русский язык и культура речи» относится к обязательной 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:

УК-4. Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном (ых) языке(ах);

УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия;
ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач 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 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 1 семестре для очной формы обучения и в форме контрольной работы и зачета в 1 семестре для очно-заочной формы обучения.

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

Б1.О.8 «Основы управленческой деятельности»

Дисциплина «Основы управленческой деятельности» относится к обязательной 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:

УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни;
УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности;
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства
ОПК-5.Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере 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 часа. Преподавание дисциплины ведется на 1 курсе в 1 семестре для очной и на 1 курсе во 2 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 1 семестре для очной и во 2 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «История (история России, всеобщая история)», «Основы управления информационной безопасностью», «Информационно-аналитическая деятельность по

обеспечению комплексной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.9 «Документоведение»

Дисциплина «Документоведение» относится к обязательной 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:

ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;

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 в 1 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 в 1 семестре для очной формы обучения и в 1 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация системы обеспечения информационной безопасности (служба ИБ)», «Конфиденциальное делопроизводство и защищенный электронный документооборот», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.10 «Экономика предприятия и организация производства»

Дисциплина «Экономика предприятия и организация производств» относится к обязательной 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:

УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности;
ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем и средств обеспечения защиты информации и для 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 2 курсе в 3 семестре для очной формы обучения и в 1 семестре и 2 семестре и на 2 курсе в 3 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 во 2 семестре и в форме контрольной работы и контрольной работы и экзамена в 3 семестре для очной и очно-заочной формы обучения.

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

Блок Б1.О.11 Группа учебных дисциплин (модулей) «Математические основы обеспечения информационной безопасности»

Б1.О.11.01 «Линейная алгебра и аналитическая геометрия»

Дисциплина «Линейная алгебра и аналитическая геометрия» относится к обязательной 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:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;

ОПК-3. Способен использовать совокупность необходимых математических методов для решения задач профессиональной деятельности;

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 единиц, 108 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 и в 1-ом семестре очно-заочной формы обучения.

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

Б1.О.11.02 «Математический анализ»

Дисциплина «Математический анализ» относится к обязательной 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:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-3. Способен использовать совокупность необходимых математических методов для решения задач профессиональной деятельности;

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 и во 2-ом семестре очно-заочной формы обучения.

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

Б1.О.11.03 «Теория графов»

Дисциплина «Теория графов» относится к обязательной 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:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-3. Способен использовать совокупность необходимых математических методов для решения задач профессиональной деятельности;

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 для очной и на 2-ом курсе в 4 семестре, продолжительностью 16 недель для очно-заочной 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 и в форме контрольной работы и экзамена в 4 семестре для очно-заочной формы обучения.

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

Б1.О.11.04 «Теория информации»

Дисциплина «Теория информации» относится к обязательной 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», отдельные разделы «Экономика предприятия и организация производства», «Документоведение»,«Математический анализ» и компетенциях: УК-3,7,8,9, ОПК-2,3,8,10,12,13.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-3. Способен использовать совокупность необходимых математических методов для решения задач профессиональной деятельности;

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 Шенона-Фэно, Хаффмана, блочные помехозащищенные коды, совершенные и квазисовершенные помехозащищенные коды; вопросы шифрования с симметричным и несимметричным ключом.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 2 курсе в 3 семестре для очной формы обучения и в 3 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 3 семестре для очной формы обучения и в форме контрольной работы и зачета с оценкой в 3 семестре для очно-заочной формы обучения.

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

Б1.О.11.05 «Теория вероятностей и математическая статистика»

Дисциплина «Теория вероятностей и математическая статистика» относится к обязательной 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-2,3,7,9.

Дисциплина направлена на формирование следующих компетенций:

ОПК-3. Способен использовать совокупность необходимых математических методов для решения задач профессиональной деятельности;
ОПК-11. Способен проводить эксперименты по заданной методике и обработку их результатов;

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, конт 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 на 2-3 курсах в 4-5 семестрах 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 в 3 семестре и в форме контрольной работы и экзамена в 4 семестре для очной формы обучения и в форме контрольной работы и зачета в 4 семестре и в форме контрольной работы и экзамена в 5 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Криптографические методы защиты информации», «Экономика информационной безопасности», «Информационные процессы и системы как объекты информационной безопасности», прохождения практики,

государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.11.06 «Дискретная математика»

Дисциплина «Дискретная математика» относится к обязательной 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-2,3,11 .

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-3. Способен использовать совокупность необходимых математических методов для решения задач профессиональной деятельности;

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 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 в 5 семестре для очной формы обучения и в форме контрольной работы и зачета в 6 семестре для очно-заочной формы обучения.

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

Блок Б1.О.12 Группа учебных дисциплин (модулей) «Физико-технические основы обеспечения информационной безопасности»

Б1.О.12.01 «Физика»

Дисциплина «Физика» относится к обязательной 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: ОПК-2,3,7,9,12, УК-9.

Дисциплина направлена на формирование следующих компетенций:

ОПК-4. Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности;
ОПК-11. Способен проводить эксперименты по заданной методике и обработку их результатов;

Содержание дисциплины охватывает круг вопросов, связанных с классическими разделами физики: механика, молекулярная физики и термодинамика, электродинамика, оптика, так и с современными: специальная теория относительности, квантовая механика и изложение на их основе элементов квантовой оптики, а 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 2-3 семестрах очно-заочной 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 в форме контрольной работы и экзамена в 3 семестре для очной формы обучения и зачёта во 2 семестре и экзамена во 3 семестре для очно-заочной 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.О.12.02 «Электротехника»

Дисциплина «Электротехника» относится к обязательной 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: ОПК-2,3,4,11.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-4. Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности;

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, имеющихся 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 очно-заочной 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 и для очно-заочной 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.О.12.03 «Электроника и схемотехника»

Дисциплина «Электроника и схемотехника» относится к обязательной 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: ОПК-2,3, 4,11,.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-4. Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности;

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 в 6 семестре для очно-заочной 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 и в форме контрольной работы и зачета в 6 семестре для очно-заочной 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.О.13 Группа учебных дисциплин (модулей) «Информационные технологии»

Б1.О.13.01 «Информатика»

Дисциплина «Информатика» относится к обязательной 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:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности;

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 и в 1 семестре очно-заочной 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 и в форме контрольной работы и экзамена в 1 семестре очно-заочной формы обучения.

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

Б1.О.13.02 «Языки программирования»

Дисциплина «Языки программирования» относится к обязательной 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 компетенцияхОПК-2,3, 11.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности;

Курс направлен на изучение объектно-ориентированных языков программирования семейства C (C++, C#) 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 C++ (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 C++ (универсальные платформы Microsoft.NET и технологии программирования Microsoft.NET Framework) и характерные особенности языка C# (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 на 3 курсе 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 работы и экзамена в 4 семестре для очной формы обучения контрольной работы и экзамена в 5 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Программно-аппаратные средства защиты информации», «Моделирование процессов и

систем защиты информации», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.13.03 «Технологии и методы программирования»

Дисциплина «Технологии и методы программирования» относится к обязательной 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-2,3,7,9,11.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности;

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 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 экзамена в 5 семестре для очной формы обучения и в форме контрольной работы и экзамена в 6 семестре для очно-заочной формы обучения.

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

Б1.О.13.04 «Информационные технологии»

Дисциплина «Информационные технологии» относится к обязательной 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: «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-2,3,7,9,11,.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-2. Способен применять информационно – коммуникационные технологии, программные средства системного и прикладного назначения, в

том числе отечественного производства, для решения задач профессиональной деятельности

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 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 в 5 семестре для очной формы обучения и контрольной работы и зачета в 6 семестре для очно-заочной формы обучения.

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

Б1.О.13.05 «Аппаратные средства вычислительной техники»

Дисциплина «Аппаратные средства вычислительной техники» относится к обязательной 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-2,3,7,9,11,.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-2. Способен применять информационно – коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;

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 на 4 курсе в 8 семестре для очно-заочной 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 и контрольной работы и экзамена в 8 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Программно-аппаратные средства защиты информации», «Моделирование процессов и систем 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.О.13.06 «Сети и системы передачи информации»

Дисциплина «Сети и системы передачи информации» относится к обязательной 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-2,3,7,9,11,.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;

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 TCPДР, архитектуру и средства взаимодействия процессов в сетях, основные принципы построения и современные тенденции развития сетей. Рассматривается архитектура и топологии построения современных ЛВС, технологии Ethernet (FastEthemet, GigabitEthemet), 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 на 4 курсе в 7 семестре для очно-заочной 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 и контрольной работы и экзамена в 7 семестре для очно-заочной 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.О.14 Группа учебных дисциплин (модулей) «Методы и средства обеспечения информационной безопасности»

Б1.О.14.01 «Основы информационной безопасности»

Дисциплина «Основы информационной безопасности» относится к обязательной 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: УК-1,2,5,10; ОПК-7; ПК-1,2,3.

Дисциплина направлена на формирование следующих компетенций:

ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;
ОПК-6. Способен при решении задач профессиональной деятельности организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;
ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;

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 5 зачетных единиц, 180 часа. Преподавание дисциплины ведется на 1-2 курсе в 2-3 семестрах для очной формы обучения и в 2-3 семестрах 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 во 2 семестре и контрольной работы и экзамена в 3 семестре для очной формы обучения и в форме контрольной работы во 2 семестре и зачета с оценкой в 3 семестре для очно-заочной формы обучения.

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

Б1.О.14.02 «Организационное и правовое обеспечение информационной безопасности»

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к обязательной 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: ОПК-1,6,7,8; УК-1,2,5,10; ПК-1,2,3.

Дисциплина направлена на формирование следующих компетенций:

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;
ОПК-6. Способен при решении задач профессиональной деятельности организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и 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 сферу 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 на 3 курсе 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 экзамена в 4 семестре и курсовой работы для очной формы обучения и экзамена в 5 семестре и курсовой работы для очно-заочной 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.О.14.03 «Основы управления информационной безопасностью»

Дисциплина «Основы управления информационной безопасностью» относится к обязательной 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», «Информационные процессы и системы как объекты информационной безопасности», «Конфиденциальное делопроизводство и защищенный электронный документооборот» и компетенциях:УК-1; ОПК-3; ДОПК-1,2,3,4.

Дисциплина направлена на формирование следующих компетенций:

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;

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 6 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 контрольная работа и зачета в 6 семестре для очной формы обучения и в форме контрольной работы и зачета в 6 семестре для очно-заочной 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.О.14.04 «Защита информации от утечки по техническим каналам»

Дисциплина «Защита информации от утечек по техническим каналам» относится к обязательной 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: ОПК-1,5,6,7,8,9, УК-2,5,10 ПК-1,2,3.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-6. Способен при решении задач профессиональной деятельности организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

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 на 4 курсе в 7 семестре для очно-заочной 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 и экзамена в 7 семестре и курсовой работы для очно-заочной формы обучения.

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

Б1.О.14.05 «Методы и средства криптографической защиты информации»

Дисциплина «Криптографические методы защиты информации» относится к обязательной 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: УК-1; ОПК-1,2,3,5,6,10.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;

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 в 9 семестре для очно-заочной 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 и контрольной работы и зачета в 9 семестре для очно-заочной 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.О.14.06 «Программно-аппаратные средства защиты информации»

Дисциплина «Программно-аппаратные средства защиты информации» относится к обязательной 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», «Методы и средства криптографической защиты информации» и компетенциях: УК-1; ОПК-2,3,5,7,9,10.

Дисциплина направлена на формирование следующих компетенций:

ОПК-6. Способен при решении задач профессиональной деятельности организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими

документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;
ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем и средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;

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 в 8 семестре для очно-заочной 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 и экзамена в 8 семестре и курсовой работы для очно-заочной 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.О.14.07 «Комплексное обеспечение защиты информации объекта информатизации (предприятия)»

Дисциплина «Комплексное обеспечение защиты информации объекта информатизации (предприятия)» относится к обязательной 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: УК-1; ОПК-2,3,5,7,9,10.

Дисциплина направлена на формирование следующих компетенций:

ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;
ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем и средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;
ДОПК-3. Способен разработать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;

Целями изучения дисциплины являются: Дать студентам знания по организации целесообразных мероприятий по защите информации на предприятиях (организациях и учреждений) 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 учреждений) 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 в 8-9 семестре для очно-заочной 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 контрольной работы и зачета в 7 семестре и в форме экзамена в 8 семестре и курсовой работы для очной формы обучения и в форме контрольной работы и зачета в 8 семестре и экзамена в 9 семестре и курсовой работы для очно-заочной 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.О.15 Дисциплины (модули) профиля: «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)»

Б1.О.15.01 «Математическая логика и теория алгоритмов»

Дисциплина «Математическая логика и теория алгоритмов» относится к обязательной 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», «Теория информации» и компетенциях: ОПК-2,3,7,9.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-3. Способен использовать совокупность необходимых математических методов для решения задач профессиональной деятельности;

Курс рассматривает основные понятия математической логики и теории алгоритмов как основы математических методов обработки информации в вычислительной технике.

Целью курса является приобретение опыта применения логических понятий и символики, ознакомление с аксиоматическим методом и логическим выводом, с классическими вариантами построения общей теории алгоритмов, с алгоритмически разрешимыми и неразрешимыми проблемами.

Содержание курса включает рассмотрение вопросов исчисления высказываний, предикатов, вычислимости функций, решения диофантовых уравнений, решения задач комбинаторной оптимизации, а также рассмотрение проблематики решения NP- полных задач.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 2 курсе 4 семестре для очной и на 3 курсе в 5 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 4 семестре для очной и в 5 семестре для очно-заочной формы обучения.

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

Б1.О.15.02 «Информационные процессы и системы как объекты информационной безопасности»

Дисциплина «Информационные процессы и системы как объекты информационной безопасности» относится к обязательной 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: «Математический анализ», «Информатика», «Языки программирования» и компетенциях: УК-1; ОПК-3,7.

Дисциплина направлена на формирование следующих компетенций:

ДОПК-1. Способен проводить анализ функционального процесса объекта информатизации с целью выявления возможных угроз, их вероятных целей, путей реализации и предполагаемого ущерба;
ДОПК-2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;
ДОПК-4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами;

Курс освещает вопросы, связанные с теорией и практикой исследования и реализации (использования) информационных процессов и систем в современном обществе.

Целью курса является формирование понимания особенностей анализа, синтеза и функционирования информационных систем, приобретение навыков

и умений исследования и использования информационных систем по профилю деятельности.

Содержание курса включает современные концепции (теории) информации, методы её исследования, модели динамики изменений объективной реальности (времени), сущность и классификацию информационных процессов, аспекты их моделирования и алгоритмизации, характеристики и классификации информационных систем, их проектирование и использование в конкретных предметных областях, а также общие аспекты безопасности информационных процессов и систем. Особое внимание обращено на кибернетические и интеллектуальные системы. Излагаются основные парадигмы теории интеллектуальных систем, включая так называемые системы «искусственного интеллекта». Рассматриваются инструментальные средства исследования, моделирования и проектирования информационных процессов и систем.

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 на 3 курсе в 5-6 семестрах 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 в 3 семестре и в форме контрольной работы и экзамена в 4 семестре для очной формы обучения и контрольной работы и зачета в 5 семестре и контрольной работы и экзамена в 6 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения всех последующих дисциплин «Конфиденциальное делопроизводство и защищенный электронный документооборот», «Моделирование процессов и систем защиты информации», «Информационная безопасность автоматизированных систем», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.15.03 «Конфиденциальное делопроизводство и защищенный электронный документооборот»

Дисциплина «Конфиденциальное делопроизводство и защищенный электронный документооборот» относится к обязательной 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: УК-1; ОПК-1,3,5,6,8,10.

Дисциплина направлена на формирование следующих компетенций:

ДОПК-1. Способен проводить анализ функционального процесса объекта информатизации с целью выявления возможных угроз, их вероятных целей, путей реализации и предполагаемого ущерба;
ДОПК-3. Способен разработать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;

Предмет изучения курса - проблемы построения и совершенствования технологии защищенного документооборота в условиях применения разнообразных типов носителей документной информации (бумажных, электронных и др.), а также различных. средств, способов и систем обработки и хранения конфиденциальных документов.

Цель курса - формирование знаний по научным, прикладным и методическим аспектам организации выполнения технологических стадий, процедур и операций с конфиденциальными документами, проектирование рациональной технологической схемы защищенного документооборота.

Тематика курса объединена в ряд логически связанных разделов. Первый носит теоретический характер и включает научные основы защищенного документооборота, рассмотрение организационных и технических каналов несанкционированного доступа к документам, функциональные возможности и эффективность различных способов и систем обработки, движения и хранения документов. Во втором разделе освещаются технологические стадии, процедуры и операции защиты и обработки документов. Третий раздел предполагает усвоение студентами технологии защиты конфиденциальных документов в архиве. В четвертом разделе дается авторская методика проектирования локальных и комплексных направлений совершенствования защищенного документооборота.

Предметом изучения курса являются основы документационного обеспечения управления (ДОУ), при этом главное место занимает рассмотрение вопросов управления документацией (документационного менеджмента) и документирования деятельности работников и структурных подразделений, в том числе служб, ответственных за выполнение режимных требований.

Целью дисциплины является формирование навыков организации эффективной системы документационного обеспечения управления деятельностью предприятия (организации, учреждения).

В курсе изучаются и анализируются законодательные и нормативно-правовые акты по документационному обеспечению управления, рассматриваются вопросы организационного регулирования документационных процессов, теории и практики современной технологии документооборота, этапы и стадии работы с документами (включая

получение, создание, обработку, отправку, хранение и уничтожение документов, экспертизу их ценности, формирование дел и передачу их в архивы), взаимодействие традиционной и электронной систем делопроизводства.

Содержание дисциплины охватывает круг вопросов, связанных с рассмотрением процесса организации электронного документооборота на предприятиях на примере системы «ДЕЛО», разработанной компанией «Электронные Офисные Системы» (ЭОС), изучением теоретических, методологических и практических проблем, охватывающих обеспечение автоматизации процессов делопроизводства и ведение полностью электронного документооборота на объекте информатизации.

Цель курса - формирование представления об электронном документе как новой составляющей в правовых отношениях. Выявление основных особенностей «электронного документа», базовых принципов взаимодействия электронного и аналогового «миров».

Тематика курса объединена в два логически связанных раздела, имеющих практический характер применения. Первый посвящен изучению архитектуры, особенности работы систем электронного документооборота и рассмотрению функциональных возможностей системы электронного делопроизводства «ДЕЛО». Второй - основным опциям системы электронного делопроизводства «ДЕЛО» и организации электронного документооборота, направленного на автоматизированную обработку конфиденциальных документов.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа. 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 (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 и контрольной работы и экзамена в 6 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Нормативные акты и стандарты по информационной безопасности», «Организация системы обеспечения информационной безопасности (служба ИБ)», «Моделирование процессов и систем защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.15.04 «Нормативные акты и стандарты по информационной безопасности»

Дисциплина «Нормативные акты и стандарты по информационной безопасности» относится к обязательной 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: УК-1; ОПК-1,3,5,6,8,10.

Дисциплина направлена на формирование следующих компетенций:

ДОПК-2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;
ДОПК-3. Способен разработать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;
ДОПК-4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами;

Курс посвящен проблеме обеспечения безопасности информационных систем в части задачи нормативного регулирования деятельности в этой области.

Цель курса - ознакомить с отечественными и зарубежными нормативными актами и иными документами в области обеспечения безопасности информационных систем и смежных областях, дать представление о практических навыках проведения аудита систем и организаций на соответствие нормативным актам.

Содержание курса включает с себя вопросы, связанные со структурой и содержанием процесса обеспечения безопасности информационных систем. Рассматриваются задачи нормативного регулирования отношений, возникающих на различных стадиях процесса обеспечения безопасности, структура и содержание системы нормативного обеспечения безопасности. Раскрываются вопросы нормативного регулирования развития терминологии в области обеспечения безопасности информационных систем, нормативного обеспечения в области анализа рисков нарушения безопасности, нормативного регулирования технической и криптографической защиты информации. Рассмотрены стандарты в области обеспечения функциональной безопасности информационных систем, организации проектирования информационных систем в защищённом исполнении, управления информационной безопасностью, тенденции развития системы нормативного обеспечения безопасности.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и на 3 курсе 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 экзамена в 5 семестре для очной формы обучения и контрольной работы и экзамена в 6 семестре для очно-заочной 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.О.15.05 «Организация системы обеспечения информационной безопасности (служба ИБ)»

Дисциплина «Организация системы обеспечения информационной безопасности (служба ИБ)» относится к обязательной 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: УК-1; ОПК-1,3,5,6,8,10.

Дисциплина направлена на формирование следующих компетенций:

ДОПК-1. Способен проводить анализ функционального процесса объекта информатизации с целью выявления возможных угроз, их вероятных целей, путей реализации и предполагаемого ущерба;
ДОПК-2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;

Цели преподавания дисциплины:

1) подготовить специалистов, владеющих знаниями в области организационных и правовых основ обеспечения информационной

безопасности (ИБ) и организации режима секретности на объектах и системах различного профиля и организационной структуры;

2) дать основные сведения о нетехнических методиках обеспечения защиты информации, составляющей государственную и коммерческую тайну, конфиденциальной информации, а также о методиках противодействия промышленному шпионажу.

Задачами изучения дисциплины являются:

1) усвоение организационных основ построения систем защиты информации и организации работ по обеспечению ИБ на объектах информатизации (ОИ), основных подходов к комплексной оценке безопасности информации на ОИ;

2) знакомство с основными положениями государственной системы защиты информации и правового обеспечения ИБ в РФ;

3) знакомство с видами и типами компьютерных преступлений и способами противодействия различным видам атак;

4) усвоение методик построения систем организационной защиты объектов информатизации.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и на 5 курсе в 9 семестре для очно-заочной 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 зачет с оценкой в 7 семестре для очной формы обучения и контрольной работы и зачет с оценкой в 9 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Экономика информационной безопасности», отдельные разделы «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.О.15.06 «Физическая защита информационных объектов»

Дисциплина «Физическая защита информационных объектов» относится к обязательной 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», «Информационные процессы и системы как объекты информационной безопасности» и компетенциях: ОПК-1,5,6,8,10; ДОПК-1,2,4.

Дисциплина направлена на формирование следующих компетенций:

ДОПК-1. Способен проводить анализ функционального процесса объекта информатизации с целью выявления возможных угроз, их вероятных целей, путей реализации и предполагаемого ущерба;
ДОПК-3. Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;

Курс рассматривает волновые процессы в их прикладном значении для защиты информации.

Курс направлен на формирование понимания физической природы волновых процессов в различных средах и возможности использования законов физики для обеспечения защиты информации.

Курс состоит из двух разделов. В первом разделе рассматриваются электромагнитные волны, физическая картина излучений, дается представление об экранировании и электромагнитной совместимости, побочных электромагнитных излучениях и наводках (ПЭМИН). Во втором разделе изучаются упругие волны, основы акустики речи и акустики помещений, инфразвук, ультразвук, а также физические поля как носители информации об объектах.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часов. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и в 8 семестре для очно-заочной 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 и контрольной работы и экзамена в 8 семестре для очно-заочной 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.О.15.07 «Информационно-аналитическая деятельность по обеспечению комплексной безопасности»

Дисциплина «Информационно-аналитическая деятельность по обеспечению комплексной безопасности» относится к обязательной 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 процессы и системы как объекты информационной безопасности», «Информационные технологии» и компетенциях: ОПК-1,5,6,7,8,9,10; ДОПК-1,2,3,4.

Дисциплина направлена на формирование следующих компетенций:

ДОПК-1. Способен проводить анализ функционального процесса объекта информатизации с целью выявления возможных угроз, их вероятных целей, путей реализации и предполагаемого ущерба;
ДОПК-2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;

Содержание дисциплины связано с изучением сущности и значения информационно-аналитической деятельности для обеспечения защиты информации, ее места в системе информационной безопасности, определением теоретических, концептуальных, методологических, организационных и правовых основ информационно-аналитического обеспечения управления.

Целью курса является формирование умений осуществлять эффективную информационно-аналитическую деятельность по обеспечению информационной безопасности предприятия, включающую организацию целенаправленного поиска, оценки и анализа информации.

Структура курса знакомит с современными методами и организацией аналитической работы, технологией и средствами поиска, сопоставления, отбора, оценки (актуальности, достоверности и др.) информации для обеспечения безопасности предприятия (организации).

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и на 5 курсе в 9 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 экзамена в 7 семестре для очной формы

обучения и контрольной работы и экзамена в 9 семестре для очно-заочной формы обучения.

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

Б1.О.15.08 «Экономика информационной безопасности»

Дисциплина «Экономика информационной безопасности» относится к обязательной 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», «Организация системы обеспечения информационной безопасности (служба ИБ)» и компетенциях: УК-5,9; ОПК-5,10,12,13; ДОПК-1,2.

Дисциплина направлена на формирование следующих компетенций:

УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности;
ДОПК-2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;
ДОПК-3. Способен разработать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;
ДОПК-4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами;

Курс содержит сведения об основных экономических понятиях и критериях определения экономической эффективности защиты информации; об основных факторах, определяющих возможную величину ущерба; о методах оценки эффективности инвестиций в защиту информации; о видах рисков; об использовании страхования в целях защиты информации.

Целью курса является формирование знаний об экономических методах защиты информации как части общих организационных мер, умении использовать современные методы расчетов для определения экономической целесообразности применения различных методов и средств защиты информации, обеспечивать выбор наиболее эффективных проектов инвестиций в защиту информации.

В содержании курса раскрываются вопросы, связанные с экономическими аспектами защиты информации, исследуются стоимостные показатели информации и виды ущерба, наносимые информации, даются основные подходы к определению затрат на защиту информации, оценка эффективности применяемых методов защиты и системы защиты информации в целом. Изучается вопросы управления ресурсами в процессе защиты информации, а также порядок формирования бюджета службы защиты информации на предприятии.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часов. Преподавание дисциплины ведется на 4 курсе в 8 семестре для очной формы обучения и на 5 курсе в 10 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 экзамена в 8 семестре для очной формы обучения и контрольной работы и экзамена в 10 семестре для очно-заочной формы обучения.

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

Б1.О.15.09 «Моделирование процессов и систем защиты информации»

Дисциплина «Моделирование процессов и систем защиты информации» относится к обязательной 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: «Конфиденциальное делопроизводство и защищенный электронный документооборот», «Физическая защита информационных объектов», «Основы управления информационной безопасностью», «Информационные процессы и системы как объекты информационной безопасности» и компетенциях: ДОПК-1,2,3,4; ОПК-5,10.

Дисциплина направлена на формирование следующих компетенций:

ДОПК-1. Способен проводить анализ функционального процесса объекта информатизации с целью выявления возможных угроз, их вероятных целей, путей реализации и предполагаемого ущерба;
ДОПК-4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами;

Предметом изучения курса являются теоретические, методологические и практические вопросы системных исследований на основе математического моделирования процессов и систем зашиты информации в области обеспечения комплексной информационной безопасности современных объектов различного назначения, включая и финансово-кредитную сферу. В дисциплине современные методы математического моделирования рассматриваются как универсальный инструмент обоснования целесообразных мер (решений) сложнейших проблем, возникающих в ходе построения и развертывания новейших вариантов информационной безопасности.

Целью курса является формирование первичных знаний, умений и практических навыков по основам моделирования процессов и систем в области защиты информации на основе разработки компьютерного моделирования и обработки результатов вычислительных экспериментов, а также формирование представления о работе с современными инструментальными системами моделирования.

Тематика курса объединена в виде логически увязанных разделов. Первый носит общетеоретический характер и включает научные основы методов и методологии анализа и синтеза выявления и разрешения проблемных вопросов по защите информации. Во втором разделе освещаются методико-прикладные аспекты математического моделирования организации комплексного обеспечения информационной безопасности применительно к типовым предприятиям (организациям и учреждениям), включая и финансово - кредитные структур. Рассматриваются в системном виде основные этапы и процессы построения комплексных систем защиты информации, состав обеспечивающих их компонентов, принципы и содержание управления, а также и вопросы оценки эффективности информационной безопасности.

Предметом изучения курса являются процессы и систем организации защиты информации с ориентацией на сложные информационные объекты.

Целевая направленность курса предусматривает формирование навыков математического обоснования целесообразных управленческих решений, прежде всего в ходе информационно-аналитической деятельности по защите информации.

В курсе также изучаются и анализируются существующие законодательные и нормативно-правовые документы по разработке и функционированию современных систем защиты информации в тесном взаимодействии со всеми видами обеспечения информационной безопасности.

В результате освоения дисциплины студент должен:

-знать: принципы построения аналитико-имитационных моделей информационных процессов, основные классы моделей и методы моделирования, методы формализации, алгоритмизации и реализации моделей на ЭВМ; приемы, методы, способы формализации объектов, процессов, явлений и реализации их на компьютере;

-уметь: использовать современные методы и инструментальные средства моделирования при исследовании процессов и проектировании систем защиты

информации; планировать проведение имитационных экспериментов и обрабатывать их результаты;

-владеть: технологией математического и компьютерного моделирования при анализе процессов и синтезе современных систем защиты информации.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Преподавание дисциплины ведется на 4 курсе в 8 семестре для очной и на 4 курсе в 7 семестре очно-заочной формы обучения 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 зачета в 8 семестре для очной и 7 семестре очно-заочной 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.О.16 Элективные курсы по физической культуре и спорту

Дисциплина «Элективные курсы по физической культуре и спорту» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений 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:

УК-7. Способен поддерживать должный уровень физической подготовленности 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 и 328 часов, 9 зачётных единиц для очно-заочной формы обучения. Преподавание дисциплины ведется на 1-3 курсах в 1,3-6 семестрах для очной формы обучения и во 1 семестре для очно-заочной 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 1,3-6 семестрах для очной формы обучения и зачета во 1 семестре для очно-заочной 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.О.17 Основы военной подготовки

Дисциплина «Основы военной подготовки» относится к обязательной части основной образовательной программы подготовки бакалавров 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой социальных и гуманитарных дисциплин.

Дисциплина базируется на ранее полученных знаниях по ранее изученным дисциплинам в средней школе, и дисциплине «Безопасность жизнедеятельности» и опирается на коммуникативные компетенции, приобретённые в средней общеобразовательной школе и компетенции: УК-7; УК-8.

В процессе обучения студент приобретает и совершенствует следующие компетенции:

УК-7. способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности;

УК-8. способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов.

Содержание дисциплины включает в себя основные направления социально-экономического, политического и военно-технического развития Российской Федерации, особенности развития международных отношений, правовые основы прохождения военной службы, строевую подготовку, основы тактической, медицинской подготовки и другие разделы.

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часа.

Преподавание дисциплины ведется на 2 курсе в третьем семестре для очной формы обучения и на 2 курсе в 3 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 аттестация в форме зачета в 3 семестре для очной формы обучения и в 3 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для формирования навыков в области военной подготовки, высокого патриотического сознания, возвышенного чувства верности своему Отечеству, готовности к его защите как важнейшей конституционной обязанности в отстаивании национальных интересов Российской Федерации и обеспечении ее военной безопасности перед лицом внешних и внутренних угроз.

Часть, формируемая участниками образовательных отношений

Б1.В.0.1 Дисциплины (модули) образовательной организации

Б1.В.01.01 «Основы исследований информационной безопасности»

Дисциплина «Основы исследований информационной безопасности» относится к дисциплинам по выбору 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:

УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;
УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности;
ПК-1. Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-2. Способность принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-3. Способность осуществлять управление с разработкой организационно-распорядительных документов и реализацию организационных мер по ЗИ в АС;

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 часа. Преподавание дисциплины ведется на 1 курсе в 1 семестре для очной формы обучения и во 1 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 экзамена в 1 семестре для очной и в 1 семестре для очно-заочной 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 «Пакеты прикладных программ»

Дисциплина «Пакеты прикладных программ» относится к дисциплинам части, формируемой участниками образовательных отношений 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:

ПК-2. Способность принимать участие в проведении экспериментальных исследований системы защиты информации

ПК-4. Способность осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

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 1Р-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 во 3 семестре для очной формы обучения и на 2 курсе в 3 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 экзамена во 3 семестре для очной формы обучения, контрольной работы и экзамена в 3 семестре для очно-заочной 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.01.03 «Социально-психологические основы управленческой деятельности»

Дисциплина «Социально-психологические основы управленческой деятельности» относится к дисциплинам части, формируемой участниками образовательных отношений, 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: УК-6,8; ПК-1.

Дисциплина направлена на формирование следующих компетенций:

УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;

ПК-3. Способность осуществлять управление с разработкой организационно-распорядительных документов и реализацию организационных мер по ЗИ в АС;

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 и в 4 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационные технологии в профессиональной деятельности», «Адаптированные информационные технологии», «Нормативные акты и стандарты по информационной безопасности», «Организация системы обеспечения информационной безопасности (служба ИБ)», «Моделирование процессов и систем защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.01.04 «Основы конкурентной разведки»

Дисциплина «Основы конкурентной разведки» относится к дисциплинам части, формируемой участниками образовательных отношений, 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», «Основы исследований информационной безопасности» и компетенциях: УК-2,7,8,10; ПК-3.

Дисциплина направлена на формирование следующих компетенций:

УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;
ПК-4 Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ ТКС при возникновении внештатных ситуаций

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа. Преподавание дисциплины ведется на 2 курсе в 3,4 семестре для очной и на 3 курсе в 5,6 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 и зачета с оценкой в 4 семестре для очной и в 5,6 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационные технологии в профессиональной деятельности», «Адаптированные информационные технологии», «Нормативные акты и стандарты по информационной безопасности», «Организация системы обеспечения информационной безопасности (служба ИБ)», «Моделирование процессов и систем защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.01.05 «История защиты информации в РФ»

Дисциплина «История защиты информации в РФ» относится к дисциплинам части, формируемой участниками образовательных отношений 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: УК-5; ОПК-1,5,6,8,13.

Дисциплина направлена на формирование следующих компетенций:

УК-5. Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах;
ПК-3. Способность осуществлять управление с разработкой организационно-распорядительных документов и реализацию организационных мер по ЗИ в АС;

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 на 2 курсе в 4 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 в форме контрольной работы и зачета с оценкой в 4 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.01.06 «Информационная безопасность автоматизированных систем»

Дисциплина «Информационная безопасность автоматизированных систем» относится к дисциплинам части, формируемой участниками образовательных отношений, 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», «Конфиденциальное делопроизводство и защищенный электронный документооборот» и компетенциях:ОПК-1,5,6,8,9; ДОПК-1,3.

Дисциплина направлена на формирование следующих компетенций:

ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

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 на 4 курсе в 7 семестре для очно-заочной 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 и контрольной работы и зачета в 7 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: отдельные разделы «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 части, формируемой участниками образовательных отношений, 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:

УК-5. Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах;
ПК-1. Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;

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. Практическая подготовка составляет 8/8 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 1 курсе в 1 семестре для очной формы обучения и на 1 курсе в 2 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 экзамена в 1 семестре для очной и контрольной работы и экзамена в 2 семестре для очно-заочной 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.О3 «Безопасность информационных технологий»

Дисциплина «Безопасность информационных технологий» относится к обязательным дисциплинам части, формируемой участниками образовательных отношений 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», «Информационные процессы и системы как объекты информационной безопасности» и компетенциях: ОПК-1,3,5,6,8; ДОПК-1,2,4.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ПК-5. Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

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 на 4 курсе в 8 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 6 семестре для очной формы обучения и в форме контрольной работы и зачета с оценкой в 8 семестре для очно-заочной 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.О4 «Гуманитарные аспекты (профессиональная этика) информационной безопасности»

Дисциплина «Гуманитарные аспекты (профессиональная этика) информационной безопасности» относится к обязательным дисциплинам части, формируемой участниками образовательных отношений 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», «Конфиденциальное делопроизводство и защищенный электронный документооборот», «Математическая логика и теория алгоритмов» и компетенциях:ОПК-1,3,5,6,8; ДОПК-1,3.

Дисциплина направлена на формирование следующих компетенций выпускника:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;

ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;

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 разрешении 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. Практическая подготовка составляет 4/4 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной и на 4 курсе в 7 семестре очно-заочной 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 и во 7 семестре 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», «Лицензирование и сертификация в области защиты информации», 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 части, формируемой участниками образовательных отношений 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: ОПК-2,3,7,9; УК-6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

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. Практическая подготовка составляет 16/16 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 2 курсе в 4 семестре для очной обучения и на 3 курсе 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 работы и зачета в 4 семестре для очной формы обучения и в форме контрольной работы 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 части, формируемой участниками образовательных отношений 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: ОПК-2,3,7,9; УК-6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

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. Практическая подготовка составляет 16/16 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 2 курсе в 4 семестре для очной обучения и на 3 курсе 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 работы и зачета в 4 семестре для очной формы обучения и в форме контрольной работы 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.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 части, формируемой участниками образовательных отношений 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-7,9.

Дисциплина направлена на формирование следующих компетенций выпускника:

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

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. Практическая подготовка составляет 8/8 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 1 курсе во 2 семестре для очной формы обучения и на 2 курсе в 3 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 экзамена во 2 семестре для очной формы обучения и в форме контрольной работы и экзамена в 3 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационные процессы и системы как объекты информационной безопасности», «Конфиденциальное делопроизводство и защищенный электронный документооборот», «Моделирование процессов и систем защиты информации», 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 части, формируемой участниками образовательных отношений 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-7,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

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. Практическая подготовка составляет 8/8 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 1 курсе во 2 семестре для очной формы обучения и на 2 курсе в 3 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 экзамена во 2 семестре для очной формы обучения и в форме контрольной работы и экзамена в 3 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационные процессы и системы как объекты информационной безопасности», «Конфиденциальное делопроизводство и защищенный электронный документооборот», «Моделирование процессов и систем защиты информации», 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 части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;

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. Практическая подготовка составляет 8/8 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и на 4 курсе в 7 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 экзамена в 5 семестре для очной формы обучения и экзамена в 7 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», «Организация системы обеспечения информационной безопасности (служба ИБ)», 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 части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;

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. Практическая подготовка составляет 8/8 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и на 4 курсе в 7 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 экзамена в 5 семестре для очной формы обучения и в форме контрольной работы и экзамена в 7 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», «Организация системы обеспечения информационной безопасности (служба ИБ)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.03.03 «Подготовка объекта информатизации к аттестации по требованиям безопасности информации (ООО "НОВО")

Дисциплина «Подготовка объекта информатизации к аттестации по требованиям безопасности информации (ООО «НОВО») относится к дисциплинам по выбору части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;

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 3 зачетных единицы, 108 часа. Практическая подготовка составляет 8/8 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и на 4 курсе в 7 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 экзамена в 5 семестре для очной формы обучения и контрольной работы и экзамена в 7 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», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.03.04 «Аттестация объекта информатизации по требованиям безопасности информации (ООО "ЦБИ")»

Дисциплина «Аттестация объекта информатизации по требованиям безопасности информации (ООО "ЦБИ")» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;

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 3 зачетных единицы, 108 часа. Практическая подготовка составляет 8/8 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и на 4 курсе в 7 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 экзамена в 5 семестре для очной формы обучения и контрольной работы и экзамена в 7 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», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», 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 части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;

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. Практическая подготовка составляет 4 часа для очно-заочной формы обучения. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и на 4 курсе в 7 семестре для очно-заочной 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 5 семестре для очной формы обучения и в форме контрольной работы и зачета с оценкой в 7 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», «Организация системы обеспечения информационной безопасности (служба ИБ)», «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 части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;

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. Практическая подготовка составляет 4 часа для очно-заочной формы обучения. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и на 4 курсе в 7 семестре для очно-заочной 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 5 семестре для очной формы обучения и в форме контрольной работы и зачета с оценкой в 7 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», «Организация системы обеспечения информационной безопасности (служба ИБ)», «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 (ООО "НОВО")

Дисциплина «Организация защиты конфиденциальной информации от несанкционированного доступа (ООО «НОВО») относится к дисциплинам по выбору части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;

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, исключающей 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. Практическая подготовка составляет 4 часа для очно-заочной формы обучения. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и на 4 курсе в 7 семестре для очно - заочной 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 5 семестре для очной формы

обучения и контрольной работы и зачета с оценкой в 7 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», «Организация системы обеспечения информационной безопасности (служба ИБ)», «Лицензирование и сертификация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.04.04 «Защита информации от НСД (ООО «ЦБИ»)»

Дисциплина «Защита информации от НСД (ООО «ЦБИ»)» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;

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, исключающей 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. Практическая подготовка составляет 4 часа для очно-заочной формы обучения. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и на 4 курсе в 7 семестре для очно - заочной 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 5 семестре для очной формы обучения и контрольной работы и зачета с оценкой в 7 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», «Организация системы обеспечения информационной безопасности (служба ИБ)», «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 части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

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. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и на 4 курсе в 8 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 в 6 семестре для очной формы обучения и контрольной работы и зачета в 8 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», «Организация системы обеспечения информационной безопасности (служба ИБ)», «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 части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

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. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и на 4 курсе в 8 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 в 6 семестре для очной формы обучения и контрольной работы и зачета в 8 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», «Организация системы обеспечения информационной безопасности (служба ИБ)», «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")»

Дисциплина «Оценка защищенности конфиденциальной информации по техническим каналам и от несанкционированного доступа (ОАО «НОВО», НТЦ «ЗАРЯ»)» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

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. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины

ведется на 3 курсе в 6 семестре для очной формы обучения и на 4 курсе в 8 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 в 6 семестре для очной формы обучения и контрольной работы и зачета в 8 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», «Организация системы обеспечения информационной безопасности (служба ИБ)», «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.05.04 «Контроль защищенности информации от утечки по техническим каналам (ООО "ЦБИ")»

Дисциплина «Контроль защищенности информации от утечки по техническим каналам (ООО "ЦБИ")» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

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. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и на 4 курсе в 8 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 в 6 семестре для очной формы обучения и контрольной работы и зачета в 8 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», «Организация системы обеспечения информационной безопасности (служба ИБ)», «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 части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9; ПК-1,2,3,4.

Дисциплина направлена на формирование следующих компетенций:

ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

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. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и на 5 курсе в 9 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 экзамена в 7 семестре для очной формы обучения и контрольной работы и экзамена в 9 семестре для очно - заочной 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 части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9; ПК-1,2,3,4.

Дисциплина направлена на формирование следующих компетенций:

ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

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. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и на 5 курсе в 9 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 экзамена в 7 семестре для очной формы обучения и контрольной работы и экзамена в 9 семестре для очно-заочной 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")»

Дисциплина «Методы и средства защиты информации от утечки по техническим каналам (ОАО «НОВО», НТЦ «ЗАРЯ»)» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений 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: ОПК-2,3,4,11; УК-4.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

Цель изучение 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. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и на 5 курсе в 9 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 экзамена в 7 семестре для очной формы обучения и контрольной работы и экзамена в 9 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Моделирование процессов и систем защиты информации», «Нормативные акты и стандарты по информационной безопасности», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)»,

прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.06.04 «Средства защиты информации и оценка эффективности защиты от утечки по техническим каналам (ООО "ЦБИ")»

Дисциплина «Средства защиты информации и оценка эффективности защиты от утечки по техническим каналам (ООО "ЦБИ")» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений 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: ОПК-2,3,4,11; УК-4.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

Цель изучение 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. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и на 5 курсе в 9 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 экзамена в 7 семестре для очной формы обучения и контрольной работы и экзамена в 9 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Моделирование процессов и систем защиты информации», «Нормативные акты и стандарты по информационной безопасности», «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 части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

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. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и на 4 курсе в 8 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 в 6 семестре для очной формы обучения и контрольной работы и зачета в 8 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», «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 части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

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. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и на 4 курсе в 8 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 в 6 семестре для очной формы обучения и контрольной работы и зачета в 8 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», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.07.03 «Технические каналы утечки конфиденциальной информации (ООО "НОВО")»

Дисциплина «Технические каналы утечки конфиденциальной информации (ООО «НОВО»)» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

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 2 зачетных единицы, 72 часа. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и на 4 курсе в 8 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 в 6 семестре для очной формы обучения и зачета в 8 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», «Организация системы обеспечения информационной безопасности (служба ИБ)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.07.04 «Технические каналы утечки информации (ООО "ЦБИ")»

Дисциплина «Технические каналы утечки конфиденциальной информации (ООО «ЦБИ»)» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

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 2 зачетных единицы, 72 часа. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и на 4 курсе в 8

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 в 6 семестре для очной формы обучения и зачета в 8 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», «Организация системы обеспечения информационной безопасности (служба ИБ)», 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 части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9; ПК-1,2,3,4.

Дисциплина направлена на формирование следующих компетенций:

ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

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. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 4 курсе в 8 семестре для очной формы обучения и в 9 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 в 8 семестре для очной формы обучения и контрольной работы и зачета в 9 семестре для очно-заочной 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 части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9; ПК-1,2,3,4.

Дисциплина направлена на формирование следующих компетенций:

ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

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. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 4 курсе в 8 семестре для очной формы обучения и в 9 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 в 8 семестре для очной формы обучения и контрольной работы и зачета в 9 семестре для очно-заочной 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")»

Дисциплина «Разработка объекта информатизации в защищенном исполнении (ОАО «НОВО»)» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9; ПК-1,2,3,4.

Дисциплина направлена на формирование следующих компетенций:

ПК-2. Способность принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

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. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 4 курсе в 8 семестре для очной формы обучения и в 9 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 в 8 семестре для очной формы обучения и контрольной работы и зачета в 9 семестре для очно - заочной 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.08.04 «Разработка и сертификация средств защиты информации и технических средств в защищенном исполнении (ООО "ЦБИ")»

Дисциплина «Разработка и сертификация средств защиты информации и технических средств в защищенном исполнении (ООО "ЦБИ")» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9; ПК-1,2,3,4.

Дисциплина направлена на формирование следующих компетенций:

ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

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. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 4 курсе в 8 семестре для очной формы обучения и в 9 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 в 8 семестре для очной формы обучения и контрольной работы и зачета в 9 семестре для очно - заочной 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 части, формируемой участниками образовательных отношений 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», «Нормативные акты и стандарты по информационной безопасности», и компетенциях: ОПК-2,3,4,8,11; УК-4; ДОПК-1,2,3,4.

Дисциплина направлена на формирование следующих компетенций:

ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

Цель изучение 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 5 семестре для очной формы обучения и на 5 курсе в 9 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 в 5 семестре для очной формы обучения и контрольной работы и зачета в 9 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Моделирование процессов и систем защиты информации», «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 части, формируемой участниками образовательных отношений 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: ОПК-2,3,4,11; УК-4.

Дисциплина направлена на формирование следующих компетенций:

ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

Цель изучение 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 5 семестре для очной формы обучения и на 5 курсе в 9 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 в 5 семестре для очной формы обучения и контрольной работы и зачета в 9 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Моделирование процессов и систем защиты информации», «Нормативные акты и стандарты по информационной безопасности», «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")»

Дисциплина «Методы и средства защиты информации от несанкционированного доступа (ООО «НОВО»)» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений 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: ОПК-2,3,4,11; УК-4.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

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 5 семестре для очной формы обучения и на 5 курсе в 9 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 5 семестре для очной формы обучения и контрольной работы и зачета в 9 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Моделирование процессов и систем защиты информации», «нормативные акты и стандарты по информационной безопасности», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.09.04 «Методы и средства обеспечения защищенности информации от несанкционированного доступа (ООО "ЦБИ")»

Дисциплина «Методы и средства обеспечения защищенности информации от несанкционированного доступа (ООО "ЦБИ")» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений 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: ОПК-2,3,4,11; УК-4.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;

ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

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 5 семестре для очной формы обучения и на 5 курсе в 9 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 5 семестре для очной формы обучения и контрольной работы и зачета в 9 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Моделирование процессов и систем защиты информации», «нормативные акты и стандарты по информационной безопасности», «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 части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;

Целями изучения дисциплины являются: Дать студентам базовые знания по основам обеспечения социотехносферной безопасности ключевых объектов информационной защиты на предприятиях, организациях и учреждений 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 учреждений) с различными формами собственности с учетом современных подходов обеспечения информационной безопасности.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Практическая подготовка составляет 16/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и в 10 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 экзамена 6 семестре для очной формы обучения и контрольной работы и экзамена в 10 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Моделирование процессов и систем защиты информации», «нормативные акты и стандарты по информационной безопасности», «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 части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности;
ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-4. Способность осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

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. Практическая подготовка составляет 16/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и в 10 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 экзамена 6 семестре для очной формы обучения и контрольной работы и экзамена в 10 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Моделирование процессов и систем защиты информации», «нормативные акты и стандарты по информационной безопасности», «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", ООО "ЦБИ")

Дисциплина «Методы и средства выявления демаскирующих признаков закладочных устройств в защищаемых помещениях (ОАО «НОВО». НТЦ «ЗАРЯ») относится к дисциплинам по выбору части, формируемой участниками образовательных отношений 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: ОПК-1,6,7,8,9,13; УК-5,6,9; ПК-1,2,3,4.

Дисциплина направлена на формирование следующих компетенций:

ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-4. Способность осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;
ПК-5. Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

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. Практическая подготовка составляет 16/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и в 10 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 экзамена в 6 семестре для очной формы обучения и контрольной работы и экзамена в 10 семестре для очно-заочной 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 части, формируемой участниками образовательных отношений 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:

УК-5. Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах;
ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;

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. Практическая подготовка составляет 16/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 1 курсе в 1 семестре для очной и 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 1 семестре для очной и очно-заочной 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 ОВЗВ» относится к обязательным дисциплинам части, формируемой участниками образовательных отношений, 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:

УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни;
ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;

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. Практическая подготовка составляет 16/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 1 курсе в 1 семестре для очной и 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 1 семестре для очной и очно-заочной 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.

Блок 2. Практика

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.

Практическая подготовка – форма организации образовательной деятельности при освоении ОПОП в условиях выполнения обучающимися

определенных видов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций по профилю ОПОП.

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: ознакомительная практика; учебно-лабораторная практика.

производственная практика: 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 универсальных 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 5, 6, 7.

Обязательная часть
Б2.В.01(П) Преддипломная практика

Производственная (преддипломная) практика (6 недель, (324 часа), 9 зачетных единиц) проводится на 4 курсе в восьмом семестре для очной формы обучения и на 5 курсе в девятом семестре для очно-заочной формы обучения с целью углубления и закрепления профессиональных знаний и навыков, полученных при теоретическом обучении и формирования компетенций:

ОПК-5.Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности
ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;
ДОПК-1. Способен проводить анализ функционального процесса объекта информатизации с целью выявления возможных угроз, их вероятных целей, путей реализации и предполагаемого ущерба;
ДОПК-2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;
ДОПК-3. Способен разработать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;
ДОПК-4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами

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 безопасности; Аудитория 2210а: Лаборатория защищенных технических средств и систем; Аудитория 2206: Лаборатория технологий обеспечения информационной безопасности, ООО «НОВО», НТЦ «ЗАРЯ», ООО «ЦБИ».

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 девятом семестре для очно-заочной формы обучения.

Часть, формируемая участниками образовательных отношений

Б2.В.01 (У) Ознакомительная практика

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 и на 2 курсе в четвертом семестре для очно-заочной формы обучения с целью углубления и закрепления первичных профессиональных знаний и навыков, полученных при теоретическом обучении и формирования компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;
УК-3. Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде;
УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни;
УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности;
ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;

ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;

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», «Защищённые 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 безопасности; 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 и в четвертом семестре для очно-заочной формы обучения.

Б2.В.02(У) Учебно-лабораторная практика

Учебная (технологическая) практика (2 недели, (108 часов), 3 зачетных единицы) проводится на 2 курсе в четвертом семестре для очной и на 3 курсе в шестом семестре для очно-заочной формы обучения с целью углубления и закрепления первичных профессиональных знаний и навыков, полученных при теоретическом обучении и формирования компетенций:

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;

ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

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», «Защищённые 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 безопасности; 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 и в шестом семестре для очно-заочной формы обучения.

Б2.В.03 (П) Технологическая практика

Производственная (проектно-технологическая) практика (2 недели, (108 часов), 3 зачетных единицы) проводится на 3 курсе в шестом семестре для очной и на 4 курсе в восьмом семестре для очно-заочной формы обучения, с целью углубления и закреп навыков, полученных при теоретическом обучении и формирования компетенций:

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;

ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

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», «Защищённые 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 безопасности; 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», ООО «ЦБИ».

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 и в восьмом 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 потребностям.

ФТД.В.01 «Технико-экономическое обоснование проекта»

Дисциплина «Технико-экономическое обоснование проекта» относится к факультативным дисциплина 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», «Конфиденциальное делопроизводство и защищенный электронный документооборот», «Криптографические методы защиты информации», а также компетенциях и компетенциях: УК-5; ОПК-1,5,6,8,9,13; ДОПК-1,3.

Дисциплина направлена на формирование следующих компетенций:

УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;
УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности;
ПК-5. Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

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 и очно-заочной форм 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 и очно-заочной 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 дисциплина 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», «Конфиденциальное делопроизводство и защищенный электронный документооборот», «Криптографические методы защиты информации», а также компетенциях и компетенциях: УК-5; ОПК-1,5,6,8,9,13; ДОПК-1,3.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;
УК-3. Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде;
УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности;
ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-5. Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

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-правого 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 4 курсе в 7 семестре для очной и очно-заочной форм 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 и курсового проекта в 6 семестре и зачета с оценкой и курсового проекта в 7 семестре для очной и очно-заочной форм 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.

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» (уровень бакалавриата).

Основная профессиональная образовательная программа обеспечена учебно-методической документацией и материалами по всем учебным дисциплинам основной 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 обучающихся, 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 **0,25** экземпляра каждого изданий, указанных в рабочих программах дисциплин (модулей), практик, на одного обучающегося из числа лиц, одновременно осваивающих соответствующую дисциплину (модуль), проходящих соответствующую практику.

Библиотека использует современные информационные технологии для обеспечения высокого уровня образовательного процесса.

Значительная часть учебной и учебно-методической литературы представлена для изучения обучающимися 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 и электронные библиотеки: ***Электронно-библиотечная система «Университетская библиотека онлайн»; Национальная электронная библиотека; «Национальный цифровой ресурс «Руконт»; Электронно-библиотечная система «ИНФРА-М» ZNANIUM.com; Электронно-библиотечная система «Издательство «Лань»; Образовательная платформа «Юрайт»; Цифровой образовательный ресурс IPR SMART.***

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 МАРК 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, является Web-сайт университета. Сайт предоставляет возможность обучающимся 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 обучающихся 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.

Материально-техническое обеспечение

Перечень материально-технического обеспечения:

- лекционные аудитории (оборудованные учебной мебелью, наглядными учебными пособиями и видеопроекционным оборудованием для презентаций, средствами звуковоспроизведения, экраном, и имеющие выход в Интернет);
- помещения для проведения семинарских, практических и лабораторных занятий (оборудованные учебной мебелью, видеопроекционным оборудованием для презентаций, средствами звуковоспроизведения, экраном, и имеющие выход в Интернет, компьютерная техника оснащена специализированным программным обеспечением);
- имеется возможность замены оборудования его виртуальными аналогами;
- 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.

Университет обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства. Состав определен в рабочих программах дисциплин (модулей) и при необходимости обновляется.

Кадровое обеспечение

Реализация ОПОП бакалавриата обеспечивается научно-педагогическими кадрами, имеющими, как правило, базовое образование, соответствующее профилю преподаваемой дисциплины, и систематически занимающимися научной и (или) научно-методической деятельностью.

Не менее 70 процентов численности педагогических работников Университета, участвующих в реализации программы бакалавриата, и лиц, привлекаемых Университетом к реализации программы бакалавриата на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), ведут научную, учебно-методическую и (или) практическую работу, соответствующую профилю преподаваемой дисциплины (модуля).

Не менее 3 процентов численности педагогических работников Университета, участвующих в реализации программы бакалавриата, и лиц, привлекаемых Университетом к реализации программы бакалавриата на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), являются руководителями и (или) работниками иных организаций, осуществляющими трудовую деятельность в профессиональной сфере, соответствующей профессиональной деятельности, к которой готовятся выпускники (иметь стаж работы в данной профессиональной сфере не менее 3 лет).

Доля педагогических работников Университета (исходя из количества замещаемых ставок, приведенного к целочисленным значениям) составляет не менее 55 процентов от общего количества лиц, привлекаемых к реализации программы бакалавриата.

Не менее 50 процентов численности педагогических работников Университета и лиц, привлекаемых к образовательной деятельности Университетом на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), имеют ученую степень (в том числе ученую степень, полученную в иностранном государстве и признаваемую в Российской Федерации) и (или) ученое звание (в том числе ученое звание, полученное в иностранном государстве и признаваемое в Российской Федерации).

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 объёме 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.

Требования к применяемым механизмам оценки качества программы бакалавриата

Качество образовательной деятельности и подготовки обучающихся по программе бакалавриата определяется в рамках системы внутренней оценки, а также системы внешней оценки, в которой Университет принимает участие на добровольной основе.

В целях совершенствования программы бакалавриата Университет при проведении регулярной внутренней оценки качества образовательной деятельности и подготовки обучающихся по программе бакалавриата привлекает работодателей и (или) их объединения, иных юридических и (или) физических лиц, включая педагогических работников Университета.

В рамках внутренней системы оценки качества образовательной деятельности по программе бакалавриата обучающимся предоставляется возможность оценивания условий, содержания, организации и качества образовательного процесса в целом и отдельных дисциплин (модулей) и практик.

Внешняя оценка качества образовательной деятельности по программе бакалавриата в рамках процедуры государственной аккредитации осуществляется с целью подтверждения соответствия образовательной деятельности по программе бакалавриата требованиям ФГОС ВО.

Внешняя оценка качества образовательной деятельности и подготовки обучающихся по программе бакалавриата осуществляется в рамках профессионально-общественной аккредитации, проводимой работодателями, их объединениями, а также уполномоченными ими организациями, в том числе иностранными организациями, либо авторизованными национальными профессионально-общественными организациями, входящими в международные структуры, с целью признания качества и уровня подготовки выпускников, отвечающими требованиям профессиональных стандартов (при наличии), требованиям рынка труда к специалистам соответствующего профиля.

Результаты внешней оценки качества по направлению подготовки 10.03.01 «Информационная безопасность» подтверждаются наличием сертификатов: Сертификат о международном признании Рег. № ОАС РКИ 192-22; Сертификат профессионально-общественной аккредитации Рег. № ОАС ССТ 22-155.

Условия освоения образовательной программы обучающимися инвалидами и лицами с ограниченными возможностями здоровья

При адаптации основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 10.03.01 «Информационная безопасность» для обучения инвалидов и лиц с ограниченными возможностями здоровья (далее – «обучающиеся инвалиды и лица с ОВЗ») организация образовательного процесса должна осуществляться в соответствии с учебными планами, графиками учебного процесса, расписанием занятий с учетом психофизического развития, индивидуальных возможностей, состояния здоровья обучающихся с ОВЗ и Индивидуальным планом реабилитации инвалидов.

Образовательный процесс по образовательной программе для обучающихся инвалидов и лиц с ОВЗ в Университете может быть реализован в следующих формах:

- в общих учебных группах (совместно с другими обучающимися) без или с применением специализированных методов обучения;
- в специализированных учебных группах (совместно с другими обучающимися с данной нозологией) с применением специализированных методов и технических средств обучения;
- по индивидуальному плану (срок обучения может быть увеличен по их заявлению не более чем на 1 год по сравнению со сроком получения образования, установленным для соответствующей формы обучения);
- с применением электронного обучения, дистанционных образовательных технологий с возможностью приема-передачи информации в доступных для них формах.

В случае обучения обучающихся инвалидов и лиц с ОВЗ в общих учебных группах с применением специализированных методов обучения, выбор конкретной методики обучения определяется исходя из рационально-необходимых процедур обеспечения доступности образовательной услуги обучающимся инвалидам и лицам с ОВЗ с учетом содержания обучения, уровня профессиональной подготовки научно-педагогических работников, методического и материально-технического обеспечения, особенностей восприятия учебной информации обучающимися инвалидами и лицами с ОВЗ.

Университет предоставляет инвалидам и лицам с ОВЗ (по их заявлению) возможность обучения по образовательной программе, учитывающей особенности их психофизического развития, индивидуальных возможностей и при необходимости, обеспечивающей коррекцию нарушений развития и социальную адаптацию указанных лиц. Для инвалидов и лиц с ОВЗ Университет устанавливает особый порядок освоения дисциплин (модулей) по физической культуре и спорту с учетом состояния их здоровья.

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Порядок организации образовательного процесса для обучающихся инвалидов и лиц с ОВЗ, в том числе требования, установленные к оснащенности образовательного процесса по образовательной программе,

определены Положением об организации образовательной деятельности для инвалидов и лиц с ограниченными возможностями здоровья в действующей редакции.

6. Воспитательная работа и характеристика среды Университета, обеспечивающие развитие культурных, социальных и личностных качеств выпускников

Система воспитательной работы Университета направлена на создание условий для активной жизнедеятельности обучающихся, их гражданского самоопределения, профессионального становления и индивидуально-личностной самореализации в созидательной деятельности для удовлетворения потребностей в нравственном, культурном, интеллектуальном, социальном и профессиональном развитии.

К основным задачами воспитательной работы в Университете относятся:

- развитие мировоззрения и актуализация системы базовых ценностей личности;
- приобщение студенчества к общечеловеческим нормам морали, национальным устоям и академическим традициям;
- воспитание уважения к закону, нормам коллективной жизни, развитие гражданской и социальной ответственности;
- воспитание положительного отношения к труду, воспитание социально значимой целеустремленности и ответственности в деловых отношениях;
- обеспечение развития личности и ее социально-психологической поддержки, формирование личностных качеств, необходимых для эффективной профессиональной деятельности;
- выявление и поддержка талантливой молодежи, формирование организаторских навыков, творческого потенциала, вовлечение обучающихся в процессы саморазвития и самореализации;
- формирование культуры и этики профессионального общения;
- воспитание внутренней потребности личности в здоровом образе жизни, ответственного отношения к природной и социокультурной среде;
- повышение уровня культуры безопасного поведения;
- развитие личностных качеств и установок, социальных навыков и управленческими способностями.

В центре системы воспитательной работы – личность обучающегося. Преподаватели, заведующие кафедрами, сотрудники институтов и кураторы решают воспитательные задачи через учебную деятельность: содержание учебной дисциплины, методику преподавания, добросовестное отношение к своим обязанностям, желание помочь каждому обучающемуся, уважительное отношение к обучающимся, умение понять и выслушать каждого, а также заинтересованность в успехах обучающихся, объективность в оценке знаний, широту эрудиции, внешний вид, честность, формирование универсальных

навыков, что оказывает междисциплинарное комплексное влияние на воспитание личности обучающихся, формируется такая ситуация развития, где каждый обучающийся может актуализировать свои потенциальные личностные возможности и развить новые навыки.

Большое влияние на воспитание обучающегося оказывает внеучебная деятельность: кураторские часы, экскурсии, круглые столы, диспуты, культурно-массовые мероприятия, конкурсы, фестивали, выставки и соревнования - это обеспечивает присутственное формирование необходимых компетенция и жизненных установок. Участником воспитательного процесса в Университете также является Управление по воспитательной работе, которое состоит из Отдела социально-психологической поддержки, Отдела развития студенческого творчества, Отела организационно-массовой работы, которые осуществляют свою работу в соответствии с утвержденными положениями об их деятельности.

В Университете созданы условия для личностного, профессионального и физического развития обучающихся, формирования у них социально значимых, нравственных качеств, активной гражданской позиции и моральной ответственности за принимаемые решения. К основными направлениям воспитательной работы в Университете относится: гражданское, патриотическое, духовно-нравственное, культурно-просветительское, научно-образовательное, профессионально-трудовое, экологическое, физическое.

Приоритетным видам деятельности обучающихся в воспитательной системе является проектная и волонтерская (добровольческая) деятельность. Проектная деятельность имеет творческую, научно-исследовательскую и практико-ориентированную направленность, осуществляется на основе проблемного обучения и активизации интереса обучающихся, что вызывает потребность в большей самостоятельности обучающихся. Проектная технология способствует социализации обучающихся при решении задач проекта, связанных с удовлетворением потребностей общества. Добровольческая деятельность имеет широкий круг направлений созидательной деятельности, включающий традиционные формы взаимопомощи и самопомощи, официальное предоставление услуг и другие формы гражданского участия. Индивидуальное и групповое добровольчество через деятельность и адресную помощь способствуют социализации обучающихся и расширению социальных связей, самореализации инициатив обучающихся, развитию личностных и профессиональных качеств, освоению новых навыков. По инициативе обучающихся в университете создан и функционирует Волонтерский центр.

В Университете утверждена и реализуется общая рабочая программа воспитания обучающихся, ежегодно утверждается и выполняется календарный план воспитательной работы, функционируют студенческое самоуправление, развивается волонтерское движение, работают студенческие клубы по интересам, кружки научно-исследовательской направленности, творческие студии и спортивные секции.

Воспитательная работа со студентами сосредоточена на развитии потребности личности в достижении личностных успехов, реализации своих целей и задач, формирования самостоятельности, самоутверждения, развития самодостаточности личности, ее основных качеств, способствующих включение в различные сферы общественной жизнедеятельности, получения определенной специализации, профессионального развития и отражается рабочей программой воспитания в соответствии с календарным графиком воспитательной работы по направлению подготовки 10.03.01 «Информационная безопасность» (Приложение 4).

7. Нормативно-методическое обеспечение системы оценки качества освоения обучающимися ОПОП ВО по направлению подготовки 10.03.01«Информационная безопасность» (ФГОС)

В соответствии с ФГОС 3++ по направлению подготовки 10.03.01 «Информационная безопасность» (уровень бакалавриата) 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 обучающихся.

Обучающиеся в Университете по образовательным программам высшего образования, при промежуточной аттестации сдают в течение учебного года как правило не более 10 экзаменов и 12 зачетов.

Для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям соответствующей ОПОП ВО Университет 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 по направлению подготовки 10.03.01 «Информационная безопасность» включает в себя защиту выпускной квалификационной работы.

Требования к содержанию, объему и структуре выпускной квалификационной работы, а также рекомендованные тематики, определяются методическими указаниями по выполнению выпускной квалификационной работы. Все выпускные квалификационные работы проходят проверку в системе «Антиплагиат» в соответствии с Положением о проверке выпускных квалификационных работ обучающихся в ФГБОУ ВО «Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова» с помощью системы «Антиплагиат».

Сроки подготовки и графики защиты выпускной квалификационной работы устанавливаются ежегодно в соответствии рабочим учебным планом.

При необходимости обучающимся предоставляется дополнительное время для подготовки.

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 педагогических работников, относящихся к профессорско-преподавательскому составу;
- Положение о рейтинговой оценке деятельности педагогических работников, относящихся к профессорско-преподавательскому составу, кафедр и основных профессиональных образовательных программ в ФГБОУ ВО «Технологический университет»;
- Положение об оценке эффективности деятельности педагогических работников, относящихся к профессорско-преподавательскому составу;
- Положение о порядке проведения аттестации работников, занимающих должности педагогических работников, относящихся к профессорско-преподавательскому составу ФГБОУ ВО «Технологический университет».

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, ФГБОУ ВО «Технологический университет» опирается в первую очередь на тех обучающихся, аспирантов и преподавателей, которые готовы представлять вуз на международной арене. С 2010 года в Университете начато обучение иностранных студентов. В настоящее время в ФГБОУ ВО «Технологический университет» по различным формам обучаются студенты из Туркменистана, Украины, Армении, Таджикистана, Азербайджана, Беларуси, Молдовы, Казахстана, Киргизии, Узбекистана, Латвии, Грузии. С целью более активной интернационализации иностранных граждан в Университете проводится Фестиваль национальных культур, организуются экскурсии по Москве и Подмосковью.

Академическая мобильность обучающихся, профессорско-преподавательского и административного штата вуза осуществляется в рамках двухсторонних межвузовских соглашений с зарубежными партнерами, а также грантовых программ по линии Министерства науки и высшего образования 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 Университета также выезжают в зарубежные вузы.

Академическая мобильность обучающихся 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 обучающиеся, прошедшие обучение в Университете, хотели бы вернуться сюда еще раз.

Технологический университет с 2013 года проводит международную конференцию по обмену опытом в сфере высшего образования и международной деятельности. Вместе с развитием университета, с ростом его образовательного, научного, интеграционного потенциала, росло его признание среди российских и зарубежных партнеров. Укреплялись международные связи вуза, и наша конференция стала важным инструментом формирования партнерства на международной образовательной арене. За 10 лет в работе конференции приняли участие преподаватели и студенты более чем из 40 стран мира, среди них как страны постсоветского пространства, это Азербайджан, Армения, Беларусь, Грузия, Казахстан, Кыргызстан, Молдавия, Туркменистан, Узбекистан, так и представители Чехии, Австрии, Словакии,

Болгарии, Швейцарии, Германии, Испании, Финляндии, Норвегии, Хорватии, Румынии, Албании, Северной Македонии, Греции, Кубы, Вьетнама, Индии и Филиппин. За все время в сборниках трудов конференции Технологического университета опубликовано более 900 статей отечественных и зарубежных авторов.

Заключены рамочные соглашения с рядом высших учебных заведений Бангладеш, Беларусь, Казахстан, Киргизия, Сербия, Турция, Узбекистан и других стран мира. В рамках подписанных соглашений обучающиеся проходят языковые стажировки за рубежом, реализуются совместные научно-образовательные проекты. По приглашению зарубежных партнеров сотрудники Университета принимают участие в научных конференциях, выступая с докладами, и публикуют статьи в научных сборниках.

С целью продвижения российского образования за рубежом ФГБОУ ВО «Технологический университет» активно участвует в международных выставках образования в странах СНГ как очно, так и заочно, организует Дни открытых дверей и круглые столы на площадках в различных странах. Такие мероприятия способствуют привлечению иностранных граждан к получению высшего образования в Российской Федерации.

В настоящее время партнёрами университета являются: Международный университет Даффодил (Бангладеш, г. Дакка), Барановичский государственный университет (Беларусь г. Барановичи), Витебский государственный технологический университет (Беларусь г. Витебск), Гродненский государственный колледж техники, технологий и дизайна (Беларусь г. Гродно), Белорусский государственный университет (Беларусь г. Минск), Белорусский государственный университет информатики и радиоэлектроники (Беларусь г. Минск), Евразийский национальный университет им. Л.Н. Гумилева, Кыргызский экономический университет им. М. Рыскулбекова (Киргизия г. Бишкек), Кыргызский национальный университет им. Ж. Баласагына (Киргизия г. Бишкек), Хесус Монтане Оропеса Университет Исла-де-ла-Ювентуд (Куба), Нишский университет (Сербия г. Ниш), Университет Мармара (Турция г. Стамбул), Фатих Султан Мехмет Вакиф университет (Турция г. Стамбул), Адыяманский университет (Турция г. Адыяман), Наманганский инженерно-технологический институт (Узбекистан г. Наманган), Наманганский инженерно-строительный институт (Узбекистан г. Наманган).

Перечень приложений

Приложение 1. Календарный учебный график.

Приложение 2. Учебный план.

Приложение 3. Описание и матрица реализации практической подготовки обучающихся.

Приложение 4. Рабочая программа воспитания и календарный план воспитательной работы.

Приложение 5. Программа учебной практики (ознакомительная практика, учебно-лабораторная).

Приложение 6. Программа производственной практики (технологическая практика, преддипломная практика).

Приложение 7. Методические рекомендации по написанию Выпускной Квалификационной Работы

Фонд оценочных средств по дисциплинам учебного плана в полном объеме представлен на образовательном портале Университета – https://ies.unitech-mo.ru/

Приложение 1. Календарный учебный график (очная форма)

Учебный план бакалавриата 10.03.01 ИБО-ОТЗИ-2023 Информационная безопасность

Календарный учебный график

Мес	Сентябрь					Октябрь					Ноябрь					Декабрь					Январь					Февраль					Март					Апрель					Май					Июнь					Июль					Август	
Нед.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
I																	Э	*	Э	Э	Э	К	К	У	У	У	У	У	У	У	У	У	У	У	*	У	У	У	Э	Э	Э	Э	К	К	К	К	К	К	К	К	К	К
II																	Э	*	Э	Э	Э	К	К	У	У	У	У	У	У	У	У	У	У	У	*	У	У	У	Э	Э	Э	Э	У	У	К	К	К	К	К	К	К	К
III																	Э	*	Э	Э	Э	К	К													*				Э	Э	Э	Э	П	П	К	К	К	К	К	К	К	К
IV																	Э	*	Э	Э	Э	К																		Э	Э	Э	Э	К	К	К	К	К	К	К	К	К	К

Сводные данные

		Курс 1			Курс 2			Курс 3			Курс 4			Итого
		Сем. 1	Сем. 2	Всего	Сем. 3	Сем. 4	Всего	Сем. 5	Сем. 6	Всего	Сем. 7	Сем. 8	Всего	
Т	Теоретическое обучение и практики	16	16	32	16	16	32	16	16	32	16	6	22	118
Э	Экзаменационные сессии	4	4	8	4	4	8	4	4	8	4	2	6	30
У	Учебная практика				2		2							2
П	Производственная практика							2		2		6	6	8
Д	Подготовка к процедуре защиты и квалификационной работы										6		6	6
К	Каникулы	2	8	10	2	6	8	2	6	8	1	9	10	36
*	Нерабочие праздничные дни (не включая воскресенья)	1 (6 дн)	1 (6 дн)	2 (12 дн)	1 (6 дн)	1 (6 дн)	2 (12 дн)	1 (6 дн)	1 (6 дн)	2 (12 дн)	1 (6 дн)	1 (6 дн)	2 (12 дн)	8 (48 дн)
	Продолжительность обучения (не включая нерабочие праздничные дни и каникулы)	более 39 нед.			более 39 нед.			более 39 нед.			более 39 нед.			
	Итого	23	29	52	23	29	52	23	29	52	27	30	52	208

Календарный учебный график (очно-заочная форма)

Учебный план бакалавриата 10.03.01 ИБЗ-ОТЗИ-2023

Календарный учебный график

Мес	Сентябрь					Октябрь				Ноябрь				Декабрь				Январь				Февраль				Март				Апрель				Май				Июль				Июль				Август			
Нед	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
I					Э				Э					Э			*			Э	К	К					Э				Э			*			Э				Э	К	К	К	К	К	К	К	К
II					Э				Э					Э			*			Э	К	К					Э				Э			*			Э				Э	У	У	К	К	К	К	К	К
III					Э				Э					Э			*			Э	К	К					Э				Э			*			Э				Э	У	У	К	К	К	К	К	К
IV					Э				Э					Э			*			Э	К	К					Э				Э			*			Э				Э	П	П	К	К	К	К	К	К
V					Э				Э					Э			*			Э	К	К					Э			П	П	П	П	*	П	Д	Д	Д	Д	Д	К	К	К	К	К	К	К	К

Сводные данные

		Курс 1			Курс 2			Курс 3			Курс 4			Курс 5			Итого
		Сем. 1	Сем. 2	Всего	Сем. 3	Сем. 4	Всего	Сем. 5	Сем. 6	Всего	Сем. 7	Сем. 8	Всего	Сем. 9	Сем. A	Всего	
	Теоретическое обучение	16	16	32	16	16	32	16	16	32	16	16	32	16	6	22	150
Э	Экзаменационные сессии	4	4	8	4	4	8	4	4	8	4	4	8	4	2	6	38
У	Учебная практика				2		2	2		2							4
П	Производственная практика										2		2	6		6	8
Д	Подготовка к процедуре защиты и защита выпускной квалификационной работы													6	6	6	6
К	Каникулы	2	8	10	2	6	8	2	6	8	2	6	8	1	9	10	44
*	Нерабочие праздничные дни (не включая воскресенья)	1 (6 дн)	1 (6 дн)	2 (12 дн)	1 (6 дн)	1 (6 дн)	2 (12 дн)	1 (6 дн)	1 (6 дн)	2 (12 дн)	1 (6 дн)	1 (6 дн)	2 (12 дн)	1 (6 дн)	1 (6 дн)	2 (12 дн)	10 (60 дн)
	Продолжительность обучения (не включая нерабочие праздничные дни и каникулы)	более 39 нед.			более 39 нед.			более 39 нед.			более 39 нед.			более 39 нед.			
	Итого	23	29	52	23	29	52	23	29	52	23	29	52	22	30	52	260

Приложение 2. Учебный план (очная форма)

Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования «Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова»

План одобрен Ученым советом вуза

Протокол № 9 от 11.04.2023

УТВЕРЖДАЮ

И.о. ректора *Старцев В.А.*

«11» 04 2023 г.

УЧЕБНЫЙ ПЛАН

по программе бакалавриата

10.03.01

Направление Информационная безопасность

Профиль: "Организация и технологии защиты информации" (по отрасли или в сфере профессиональной деятельности)

Кафедра: Информационной безопасности

Институт: Инфокоммуникационных систем и технологий

Квалификация: бакалавр

Форма обучения: Очная
Срок получения образования: 4г

Основной	*Типы задач профессиональной деятельности*
+	эксплуатационный
+	проектно-технологический
+	экспериментально-исследовательский
+	организационно-управленческий

Год начала подготовки (по учебному плану) 2023

Образовательный стандарт (ФГОС) № 1427 от 17.11.2020

СОГЛАСОВАНО

Проректор по учебно-методической работе / Бабина Н.В./

Начальник учебно-методического управления / Тришкина Т.В./

Директор института / Парафейников И.В./

Зав. кафедрой / Соляной В.Н./

План Учебный план бакалавриата 10.03.01 ИБО-ОТЗИ-2023

-	-	Форма контроля						з.е.	Итого акад.часов									Курс 1		Курс 2		Курс 3		Курс 4		-
Индекс	Наименование	Экзамен	Зачет	Зачет с оц.	КП	КР	Контр.	Факт	По плану	Конт. раб.	Ауд.	Лек	Лаб	Пр	СР	Интер часы	Пр. подгот	Итого	Ауд.	Итого	Ауд.	Итого	Ауд.	Итого	Ауд.	Компетенции
Блок 1.Дисциплины (модули)								213	8104	4172	3494	1252	240	2002	3932	773	124	2116	934	2288	1044	2188	928	1512	588	
Обязательная часть								155	6016	3144	2674	952	208	1514	2872	555		1684	758	1820	884	1324	576	1188	456	
Б1.О.01	Философия	2					2	4	144	58	48	16		32	86	12		144	48							УК-1; ОПК-8
Б1.О.02	История России	3		2			23	4	144	128	128	64		64	16	32		72	64	72	64					УК-1; УК-5
Б1.О.03	Основы российской государственности		1				1	2	72	64	54	18		36	8	12		72	54							УК-5
Б1.О.04	Иностранный язык	24	13				1234	10	360	168	128			128	192	10		216	64	144	64					УК-4; ОПК-8
Б1.О.05	Безопасность жизнедеятельности		1				1	3	108	42	32	16		16	66	8		108	32							УК-7; УК-8
Б1.О.06	Физическая культура		2					2	72	48	48	16		32	24	4		72	48							УК-7
Б1.О.07	Русский язык и культура речи		1				1	2	72	42	32	16		16	30	8		72	32							УК-4; УК-5; ОПК-8
Б1.О.08	Основы управленческой деятельности		1				1	3	108	42	32	16		16	66	8		108	32							УК-6; УК-9; ОПК-1; ОПК-5
Б1.О.09	Документоведение		1				1	2	72	42	32	16		16	30	8		72	32							ОПК-8; ОПК-10
Б1.О.10	Экономика предприятия и организация производства	23					23	6	216	116	96	32		64	100	8		108	48	108	48					УК-9; ОПК-12
Б1.О.11	**Группа учебных дисциплин (модулей) "Математические основы обеспечения информационной безопасности":**	**1234**	**35**	**3**			**12333 45**	**21**	**756**	**422**	**352**	**144**		**208**	**334**	**42**		**252**	**128**	**432**	**192**	**72**	**32**			**УК-1; ОПК-3; ОПК-11**
Б1.О.11.01	Линейная алгебра и аналитическая геометрия	1					1	3	108	74	64	32		32	34	12		108	64							УК-1; ОПК-3
Б1.О.11.02	Математический анализ	2					2	4	144	74	64	32		32	70	8		144	64							УК-1; ОПК-3
Б1.О.11.03	Теория графов	3					3	3	108	58	48	16		32	50	4				108	48					УК-1; ОПК-3
Б1.О.11.04	Теория информации			3			3	3	108	58	48	16		32	50	2				108	48					УК-1; ОПК-3
Б1.О.11.05	Теория вероятностей и математическая статистика	4	3				34	6	216	116	96	32		64	100	12				216	96					ОПК-3; ОПК-11
Б1.О.11.06	Дискретная математика		5				5	2	72	42	32	16		16	30	4						72	32			УК-1; ОПК-3
Б1.О.12	**Группа учебных дисциплин (модулей) "Физико-технические основы обеспечения информационной безопасности":**	**3**	**245**				**2345**	**12**	**432**	**296**	**256**	**96**	**48**	**112**	**136**	**48**		**108**	**48**	**216**	**128**	**108**	**80**			**УК-1; ОПК-4; ОПК-11**
Б1.О.12.01	Физика	3	2				23	6	216	116	96	32	16	48	100	12		108	48	108	48					ОПК-4; ОПК-11
Б1.О.12.02	Электротехника		4				4	3	108	90	80	32	16	32	18	18				108	80					УК-1; ОПК-4
Б1.О.12.03	Электроника и схемотехника		5				5	3	108	90	80	32	16	32	18	18						108	80			УК-1; ОПК-4
Б1.О.13	**Группа учебных дисциплин (модулей) "Информационные технологии":**	**14566**	**5**				**14556 6**	**21**	**756**	**364**	**304**	**112**	**64**	**128**	**392**	**93**		**144**	**64**	**108**	**48**	**504**	**192**			**УК-1; ОПК-2; ОПК-7; ОПК-9**
Б1.О.13.01	Информатика	1					1	4	144	74	64	16	16	32	70	18		144	64							УК-1; ОПК-7
Б1.О.13.02	Языки программирования	4					4	3	108	58	48	16		32	50	12				108	48					УК-1; ОПК-7
Б1.О.13.03	Технологии и методы программирования	5					5	3	108	58	48	16	16	16	50	9						108	48			УК-1; ОПК-7
Б1.О.13.04	Информационные технологии		5				5	3	108	42	32	16		16	66	18						108	32			УК-1; ОПК-2
Б1.О.13.05	Аппаратные средства вычислительной техники	6					6	4	144	58	48	16	16	16	86	18						144	48			УК-1; ОПК-2
Б1.О.13.06	Сети и системы передачи информации	6					6	4	144	74	64	32	16	16	70	18						144	64			УК-1; ОПК-9
Б1.О.14	**Группа учебных дисциплин (модулей) "Методы и средства обеспечения информационной безопасности":**	**4678**	**2677**	**3**		**4678**	**23677**	**30**	**1080**	**524**	**440**	**188**	**32**	**220**	**556**	**120**		**72**	**32**	**252**	**112**	**252**	**112**	**504**	**184**	**УК-1; ОПК-1; ОПК-5; ОПК-6; ОПК-8; ОПК-9; ОПК-10; ОПК-12; ДОПК-3**
Б1.О.14.01	Основы информационной безопасности		2	3			23	4	144	84	64	32		32	60	18		72	32	72	32					ОПК-1; ОПК-6; ОПК-8
Б1.О.14.02	Организационное и правовое обеспечение информационной безопасности	4				4		5	180	86	80	32		48	94	12				180	80					ОПК-5; ОПК-6
Б1.О.14.03	Основы управления информационной безопасностью		6				6	3	108	58	48	16		32	50	12						108	48			ОПК-5; ОПК-10
Б1.О.14.04	Защита информации от утечки по техническим каналам	6				6		4	144	74	64	32	16	16	70	18						144	64			УК-1; ОПК-6
Б1.О.14.05	Методы и средства криптографической защиты информации		7				7	3	108	58	48	16		32	50	12								108	48	УК-1; ОПК-9
Б1.О.14.06	Программно-аппаратные средства защиты информации	7				7		3	108	58	48	16	16	16	50	18								108	48	ОПК-6; ОПК-10; ОПК-12
Б1.О.14.07	Комплексное обеспечение защиты информации объекта информатизации (предприятия)	8	7			8	7	8	288	106	88	44		44	182	30								288	88	ОПК-8; ОПК-12; ДОПК-3
Б1.О.15	**Дисциплины (модули) профиля: "Организация и технология защиты информации" (по отрасли или в сфере профессиональной деятельности)**	**45577 8**	**48**	**7**			**44557 7788**	**33**	**1188**	**560**	**464**	**168**	**64**	**232**	**628**	**126**				**252**	**96**	**252**	**96**	**684**	**272**	**УК-1; УК-9; ОПК-3; ДОПК-1; ДОПК-2; ДОПК-3; ДОПК-4**
Б1.О.15.01	Математическая логика и теория алгоритмов		4				4	3	108	42	32	16		16	66	12				108	32					УК-1; ОПК-3
Б1.О.15.02	Информационные процессы и системы как объекты информационной безопасности	4					4	4	144	84	64	32		32	60	12				144	64					ДОПК-1; ДОПК-2; ДОПК-4
Б1.О.15.03	Конфиденциальное делопроизводство и защищенный электронный документооборот	5					5	4	144	58	48	16	16	16	86	18						144	48			ДОПК-1; ДОПК-3
Б1.О.15.04	Нормативные акты и стандарты по информационной безопасности	5					5	3	108	58	48	16	16	16	50	12						108	48			ДОПК-2; ДОПК-3; ДОПК-4

План Учебный план бакалавриата 10.03.01 ИБО-ОТЗИ-2023

-	-	Форма контроля						з.е.	Итого акад.часов									Курс 1		Курс 2		Курс 3		Курс 4		-
Индекс	Наименование	Экзамен	Зачет	Зачет с оц.	КП	КР	Контр.	Факт	По плану	Конт. раб.	Ауд.	Лек	Лаб	Пр	СР	Интер часы	Пр. подгот	Итого	Ауд.	Итого	Ауд.	Итого	Ауд.	Итого	Ауд.	Компетенции
Б1.О.15.05	Организация системы обеспечения информационной безопасности (служба ИБ)			7			7	4	144	74	64	32		32	70	18								144	64	ДОПК-1; ДОПК-2
Б1.О.15.06	Физическая защита информационных объектов	7					7	4	144	58	48	16	16	16	86	18								144	48	ДОПК-1; ДОПК-3
Б1.О.15.07	Информационно-аналитическая деятельность по обеспечению комплексной безопасности	7					7	4	144	74	64	16	16	32	70	18								144	64	ДОПК-1; ДОПК-2
Б1.О.15.08	Экономика информационной безопасности	8					8	4	144	56	48	12		36	88	6								144	48	УК-9; ДОПК-2; ДОПК-3; ДОПК-4
Б1.О.15.09	Моделирование процессов и систем защиты информации		8				8	3	108	56	48	12		36	52	12								108	48	ДОПК-1; ДОПК-4
Б1.О.16	Элективные курсы по физической культуре и спорту		13456						328	160	160			160	168			64	32	128	64	136	64			УК-7
Б1.О.17	Основы военной подготовки		3						108	68	68	34		34	40	16				108	68					УК-7; УК-8
Часть, формируемая участниками образовательных отношений								58	2088	1028	820	300	32	488	1060	218	124	432	176	468	160	864	352	324	132	
Б1.В.01	**Дисциплины (модули) образовательной организации:**	**13**	**337**	**45**			**13334 57**	**19**	**684**	**310**	**240**	**80**	**16**	**144**	**374**	**54**		**108**	**32**	**360**	**112**	**108**	**48**	**108**	**48**	**УК-2; УК-5; УК-7; УК-10; ПК-1; ПК-2; ПК-3; ПК-4; ПК-5**
Б1.В.01.01	Основы исследований информационной безопасности	1					1	3	108	42	32	16		16	66	9		108	32							УК-2; УК-10; ПК-1; ПК-2; ПК-3
Б1.В.01.02	Пакеты прикладных программ	3					3	4	144	58	48	16		32	86	12				144	48					ПК-2; ПК-4
Б1.В.01.03	Социально-психологические основы управленческой деятельности		3				3	2	72	42	32	16		16	30	6				72	32					УК-2; ПК-3
Б1.В.01.04	Основы конкурентной разведки		3	4			34	4	144	52	32			32	92	6				144	32					УК-2; ПК-4
Б1.В.01.05	История защиты информации в РФ			5			5	3	108	58	48	16		32	50	9						108	48			УК-5; ПК-3
Б1.В.01.06	Информационная безопасность автоматизированных систем		7				7	3	108	58	48	16	16	16	50	12								108	48	ПК-3; ПК-5
Б1.В.02	Основы права	1					1	3	108	58	48	16		32	50	9	8	108	48							УК-5; ПК-1
Б1.В.03	Безопасность информационных технологий			6			6	3	108	42	32	16		16	66	8						108	32			УК-1; ПК-5
Б1.В.04	Гуманитарные аспекты (профессиональная этика) информационной безопасности		6				6	2	72	42	32	16		16	30	9	4					72	32			УК-1; ПК-3
Б1.В.ДВ.01	**Дисциплины по выбору Блок 1.В.ДВ.1**		**4**				**4**	**3**	**108**	**58**	**48**	**16**		**32**	**50**	**18**	**16**			**108**	**48**					**ПК-2; ПК-4**
Б1.В.ДВ.01.01	Операционные системы, среды и оболочки		4				4	3	108	58	48	16		32	50	18	16			108	48					ПК-2; ПК-4
Б1.В.ДВ.01.02	Базы данных, системы управления базами данных		4				4	3	108	58	48	16		32	50	18	16			108	48					ПК-1; ПК-4
Б1.В.ДВ.02	**Дисциплины по выбору Блок 1.В.ДВ.2**	**2**					**2**	**3**	**108**	**58**	**48**	**16**		**32**	**50**	**9**	**8**	**108**	**48**							**ПК-1; ПК-4**
Б1.В.ДВ.02.01	Основы алгоритмизации и программирования	2					2	3	108	58	48	16		32	50	9	8	108	48							ПК-1; ПК-4
Б1.В.ДВ.02.02	Пакеты прикладных математических программ	2					2	3	108	58	48	16		32	50	9	8	108	48							ПК-1; ПК-4
Б1.В.ДВ.03	**Дисциплины по выбору Блок 1.В.ДВ.3**	**5**					**5**	**3**	**108**	**42**	**32**	**16**		**16**	**66**	**12**	**8**					**108**	**32**			**ПК-1; ПК-2**
Б1.В.ДВ.03.01	Информационная безопасность кредитно-финансовых операций	5					5	3	108	42	32	16		16	66	12	8					108	32			ПК-1; ПК-2
Б1.В.ДВ.03.02	Защищенные электронные технологии банка	5					5	3	108	42	32	16		16	66	12	8					108	32			ПК-1; ПК-2
Б1.В.ДВ.03.03	Подготовка объекта информатизации к аттестации по требованиям безопасности информации (ООО "НОВО")	5					5	3	108	42	32	16		16	66	12	8					108	32			ПК-1; ПК-2
Б1.В.ДВ.03.04	Аттестация объекта информатизации по требованиям безопасности информации (ООО "ЦБИ"	5					5	3	108	42	32	16		16	66	12	8					108	32			ПК-1; ПК-2
Б1.В.ДВ.04	**Дисциплины по выбору Блок 1.В.ДВ.4**			**5**			**5**	**3**	**108**	**58**	**48**	**16**	**16**	**16**	**50**	**12**						**108**	**48**			**ПК-2; ПК-3**
Б1.В.ДВ.04.01	Информационно-психологическая безопасность персонала предприятия			5			5	3	108	58	48	16	16	16	50	12						108	48			ПК-2; ПК-3
Б1.В.ДВ.04.02	Защита общества от информации, запрещенной к распространению			5			5	3	108	58	48	16	16	16	50	12						108	48			ПК-2; ПК-3
Б1.В.ДВ.04.03	Организация защиты конфиденциальной информации от несанкционированного доступа (ООО "НОВО")			5			5	3	108	58	48	16	16	16	50	12						108	48			ПК-2; ПК-3
Б1.В.ДВ.04.04	Защита информации от НСД (ООО "ЦБИ")			5			5	3	108	58	48	16	16	16	50	12						108	48			ПК-2; ПК-3
Б1.В.ДВ.05	**Дисциплины по выбору Блок 1.В.ДВ.5**		**6**				**6**	**2**	**72**	**42**	**32**	**16**		**16**	**30**	**12**	**12**					**72**	**32**			**ПК-3; ПК-4**
Б1.В.ДВ.05.01	Разработка политики информационной безопасности в организациях		6				6	2	72	42	32	16		16	30	12	12					72	32			ПК-3; ПК-4
Б1.В.ДВ.05.02	Разработка политики информационной безопасности в Интернет-системах		6				6	2	72	42	32	16		16	30	12	12					72	32			ПК-3; ПК-4
Б1.В.ДВ.05.03	Оценка защищенности конфиденциальной информации по техническим каналам и от несанкционированного доступа (ООО "НОВО")		6				6	2	72	42	32	16		16	30	12	12					72	32			ПК-1; ПК-3; ПК-4
Б1.В.ДВ.05.04	Контроль защищенности информации от утечки по техническим каналам (ООО "ЦБИ")		6				6	2	72	42	32	16		16	30	12	12					72	32			ПК-1; ПК-3; ПК-4
Б1.В.ДВ.06	**Дисциплины по выбору Блок 1.В.ДВ.6**	**7**					**7**	**4**	**144**	**58**	**48**	**16**		**32**	**86**	**18**	**12**							**144**	**48**	**ПК-3; ПК-4**

План Учебный план бакалавриата 10.03.01 ИБО-ОТЗИ-2023

-	-	Форма контроля						з.е.	Итого акад.часов									Курс 1		Курс 2		Курс 3		Курс 4		-
Индекс	Наименование	Экзамен	Зачет	Зачет с оц.	КП	КР	Контр.	Факт	По плану	Конт. раб.	Ауд.	Лек	Лаб	Пр	СР	Интер часы	Пр. подгот	Итого	Ауд.	Итого	Ауд.	Итого	Ауд.	Итого	Ауд.	Компетенции
Б1.В.ДВ.06.01	Организация защиты персональных данных на предприятии	7					7	4	144	58	48	16		32	86	18	12							144	48	ПК-3; ПК-4
Б1.В.ДВ.06.02	Правовая охрана результатов интеллектуальной деятельности	7					7	4	144	58	48	16		32	86	18	12							144	48	ПК-3; ПК-4
Б1.В.ДВ.06.03	Методы и средства защиты информации от утечки по техническим каналам (ООО "НОВО")	7					7	4	144	58	48	16		32	86	18	12							144	48	ПК-1; ПК-3; ПК-4
Б1.В.ДВ.06.04	Средства защиты информации и оценка эффективности защиты от утечки по техническим каналам (ООО "ЦБИ")	7					7	4	144	58	48	16		32	86	18	12							144	48	ПК-1; ПК-3; ПК-4
Б1.В.ДВ.07	**Дисциплины по выбору Блок 1.В.ДВ.7**		**6**				**6**	**2**	**72**	**42**	**32**	**16**		**16**	**30**	**9**	**12**					**72**	**32**			**ПК-4; ПК-5**
Б1.В.ДВ.07.01	Защита профессиональной тайны в различных сферах деятельности		6				6	2	72	42	32	16		16	30	9	12					72	32			ПК-4; ПК-5
Б1.В.ДВ.07.02	Информационная безопасность операционных систем и баз данных		6				6	2	72	42	32	16		16	30	9	12					72	32			ПК-4; ПК-5
Б1.В.ДВ.07.03	Технические каналы утечки конфиденциальной информации (ООО "НОВО")		6				6	2	72	42	32	16		16	30	9	12					72	32			ПК-4; ПК-5
Б1.В.ДВ.07.04	Технические каналы утечки информации (ООО "ЦБИ")		6				6	2	72	42	32	16		16	30	9	12					72	32			ПК-4; ПК-5
Б1.В.ДВ.08	**Дисциплины по выбору Блок 1.В.ДВ.8**		**8**				**8**	**2**	**72**	**44**	**36**	**12**		**24**	**28**	**18**	**12**							**72**	**36**	**ПК-4; ПК-5**
Б1.В.ДВ.08.01	Лицензирование и сертификация в области защиты информации		8				8	2	72	44	36	12		24	28	18	12							72	36	ПК-4; ПК-5
Б1.В.ДВ.08.02	Аттестация в области защиты информации		8				8	2	72	44	36	12		24	28	18	12							72	36	ПК-4; ПК-5
Б1.В.ДВ.08.03	Разработка объекта информатизации в защищенном исполнении (ООО "НОВО")		8				8	2	72	44	36	12		24	28	18	12							72	36	ПК-2; ПК-4; ПК-5
Б1.В.ДВ.08.04	Разработка и сертификация средств защиты информации и технических средств в защищенном исполнении (ООО "ЦБИ")		8				8	2	72	44	36	12		24	28	18	12							72	36	ПК-4; ПК-5
Б1.В.ДВ.09	**Дисциплины по выбору Блок 1.В.ДВ.9**		**5**				**5**	**3**	**108**	**58**	**48**	**16**		**32**	**50**	**12**						**108**	**48**			**ПК-3; ПК-5**
Б1.В.ДВ.09.01	Радиоэлектронные системы и средства как объекты информационной безопасности		5				5	3	108	58	48	16		32	50	12						108	48			ПК-3; ПК-5
Б1.В.ДВ.09.02	Основы радиоэлектронной разведки (РЭР)		5				5	3	108	58	48	16		32	50	12						108	48			ПК-3; ПК-5
Б1.В.ДВ.09.03	Методы и средства защиты информации от несанкционированного доступа (ООО "НОВО")		5				5	3	108	58	48	16		32	50	12						108	48			ПК-1; ПК-3; ПК-5
Б1.В.ДВ.09.04	Методы и средства обеспечения защищенности информации от несанкционированного доступа (ООО "ЦБИ")		5				5	3	108	58	48	16		32	50	12						108	48			ПК-1; ПК-3; ПК-5
Б1.В.ДВ.10	**Дисциплины по выбору Блок 1.В.ДВ.10**	**6**					**6**	**3**	**108**	**58**	**48**	**16**		**32**	**50**	**9**	**16**					**108**	**48**			**ПК-1; ПК-2; ПК-3**
Б1.В.ДВ.10.01	Социотехносферная безопасность объектов информационной защиты	6					6	3	108	58	48	16		32	50	9	16					108	48			ПК-1; ПК-2; ПК-3
Б1.В.ДВ.10.02	Эффективность защищенных информационных систем	6					6	3	108	58	48	16		32	50	9	16					108	48			УК-9; ПК-1; ПК-2; ПК-4
Б1.В.ДВ.10.03	Методы и средства выявления демаскирующих признаков закладочных устройств в защищаемых помещениях (ООО "НОВО", ООО "ЦБИ")	6					6	3	108	58	48	16		32	50	9	16					108	48			ПК-2; ПК-4; ПК-5
Б1.В.ДВ.11	**Дисциплины по выбору Блок 1.В.ДВ.11**			**1**				**3**	**108**	**58**	**48**	**16**		**32**	**50**	**9**	**16**	**108**	**48**							**УК-5; ПК-1**
Б1.В.ДВ.11.01	Введение в профессию			1				3	108	58	48	16		32	50	9	16	108	48							УК-5; ПК-1
Б1.В.ДВ.11.02	Профессиональные адаптации инвалидов и лиц с ОВЗ			1				3	108	58	48	16		32	50	9	16	108	48							УК-6; ПК-1
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.Практика								18	648	16	16			16	632			108	16	108		108		324		
Обязательная часть								9	324						324									324		
Б2.О.01(П)	Преддипломная практика			8				9	324						324									324		ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ДОПК-1; ДОПК-2; ДОПК-3; ДОПК-4
Часть, формируемая участниками образовательных отношений								9	324	16	16			16	308			108	16	108		108				
Б2.В.01(У)	Ознакомительная практика			2				3	108	16	16			16	92			108	16							УК-1; УК-2; УК-3; УК-6; УК-9; ПК-1; ПК-2; ПК-3
Б2.В.02(У)	Учебно-лабораторная практика			4				3	108						108					108						ПК-1; ПК-2; ПК-3; ПК-4
Б2.В.03(П)	Технологическая практика			6				3	108						108							108				ПК-1; ПК-2; ПК-3; ПК-4; ПК-5
Блок 3.Государственная итоговая аттестация								9	324						324									324		
Б3.01(Д)	Подготовка и защита ВКР							9	324						324									324		УК-1; УК-2; УК-3; УК-4; УК-5; УК-6; УК-7; УК-8; УК-9; УК-10; ОПК-1; ОПК-2; ОПК-3; ОПК-4; ОПК-5; ОПК-6; ОПК-7; ОПК-8; ОПК-9; ОПК-10; ОПК-11; ОПК-12; ОПК-13; ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ДОПК-1; ДОПК-2; ДОПК-3; ДОПК-4
ФТД.Факультативные дисциплины								6	216	104	80			80	112	20						144	48	72	32	

План Учебный план бакалавриата 10.03.01 ИБО-ОТЗИ-2023

-	-	Форма контроля						з.е.	Итого акад.часов									Курс 1		Курс 2		Курс 3		Курс 4		-
Индекс	Наименование	Экзамен	Зачет	Зачет с оц.	КП	КР	Контр.	Факт	По плану	Конт. раб.	Ауд.	Лек	Лаб	Пр	СР	Интер часы	Пр. подгот	Итого	Ауд.	Итого	Ауд.	Итого	Ауд.	Итого	Ауд.	Компетенции
ФТД.01	Технико-экономическое обоснование проекта		5					2	72	24	16			16	48	4						72	16			УК-2; УК-10; ПК-5
ФТД.02	Разработка и реализация проекта		6	7	7			4	144	80	64			64	64	16						72	32	72	32	УК-1; УК-2; УК-3; УК-10; ПК-2; ПК-5
	Итого з.е./Акад.часов (без факультативов)							240	9076	4188	3510	1252	240	2018	4888	773	124	2224	950	2396	1044	2296	928	2160	588	

Учебный план (очно-заочная форма)

Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования «Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова»

План одобрен Ученым советом вуза

Протокол № 9 от 12.04.2022

УЧЕБНЫЙ ПЛАН

по программе бакалавриата

10.03.01

Направление Информационная безопасность

Профиль: "Организация и технологии защиты информации" (по отрасли или в сфере профессиональной деятельности)

Кафедра: Информационной безопасности

Институт: Международного и дистанционного образования

УТВЕРЖДАЮ

И.о. ректора Кочетов В.А.

11.07.2023

Квалификация: бакалавр

Форма обучения: Очно-заочная
Срок получения образования: 5л

Основной	*Типы задач профессиональной деятельности*
+	эксплуатационный
+	проектно-технологический
+	экспериментально-исследовательский
+	организационно-управленческий

Год начала подготовки (по учебному плану) 2023

Образовательный стандарт (ФГОС) № 1427 от 17.11.2020

СОГЛАСОВАНО

Проректор по учебно-методической работе *Бабина Н.В./*

Начальник учебно-методического управления *Тришкина Т.В./*

Директор института *Баширова С.В./*

Зав. кафедрой *Соляной В.Н./*

План Учебный план бакалавриата 10.03.01 ИБЗ-ОТЗИ-2023 Информационна

-	-	Форма контроля						з.е.	Итого акад.часов										Курс 1		Курс 2		Курс 3		Курс 4		Курс 5		-
Индекс	Наименование	Экзамен	Зачет	Зачет с оц.	КП	КР	Контр.	Факт	По плану	Конт. раб.	Ауд.	Лек	Лаб	Пр	СР	Интер часы	Пр. подгот		Итого	Ауд.	Итого	Ауд.	Итого	Ауд.	Итого	Ауд.	Итого	Ауд.	Компетенции
Блок 1 Дисциплины (модули)								213	8104	2096	1744	770	96	878	6008	590	130		2092	408	1656	392	1656	356	1584	356	1116	232	
Обязательная часть								155	6016	1614	1276	570	84	622	4402	434	102		1768	348	1224	300	1404	296	936	200	684	132	
Б1.О.01	Философия	4					4	4	144	26	24	12		12	118	8					144	24							УК-1; ОПК-8
Б1.О.02	История России	3		2			23	4	144	66	64	48		16	78	16			72	32	72	32							УК-1; УК-5
Б1.О.03	Основы российской государственности		2				2	2	72	16	16	8		8	56	4			72	16									УК-5
Б1.О.04	Иностранный язык	24	13				1234	10	360	104	64			64	256	48	16		180	32	180	32							УК-4; ОПК-8
Б1.О.05	Безопасность жизнедеятельности		2				2	3	108	20	20	8		12	88	8			108	20									УК-7; УК-8
Б1.О.06	Физическая культура		2					2	72	8	8	8			64				72	8									УК-7
Б1.О.07	Русский язык и культура речи		1				1	2	72	20	20	8		12	52	8	4		72	20									УК-4; УК-5; ОПК-8
Б1.О.08	Основы управленческой деятельности		2				2	3	108	24	24	12		12	84	8			108	24									УК-6; УК-9; ОПК-1; ОПК-5
Б1.О.09	Документоведение		1				1	2	72	16	16	8		8	56	4			72	16									ОПК-8; ОПК-10
Б1.О.10	Экономика предприятия и организация производства	23					23	6	216	86	48	24		24	130	16			108	24	108	24							УК-9; ОПК-12
Б1.О.11	**Группа учебных дисциплин (модулей) "Математические основы обеспечения информационной безопасности":**	**1245**	**46**	**3**			**1134456**	**21**	**756**	**208**	**200**	**92**		**108**	**548**	**56**	**4**		**252**	**84**	**324**	**76**	**180**	**40**					**УК-1; ОПК-3; ОПК-11**
Б1.О.11.01	Линейная алгебра и аналитическая геометрия	1					1	3	108	30	28	12		16	78	4			108	28									УК-1; ОПК-3
Б1.О.11.02	Математический анализ	2					1	4	144	58	56	24		32	86	20			144	56									УК-1; ОПК-3
Б1.О.11.03	Теория графов	4					4	3	108	30	28	12		16	78	4					108	28							УК-1; ОПК-3
Б1.О.11.04	Теория информации			3			3	3	108	24	24	12		12	84	8					108	24							УК-1; ОПК-3
Б1.О.11.05	Теория вероятностей и математическая статистика	5	4				45	6	216	50	48	24		24	166	16	4				108	24	108	24					ОПК-3; ОПК-11
Б1.О.11.06	Дискретная математика		6				6	2	72	16	16	8		8	56	4							72	16					УК-1; ОПК-3
Б1.О.12	**Группа учебных дисциплин (модулей) "Физико-технические основы обеспечения информационной безопасности":**	**3**	**246**				**2346**	**12**	**432**	**110**	**108**	**40**	**20**	**48**	**322**	**30**	**8**		**108**	**24**	**216**	**60**	**108**	**24**					**УК-1; ОПК-4; ОПК-11**
Б1.О.12.01	Физика	3	2				23	6	216	54	52	24	4	24	162	12	4		108	24	108	28							ОПК-4; ОПК-11
Б1.О.12.02	Электротехника		4				4	3	108	32	32	8	8	16	76	10					108	32							УК-1; ОПК-4
Б1.О.12.03	Электроника и схемотехника		6				6	3	108	24	24	8	8	8	84	8	4						108	24					УК-1; ОПК-4
Б1.О.13	**Группа учебных дисциплин (модулей) "Информационные технологии":**	**15678**	**6**				**156678**	**21**	**756**	**170**	**160**	**64**	**32**	**64**	**586**	**42**	**8**		**144**	**24**			**324**	**72**	**288**	**64**			**УК-1; ОПК-2; ОПК-7; ОПК-9**
Б1.О.13.01	Информатика	1					1	4	144	26	24	8	8	8	118	6			144	24									УК-1; ОПК-7
Б1.О.13.02	Языки программирования	5					5	3	108	26	24	8		16	82	4							108	24					УК-1; ОПК-7
Б1.О.13.03	Технологии и методы программирования	6					6	3	108	26	24	8	8	8	82	8	4						108	24					УК-1; ОПК-7
Б1.О.13.04	Информационные технологии		6				6	3	108	24	24	8		16	84	12	4						108	24					УК-1; ОПК-2
Б1.О.13.05	Аппаратные средства вычислительной техники	8					8	4	144	34	32	16	8	8	110	4									144	32			УК-1; ОПК-2
Б1.О.13.06	Сети и системы передачи информации	7					7	4	144	34	32	16	8	8	110	8									144	32			УК-1; ОПК-9
Б1.О.14	**Группа учебных дисциплин (модулей) "Методы и средства обеспечения информационной безопасности":**	**5789**	**689**	**3**		**5789**	**2689**	**30**	**1080**	**444**	**220**	**96**	**16**	**108**	**636**	**80**	**30**		**72**	**16**	**72**	**16**	**288**	**48**	**396**	**84**	**252**	**56**	**УК-1; ОПК-1; ОПК-5; ОПК-6; ОПК-8; ОПК-9; ОПК-10; ОПК-12; ДОПК-3**
Б1.О.14.01	Основы информационной безопасности			3			2	4	144	32	32	16		16	112	8	4		72	16	72	16							ОПК-1; ОПК-6; ОПК-8
Б1.О.14.02	Организационное и правовое обеспечение информационной безопасности	5				5		5	180	84	28	12		16	96	16	6						180	28					ОПК-5; ОПК-6
Б1.О.14.03	Основы управления информационной безопасностью		6				6	3	108	20	20	8		12	88	12	8						108	20					ОПК-5; ОПК-10
Б1.О.14.04	Защита информации от утечки по техническим каналам	7				7		4	144	84	28	12	8	8	60	6									144	28			УК-1; ОПК-6
Б1.О.14.05	Методы и средства криптографической защиты информации		9				9	3	108	28	28	12		16	80	10											108	28	УК-1; ОПК-9
Б1.О.14.06	Программно-аппаратные средства защиты информации	8				8		3	108	84	28	12	8	8	24	8									108	28			ОПК-6; ОПК-10; ОПК-12
Б1.О.14.07	Комплексное обеспечение защиты информации объекта информатизации (предприятия)	9	8			9	8	8	288	112	56	24		32	176	20	12								144	28	144	28	ОПК-8; ОПК-12; ДОПК-3
Б1.О.15	**Дисциплины (модули) профиля: "Организация и технология защиты информации" (по отрасли или в сфере профессиональной деятельности)**	**66689A**	**557**	**9**			**5566678899A**	**33**	**1188**	**252**	**240**	**108**	**16**	**116**	**936**	**90**	**32**						**504**	**112**	**252**	**52**	**432**	**76**	**УК-1; УК-9; ОПК-3; ДОПК-1; ДОПК-2; ДОПК-3; ДОПК-4**
Б1.О.15.01	Математическая логика и теория алгоритмов		5				5	3	108	24	24	8		16	84	8	4						108	24					УК-1; ОПК-3
Б1.О.15.02	Информационные процессы и системы как объекты информационной безопасности	6	5				56	4	144	42	40	16		24	102	8	4						144	40					ДОПК-1; ДОПК-2; ДОПК-4
Б1.О.15.03	Конфиденциальное делопроизводство и защищенный электронный документооборот	6					6	4	144	26	24	12	4	8	118	12							144	24					ДОПК-1; ДОПК-3
Б1.О.15.04	Нормативные акты и стандарты по информационной безопасности	6					6	3	108	26	24	12	4	8	82	10							108	24					ДОПК-2; ДОПК-3; ДОПК-4

План Учебный план бакалавриата 10.03.01 ИБЗ-ОТЗИ-2023 Информационна

-	-	Форма контроля						з.е.	Итого акад.часов									Курс 1		Курс 2		Курс 3		Курс 4		Курс 5		-
Индекс	Наименование	Экзамен	Зачет	Зачет с оц.	КП	КР	Контр.	Факт	По плану	Конт. раб.	Ауд.	Лек	Лаб	Пр	СР	Интер часы	Пр. подгот	Итого	Ауд.	Итого	Ауд.	Итого	Ауд.	Итого	Ауд.	Итого	Ауд.	Компетенции
Б1.О.15.05	Организация системы обеспечения информационной безопасности (служба ИБ)			9			9	4	144	28	28	12		16	116	12	8									144	28	ДОПК-1; ДОПК-2
Б1.О.15.06	Физическая защита информационных объектов	8					8	4	144	26	24	12	4	8	118	10								144	24			ДОПК-1; ДОПК-3
Б1.О.15.07	Информационно-аналитическая деятельность по обеспечению комплексной безопасности	9					9	4	144	26	24	12	4	8	118	8	8									144	24	ДОПК-1; ДОПК-2
Б1.О.15.08	Экономика информационной безопасности	А					А	4	144	26	24	12		12	118	12	8									144	24	УК-9; ДОПК-2; ДОПК-3; ДОПК-4
Б1.О.15.09	Моделирование процессов и систем защиты информации		7				7	3	108	28	28	12		16	80	10								108	28			ДОПК-1; ДОПК-4
Б1.О.16	Элективные курсы по физической культуре и спорту		1						328	8	8	8			320			328	8									УК-7
Б1.О.17	Основы военной подготовки		3						108	36	36	26		10	72	16				108	36							УК-7; УК-8
Часть, формируемая участниками образовательных отношений								58	2088	482	468	200	12	256	1606	156	28	324	60	432	92	252	60	648	156	432	100	
Б1.В.01	**Дисциплины (модули) образовательной организации:**	**13**	**457**	**46**			**1344567**	**19**	**684**	**144**	**140**	**60**	**4**	**76**	**540**	**38**	**8**	**108**	**20**	**324**	**68**	**144**	**32**	**108**	**20**			**УК-2; УК-5; УК-7; УК-10; ПК-1; ПК-2; ПК-3; ПК-4; ПК-5**
Б1.В.01.01	Основы исследований информационной безопасности	1					1	3	108	22	20	8		12	86	8	4	108	20									УК-2; УК-10; ПК-1; ПК-2; ПК-3
Б1.В.01.02	Пакеты прикладных програми	3					3	4	144	26	24	12		12	118	4				144	24							ПК-2; ПК-4
Б1.В.01.03	Социально-психологические основы управленческой деятельности		4				4	2	72	20	20	8		12	52	4				72	20							УК-2; ПК-3
Б1.В.01.04	Основы конкурентной разведки		5	6			56	4	144	32	32	16		16	112	8						144	32					УК-2; ПК-4
Б1.В.01.05	История защиты информации в РФ			4			4	3	108	24	24	8		16	84	6				108	24							УК-5; ПК-3
Б1.В.01.06	Информационная безопасность автоматизированных систем		7				7	3	108	20	20	8	4	8	88	8	4							108	20			ПК-3; ПК-5
Б1.В.02	Основы права	1					1	3	108	22	20	8		12	86			108	20									УК-5; ПК-1
Б1.В.03	Безопасность информационных технологий			8			8	3	108	24	24	8		16	84	8								108	24			УК-1; ПК-5
Б1.В.04	Гуманитарные аспекты (профессиональная этика) информационной безопасности		7				7	2	72	16	16	8		8	56	8	4							72	16			УК-1; ПК-3
Б1.В.ДВ.01	**Дисциплины по выбору Блок 1.В.ДВ.1**		**5**				**5**	**3**	**108**	**28**	**28**	**12**		**16**	**80**	**10**						**108**	**28**					**ПК-2; ПК-4**
Б1.В.ДВ.01.01	Операционные системы, среды и оболочки		5				5	3	108	28	28	12		16	80	10						108	28					ПК-2; ПК-4
Б1.В.ДВ.01.02	Базы данных, системы управления базами данных		5				5	3	108	28	28	12		16	80	10						108	28					ПК-1; ПК-4
Б1.В.ДВ.02	**Дисциплины по выбору Блок 1.В.ДВ.2**	**3**					**3**	**3**	**108**	**26**	**24**	**12**		**12**	**82**	**10**				**108**	**24**							**ПК-1; ПК-4**
Б1.В.ДВ.02.01	Основы алгоритмизации и программирования	3					3	3	108	26	24	12		12	82	10				108	24							ПК-1; ПК-4
Б1.В.ДВ.02.02	Пакеты прикладных математических программ	3					3	3	108	26	24	12		12	82	10				108	24							ПК-1; ПК-4
Б1.В.ДВ.03	**Дисциплины по выбору Блок 1.В.ДВ.3**	**7**					**7**	**3**	**108**	**30**	**28**	**12**		**16**	**78**	**10**								**108**	**28**			**ПК-1; ПК-2**
Б1.В.ДВ.03.01	Информационная безопасность кредитно-финансовых операций	7					7	3	108	30	28	12		16	78	10								108	28			ПК-1; ПК-2
Б1.В.ДВ.03.02	Защищенные электронные технологии банка	7					7	3	108	30	28	12		16	78	10								108	28			ПК-1; ПК-2
Б1.В.ДВ.03.03	Подготовка объекта информатизации к аттестации по требованиям безопасности информации (ООО "НОВО")	7					7	3	108	30	28	12		16	78	10								108	28			ПК-1; ПК-2
Б1.В.ДВ.03.04	Аттестация объекта информатизации по требованиям безопасности информации (ООО "ЦБИ")	7					7	3	108	30	28	12		16	78	10								108	28			ПК-1; ПК-2
Б1.В.ДВ.04	**Дисциплины по выбору Блок 1.В.ДВ.4**			**7**			**7**	**3**	**108**	**28**	**28**	**12**	**8**	**8**	**80**	**8**	**4**							**108**	**28**			**ПК-2; ПК-3**
Б1.В.ДВ.04.01	Информационно-психологическая безопасность персонала предприятия			7			7	3	108	28	28	12	8	8	80	8	4							108	28			ПК-2; ПК-3
Б1.В.ДВ.04.02	Защита общества от информации, запрещенной к распространению			7			7	3	108	28	28	12	8	8	80	8	4							108	28			ПК-2; ПК-3
Б1.В.ДВ.04.03	Организация защиты конфиденциальной информации от несанкционированного доступа (ООО "НОВО")			7			7	3	108	28	28	12	8	8	80	8	4							108	28			ПК-2; ПК-3
Б1.В.ДВ.04.04	Защита информации от НСД (ООО"ЦБИ")			7			7	3	108	28	28	12	8	8	80	8	4							108	28			ПК-2; ПК-3
Б1.В.ДВ.05	**Дисциплины по выбору Блок 1.В.ДВ.5**		**8**				**8**	**2**	**72**	**20**	**20**	**8**		**12**	**52**	**10**								**72**	**20**			**ПК-3; ПК-4**
Б1.В.ДВ.05.01	Разработка политики информационной безопасности в организациях		8				8	2	72	20	20	8		12	52	10								72	20			ПК-3; ПК-4
Б1.В.ДВ.05.02	Разработка политики информационной безопасности в Интернет-системах		8				8	2	72	20	20	8		12	52	10								72	20			ПК-3; ПК-4
Б1.В.ДВ.05.03	Оценка защищенности конфиденциальной информации по техническим каналам и от несанкционированного доступа (ООО "НОВО")		8				8	2	72	20	20	8		12	52	10								72	20			ПК-1; ПК-3; ПК-4
Б1.В.ДВ.05.04	Контроль защищенности информации от утечки по техническим каналам (ООО "ЦБИ")		8				8	2	72	20	20	8		12	52	10								72	20			ПК-1; ПК-3; ПК-4
Б1.В.ДВ.06	**Дисциплины по выбору Блок 1.В.ДВ.6**	**9**					**9**	**4**	**144**	**34**	**32**	**16**		**16**	**110**	**8**										**144**	**32**	**ПК-3; ПК-4**

План Учебный план бакалавриата 10.03.01 ИБЗ-ОТЗИ-2023 Информационна

-	-	Форма контроля						з.е.	Итого акад.часов									Курс 1		Курс 2		Курс 3		Курс 4		Курс 5		-
Индекс	Наименование	Экзамен	Зачет	Зачет с оц.	КП	КР	Контр.	Факт	По плану	Конт. раб.	Ауд.	Лек	Лаб	Пр	СР	Интер часы	Пр. подгот	Итого	Ауд.	Итого	Ауд.	Итого	Ауд.	Итого	Ауд.	Итого	Ауд.	Компетенции
Б1.В.ДВ.06.01	Организация защиты персональных данных на предприятии	9					9	4	144	34	32	16		16	110	8										144	32	ПК-3; ПК-4
Б1.В.ДВ.06.02	Правовая охрана результатов интеллектуальной деятельности	9					9	4	144	34	32	16		16	110	8										144	32	ПК-3; ПК-4
Б1.В.ДВ.06.03	Методы и средства защиты информации от утечки по техническим каналам (ООО "НОВО")	9					9	4	144	34	32	16		16	110	8										144	32	ПК-1; ПК-3; ПК-4
Б1.В.ДВ.06.04	Средства защиты информации и оценка эффективности защиты от утечки по техническим каналам (ООО "ЦБИ")	9					9	4	144	34	32	16		16	110	8										144	32	ПК-1; ПК-3; ПК-4
Б1.В.ДВ.07	**Дисциплины по выбору Блок 1.В.ДВ.7**		**8**				**8**	**2**	**72**	**20**	**20**	**8**		**12**	**52**	**8**								**72**	**20**			**ПК-4; ПК-5**
Б1.В.ДВ.07.01	Защита профессиональной тайны в различных сферах деятельности		8				8	2	72	20	20	8		12	52	8								72	20			ПК-4; ПК-5
Б1.В.ДВ.07.02	Информационная безопасность операционных систем и баз данных		8				8	2	72	20	20	8		12	52	8								72	20			ПК-4; ПК-5
Б1.В.ДВ.07.03	Технические каналы утечки конфиденциальной информации (ООО "НОВО")		8				8	2	72	20	20	8		12	52	8								72	20			ПК-4; ПК-5
Б1.В.ДВ.07.04	Технические каналы утечки информации ООО "ЦБИ")		8				8	2	72	20	20	8		12	52	8								72	20			ПК-4; ПК-5
Б1.В.ДВ.08	**Дисциплины по выбору Блок 1.В.ДВ.8**		**9**				**9**	**2**	**72**	**20**	**20**	**8**		**12**	**52**	**12**	**4**									**72**	**20**	**ПК-4; ПК-5**
Б1.В.ДВ.08.01	Лицензирование и сертификация в области защиты информации		9				9	2	72	20	20	8		12	52	12	4									72	20	ПК-4; ПК-5
Б1.В.ДВ.08.02	Аттестация в области защиты информации		9				9	2	72	20	20	8		12	52	12	4									72	20	ПК-4; ПК-5
Б1.В.ДВ.08.03	Разработка объекта информатизации в защищенном исполнении (ООО "НОВО")		9				9	2	72	20	20	8		12	52	12	4									72	20	ПК-2; ПК-4; ПК-5
Б1.В.ДВ.08.04	Разработка и сертификация средств защиты информации и технических средств в защищенном исполнении (ООО "ЦБИ")		9				9	2	72	20	20	8		12	52	12	4									72	20	ПК-4; ПК-5
Б1.В.ДВ.09	**Дисциплины по выбору Блок 1.В.ДВ.9**		**9**				**9**	**3**	**108**	**28**	**28**	**12**		**16**	**80**	**10**										**108**	**28**	**ПК-3; ПК-5**
Б1.В.ДВ.09.01	Радиоэлектронные системы и средства как объекты информационной безопасности		9				9	3	108	28	28	12		16	80	10										108	28	ПК-3; ПК-5
Б1.В.ДВ.09.02	Основы радиоэлектроной разведки (РЭР)		9				9	3	108	28	28	12		16	80	10										108	28	ПК-3; ПК-5
Б1.В.ДВ.09.03	Методы и средства защиты информации от несанкционированного доступа (ООО "НОВО")		9				9	3	108	28	28	12		16	80	10										108	28	ПК-1; ПК-3; ПК-5
Б1.В.ДВ.09.04	Методы и средства обеспечения защищенности информации от несанкционированного доступа (ООО "ЦБИ")		9				9	3	108	28	28	12		16	80	10										108	28	ПК-1; ПК-3; ПК-5
Б1.В.ДВ.10	**Дисциплины по выбору Блок 1.В.ДВ.10**	**А**					**А**	**3**	**108**	**22**	**20**	**8**		**12**	**86**	**10**										**108**	**20**	**ПК-1; ПК-2; ПК-3**
Б1.В.ДВ.10.01	Социотехносферная безопасность объектов информационной защиты	А					А	3	108	22	20	8		12	86	10										108	20	ПК-1; ПК-2; ПК-3
Б1.В.ДВ.10.02	Эффективность защищенных информационных систем	А					А	3	108	22	20	8		12	86	10										108	20	УК-9; ПК-1; ПК-2; ПК-4
Б1.В.ДВ.10.03	Методы и средства выявления демаскирующих признаков закладочных устройств в защищаемых помещениях (ООО"НОВО", ООО "ЦБИ")	А					А	3	108	22	20	8		12	86	10										108	20	ПК-2; ПК-4; ПК-5
Б1.В.ДВ.11	**Дисциплины по выбору Блок 1.В.ДВ.11**			**1**				**3**	**108**	**20**	**20**	**8**		**12**	**88**	**6**	**8**	**108**	**20**									**УК-5; ПК-1**
Б1.В.ДВ.11.01	Введение в профессию			1				3	108	20	20	8		12	88	6	8	108	20									УК-5; ПК-1
Б1.В.ДВ.11.02	Профессиональные адаптации инвалидов и лиц с ОВЗ			1				3	108	20	20	8		12	88	6	8	108	20									УК-6; ПК-1
Блок 2.Практика								18	648						648					108		108		108		324		
Обязательная часть								9	324						324											324		
Б2.О.01(П)	Преддипломная практика			А				9	324						324											324		ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ДОПК-1; ДОПК-2; ДОПК-3; ДОПК-4
Часть, формируемая участниками образовательных отношений								9	324						324					108		108		108				
Б2.В.01(У)	Ознакомительная практика			4				3	108						108					108								УК-1; УК-2; УК-3; УК-6; УК-9; ПК-1; ПК-2; ПК-3
Б2.В.02(У)	Учебно-лабораторная практика			6				3	108						108							108						ПК-1; ПК-2; ПК-3; ПК-4
Б2.В.03(П)	Технологическая практика			8				3	108						108									108				ПК-1; ПК-2; ПК-3; ПК-4; ПК-5
Блок 3.Государственная итоговая аттестация								9	324						324											324		
Б3.01(Д)	Подготовка и защита ВКР							9	324						324											324		УК-1; УК-2; УК-3; УК-4; УК-5; УК-6; УК-7; УК-8; УК-9; УК-10; ОПК-1; ОПК-2; ОПК-3; ОПК-4; ОПК-5; ОПК-6; ОПК-7; ОПК-8; ОПК-9; ОПК-10; ОПК-11; ОПК-12; ОПК-13; ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ДОПК-1; ДОПК-2; ДОПК-3; ДОПК-4
ФТД.Факультативные дисциплины								6	216	60	24			24	156	12						144	16	72	8			
ФТД.01	Технико-экономическое обоснование проекта		5					2	72	8	8			8	64	4						72	8					УК-2; УК-10; ПК-5
ФТД.02	Разработка и реализация проекта		6	7	7			4	144	52	16			16	92	8						72	8	72	8			УК-1; УК-2; УК-3; УК-10; ПК-2; ПК-5
	Итого з.е./Акад.часов (без факультативов)							240	9076	2096	1744	770	96	878	6980	590	130	2092	408	1764	392	1764	356	1692	356	1764	232	

Приложение 3

Описание и матрица реализации практической подготовки обучающихся

Практическая подготовка – форма организации образовательной деятельности при освоении образовательной программы в условиях выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенции по профилю соответствующей образовательной программы (пункт 24 статьи 2 Федерального закона «Об образовании в Российской Федерации», в редакции Федерального закона от 2 декабря 2019 г. №403-ФЗ) (далее – Закон об образовании).

Практическая подготовка представляет собой форму обучения, направленную на закрепление и развитие профильных навыков и компетенций, при которой обучающийся выполняет виды работ, связанные с будущей профессиональной деятельностью. Практическая подготовка обеспечивает необходимый уровень профессиональной подготовки обучающихся в соответствии с требованиями регионального рынка труда.

Образовательная программа по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» в соответствии с частью 6 статьи 13 Закона об образовании в интересах повышения качества образования и усиления практической подготовки обучающихся, обеспечивает проведение практической подготовки обучающихся при реализации отдельных учебных предметов, курсов, дисциплин (модулей), практик, иных компонентов, предусмотренных учебным планом.

Практическая подготовка организуется в форме практики путем непосредственного выполнения обучающимися определенных видов работ, а также в форме практических занятий, практикумов, лабораторных работ и иных аналогичных видов учебной деятельности, предусматривающих участие

обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью (табл. 1).

Таблица 1 – Матрица реализации практической подготовки обучающихся

Индекс	Наименование дисциплины	Формируемые компетенции	Практическая подготовка (кол-во часов)
Блок 1.В.02	Основы права	ПК-1	8/8
Блок 1.В.04	Гуманитарные аспекты (профессиональная этика) информационной безопасности	ПК-3	4/4
Блок 1.В.ДВ.01.01	Операционные системы, среды и оболочки	ПК-2;ПК-4	16/16
Блок 1.В.ДВ.01.02	Базы данных, системы управления базами данных	ПК-1;ПК-4	16/16
Блок 1.В.ДВ.02.01	Основы алгоритмизации и программирования	ПК-1;ПК-4	8/8
Блок 1.В.ДВ.02.02	Пакеты прикладных математических программ	ПК-1;ПК-4	8/8
Блок 1.В.ДВ.03.01	Информационная безопасность кредитно-финансовых операций	ПК-1;ПК-2	8/8
Блок 1.В.ДВ.03.02	Защищенные электронные технологии банка	ПК-1;ПК-2	8/8
Блок 1.В.ДВ.03.03	Подготовка объекта информатизации к аттестации по требованиям безопасности информации (ООО «НОВО»)	ПК-1;ПК-2	8/8
Блок 1.В.ДВ.03.04	Аттестация объекта информатизации по требованиям безопасности информации (ООО "ЦБИ")	ПК-1;ПК-2	8/8
Блок 1.В.ДВ.05.01	Разработка политики информационной безопасности в организациях	ПК-3;ПК-4	12/12
Блок 1.В.ДВ.05.02	Разработка политики информационной безопасности в Интернет-системах	ПК-3;ПК-4	12/12
Блок 1.В.ДВ.05.03	Оценка защищенности	ПК-1;ПК-3;ПК-4	12/12

	конфиденциальной информации по техническим каналам и от несанкционированного доступа (ООО «НОВО»)		
Блок 1.В.ДВ.05.04	Контроль защищенности информации от утечки по техническим каналам (ООО "ЦБИ")	ПК-3;ПК-4	12/12
Блок 1.В.ДВ.06.01	Организация защиты персональных данных на предприятии	ПК-3;ПК-4	12/12
Блок 1.В.ДВ.06.02	Правовая охрана результатов интеллектуальной деятельности	ПК-3;ПК-4	12/12
Блок 1.В.ДВ.06.03	Методы и средства защиты информации от утечки по техническим каналам (ООО «НОВО»)	ПК-1;ПК-3;ПК-4	12/12
Блок 1.В.ДВ.06.04	Средства защиты информации и оценка эффективности защиты от утечки по техническим каналам (ООО "ЦБИ")	ПК-1;ПК-3;ПК-4	12/12
Блок 1.В.ДВ.07.01	Защита профессиональной тайны в различных сферах деятельности	ПК-4;ПК-5	12/12
Блок 1.В.ДВ.07.02	Информационная безопасность операционных систем и баз данных	ПК-4;ПК-5	12/12
Блок 1.В.ДВ.07.03	Технические каналы утечки конфиденциальной информации (ООО «НОВО»)	ПК-4;ПК-5	12/12
Блок 1.В.ДВ.07.04	Технические каналы утечки информации (ООО "ЦБИ")	ПК-4;ПК-5	12/12
Блок 1.В.ДВ.08.01	Лицензирование и сертификация в области защиты информации	ПК-4;ПК-5	12/12
Блок 1.В.ДВ.08.02	Аттестация в области защиты информации	ПК-4;ПК-5	12/12
Блок 1.В.ДВ.08.03	Разработка объекта информатизации в защищенном исполнении (ООО «НОВО»)	ПК-2;ПК-4;ПК-5	12/12
Блок 1.В.ДВ.08.04	Разработка и сертификация средств защиты информации и технических средств в	ПК-2;ПК-4;ПК-5	12/12

	защищенном исполнении (ООО "ЦБИ")		
Блок 1.В.ДВ.10.01	Социотехносферная безопасность объектов информационной защиты	ПК-1;ПК-2;ПК-3	16/12
Блок 1.В.ДВ.10.02	Эффективность защищенных информационных систем	ПК-1;ПК-2;ПК-4	16/12
Блок 1.В.ДВ.10.03	Методы и средства выявления демаскирующих признаков закладочных устройств в защищаемых помещениях (ООО «НОВО»)	ПК-2;ПК-4;ПК-5	16/12
Блок 1.В.ДВ.11.01	Введение в профессию	ПК-1	16/12
Блок 1.В.ДВ.11.02	Профессиональные адаптации инвалидов и лиц с ОВЗ	ПК-1	16/12

Количество часов, отведенных на практическую подготовку обучающихся, определено исходя из содержания и направленности образовательной программы, ее компонентов и возможности их реализации в форме практической подготовки в соответствии с утвержденным в Университете Положением о практической подготовке обучающихся.

Приложение 4. Рабочая программа воспитания и календарный план воспитательной работы

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ВОСПИТАНИЯ

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Год набора 2023

Королев
2023

СОДЕРЖАНИЕ

1. Общие положения

Рабочая программа воспитания разработана в соответствии с нормами и положениями:

- Федерального закона от 29.01.2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
- Федерального закона от 31.07.2020 №304-ФЗ «О внесении изменений в Федеральный закон «Об образовании в Российской Федерации» по вопросам воспитания обучающихся»;
- Федерального закона от 05.02.2018 г. №15-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам добровольчества (волонтерства)»;
- Указа Президента Российской Федерации от 19.12.2012 г. №1666 «О стратегии государственной национальной политики Российской Федерации на период до 2025 года»;
- Указа Президента Российской Федерации от 24.12.2014 г. №808 «Об утверждении Основ Государственной культурной политики»;
- Указа Президента Российской Федерации от 31.12.2015 №683 «О стратегии национальной безопасности Российской Федерации (с изменениями от 06.03.2018 г);
- Указа Президента Российской Федерации от 07.05.2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»;
- Указа Президента Российской Федерации от 09.05.2017 г. № 203 «Стратегия развития информационного общества в Российской Федерации на 2017-2030 гг»;
- Приказа Минобрнауки России от 6 апреля 2021 г. № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»;
- Распоряжения Правительства от 29.05.2015 г. №996-р «Стратегия развития воспитания в Российской Федерации на период до 2025 года»;
- Распоряжения Правительства от 29.11.2014 г. №2403-р «основы государственной молодежной политики Российской Федерации на период до 2025 года»;
- Плана мероприятий по реализации Основ государственной молодежной политики Российской Федерации на период до 2025 года, утвержденных распоряжением Правительства Российской Федерации 29.11.2-14 г.№2403-р;
- Постановления Правительства Российской Федерации от 26.12.2017 г. № 1642 «Об утверждении государственной программы Российской Федерации «Развитие образования»;

− Письма Министерства образования и науки Российской Федерации от 14.02.2014 № ВК-262/09 «Методические рекомендации о создании и деятельности советов обучающихся в образовательных организациях»;

− Приказа Федеральной службы по надзору в сфере образования и науки (Рособрнадзор) от 14.08.2020 №831 «Об утверждении Требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети «Интернет» и формату предоставления информации».

2. Цели и задачи воспитательной работы

Целеполагающей основой воспитательной работы в Университете является создание условий для активной жизнедеятельности обучающихся, их гражданского самоопределения, профессионального становления и индивидуально-личностной самореализации в созидательной деятельности для удовлетворения потребностей в нравственном, культурном, интеллектуальном, социальном и профессиональном развитии.

К основным задачами воспитательной работы в Университете относятся:

- развитие мировоззрения и актуализация системы базовых ценностей личности;
- приобщение обучающихся к общечеловеческим нормам морали, национальным устоям и академическим традициям;
- воспитание уважения к закону, нормам коллективной жизни, развитие гражданской и социальной ответственности;
- воспитание положительного отношения к труду, воспитание социально значимой целеустремленности и ответственности в деловых отношениях;
- обеспечение развития личности и ее социально-психологической поддержки, формирование личностных качеств, необходимых для эффективной профессиональной деятельности;
- выявление и поддержка талантливой молодежи, формирование организаторских навыков, творческого потенциала, вовлечение обучающихся в процессы саморазвития и самореализации;
- формирование культуры и этики профессионального общения;
- воспитание внутренней потребности личности в здоровом образе жизни, ответственного отношения к природной и социокультурной среде;
- повышение уровня культуры безопасного поведения;
- развитие личностных качеств и установок, социальных навыков и управленческих способностей.

В центре системы воспитательной работы – личность обучающегося. Преподаватели, заведующие кафедрами, сотрудники институтов и кураторы решают воспитательные задачи через учебную деятельность: содержание учебной дисциплины, методику преподавания, добросовестное отношение к своим обязанностям, желание помочь каждому обучающемуся, уважительное

отношение к обучающимся, умение понять и выслушать каждого, а также заинтересованность в успехах обучающихся, объективность в оценке знаний, широту эрудиции, внешний вид, честность, формирование универсальных навыков, что оказывает междисциплинарное комплексное влияние на воспитание личности обучающихся, формируется такая ситуация развития, где каждый обучающийся может актуализировать свои потенциальные личностные возможности и развить новые навыки.

3. Направления воспитательной работы и матрица реализуемых видов воспитательной деятельности

Система воспитательной работы Университета направлена на создание условий для активной жизнедеятельности обучающихся, их гражданского самоопределения, профессионального становления и индивидуально-личностной самореализации в созидательной деятельности для удовлетворения потребностей в нравственном, культурном, интеллектуальном, социальном и профессиональном развитии.

№ п/п	Направления воспитательной работы	Воспитательные задачи
1	Гражданско-патриотическое, правовое воспитание	Формирование патриотического сознания и поведения обучающихся, уважения к закону и правопорядку, готовности к достойному служению обществу и государству, нетерпимого отношения к коррупционному поведению
2	Духовно-нравственное воспитание	Повышение степени освоения личностью социального опыта, ценностей культурно-регионального сообщества, культуры, приобщение студентов к нравственным ценностям, развитие нравственных чувств; становление нравственной воли; побуждение к нравственному поведению; развитие культуры межнационального общения и формирование установок на равнозначность и равноценность каждого члена общества, социальная адаптация иностранных граждан, социальная адаптация лиц с ограниченными возможностями здоровья и инвалидов
3	Культурно-просветительское воспитание	Поддержка и развитие творческих способностей и талантов обучающихся; создание условий для развития

		эстетического вкуса, повышения уровня культуры, приобщение к культурному наследию и традициям народов России
4	Научно-образовательное воспитание	Содействие профессиональному самоопределению обучающихся, их профессиональному развитию; формирование исследовательского и критического мышления, мотивации к научно-исследовательской деятельности
5	Профессионально-трудовое / бизнес-ориентирующее воспитание	Помощь в формировании критериев выбора будущей специальности и в создании индивидуальной траектории профессионального развития
6	Экологическое воспитание	Формирование ответственного отношения к окружающей среде и экологического сознания; соблюдение нравственных и правовых принципов природопользования, пропаганда идей активной деятельности по изучению и охране природы; формирование научного знания и представления о системе «человек-природа»
7	Физическое воспитание и формирование здорового образа жизни	Формирование навыков здорового образа жизни, массового спорта и физической культуры, профилактика вредных привычек
8	Военно-патриотическое воспитание	Формирование базовых навыков в области военной подготовки, изучение тем военно-политической и правовой подготовки. Формирование высокого патриотического сознания, возвышенного чувства верности своему Отечеству, готовности к его защите как важнейшей конституционной обязанности в отстаивании национальных интересов Российской Федерации и обеспечении ее военной безопасности перед лицом внешних и внутренних угроз

Воспитательная работа со студентами сосредоточена на развитии потребности личности в достижении личностных успехов, реализации своих целей и задач, формирования самостоятельности, самоутверждения, развития самодостаточности личности, ее основных качеств, способствующих включение в различные сферы общественной жизнедеятельности, получения определенной специализации, профессионального развития и отражается дисциплинами учебного плана (табл. 1).

Таблица 1 – Матрица реализуемых видов воспитательной деятельности

Индекс	Наименование дисциплины	Код компетенций	Реализуемый вид воспитательной деятельности
Б1.О.01	Философия	УК-1;	Гражданско-патриотическое, духовно-нравственное
Б1.О.02	История России	УК-5	Гражданско-патриотическое
Б1.О.03	Основы российской государственности	УК-5	Гражданско-патриотическое
Б1.О.04	Иностранный язык	УК-4;	Духовно-нравственное
Б1.О.05	Безопасность жизнедеятельности	УК-7; УК-8	Экологическое
Б1.О.06	Физическая культура	УК-7	Физическое воспитание и формирование здорового образа жизни
Б1.О.08	Основы управленческой деятельности	УК-6; УК-9	Бизнес-ориентирующее
Б1.О.01.10	Экономика предприятия и организация производства	УК-9	Бизнес-ориентирующее
Б1.О.13.01	Информатика	УК-1	Бизнес-ориентирующее
Б1.О.16	Элективные курсы по физической культуре и спорту	УК-7	Физическое воспитание и формирование здорового образа жизни
Б1.О.17	Основы военной подготовки	УК-7; УК-8	Военно-патриотическое воспитание
Б1.В.01.03	Социально-педагогические основы управленческой деятельности	УК-2	Духовно-нравственное
Б1.В.01.04	Основы конкурентной разведки	УК-2	Духовно-нравственное, культурно-творческое
Б1.В.02	Основы права	УК-5	Правовое
Б1.В.03	Безопасность информационных технологий	УК-1	Духовно-нравственное, Профессионально-трудовое
Б1.В.ДВ.11.01	Введение в профессию	УК-5	Профессионально-трудовое
Б1.В.ДВ.11.02	Профессиональные адаптации инвалидов и лиц с ОВЗ	УК-6	Гражданско-патриотическое
ФТД.01	Технико-экономическое обоснование проекта	УК-2	Бизнес-ориентирующее
ФТД.02	Разработка и реализация проекта	УК-1; УК-2; УК-3; УК-10	Духовно-нравственное

Представленные в матрице дисциплины и соответствующие им компетенции отражают реализуемый вид воспитательной деятельности в

рамках освоения образовательной программы по направлению подготовки 10.03.01 Информационная безопасность согласно учебного плана.

Формами аттестации являются:

аттестация по дисциплине в форме, предусмотренной учебным планом (зачет / зачет с оценкой / экзамен);

отчет по самостоятельной работе обучающегося в форме портфолио, размещённого в личном кабинете обучающегося в электронно-информационной образовательной среде Университета по результатам каждого учебного года;

отчет о результатах воспитательной деятельности в рамках ежегодного отчета кафедры.

4. Мониторинг качества воспитательной работой

С целью повышения эффективности воспитательной работы проводится мониторинг состояния воспитательной работы в Университете, определяющий жизненные ценности студенческой молодежи, возникающие проблемы, перспективы развития и т.д., на основании которого совершенствуются формы и методы воспитания.

Обучающиеся Университета учитывают свои индивидуальные достижения в портфолио, которое содержит общую информацию об обучающемся и его заслугах в разных областях образовательного пространства.

Ежегодная оценка результативности воспитательной работы Университета осуществления на Ученом совете в форе предоставления доклада о воспитательной и внеучебной работе Проректором по внеучебной и воспитательной работе университета не реже одного раза в год.

Контроль за качеством воспитательной работы осуществляется с помощью анкетирования обучающихся. По результатам проводится корректировка работы.

5. Материально-техническое обеспечение

К инфраструктуре, обеспечивавший воспитательную работу в рамках учебной и внеучебной деятельности, относятся здания, сооружения, оборудование, транспорт и иное имущество, находящееся в оперативном управлении Университета или ином имущественном праве.

Для организации воспитательной работы имеются:

- учебные аудитории, оборудованные мультимедийными средствами для представления презентаций лекций и показа учебных фильмов, проведения мастер-классов;
- спортивная инфраструктура, обеспечивающая проведение практических занятий;
- помещения для организации и проведения культурно-досуговой деятельности;
- помещения для работы органов студенческого самоуправления.

Государственное бюджетное образовательное учреждение высшего образования
Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова

УТВЕРЖДАЮ
Ректор
«Технологического университета»
_____А.Ю. Щиканов
«09» января 2023 г.

Календарный план

событий и мероприятий воспитательной направленности

на 2023 - 2024 учебный год

г. Королев
Московская область
2023 г.

Календарный план событий и мероприятий воспитательной направленности

на 2023 – 2024 учебный год

Направления воспитательной деятельности	Мероприятие	Сроки проведения	Ответственный исполнитель	Форма проведения	Предполагаемое количество участников
Физическое	**Наши традиции.** Выезд студентов «Технологического университета» для подготовки к сдаче норм ГТО	31 августа 2023 г.	Проректор по МПиВР, Начальник Управления по воспит. работе, начальник ОРСТ, начальник ООМР, начальник ОСПП, деканы, кураторы групп	Спортивные соревнования	500
Научно-образовательное	День знаний – праздник, начало нового учебного года в подразделениях	01 сентября 2023 г.	Директора институтов	Торжественная линейка	3500
Гражданско-патриотическое	Мероприятие, посвящённое «Дню солидарности в борьбе с терроризмом»	03 сентября 2023 г.	Начальник ОРСТ	Акция памяти	50
Физическое	Проведение мероприятия «Здоровье – твоё богатство»: - акция «Обменяй сигарету на конфету»	04 сентября 2023 г.	Начальник ОСПП, зам. деканов факультетов, кураторы учебных групп	Акция	100
Гражданско-патриотическое	Участие студентов «МГОТУ» в мероприятиях, посвящённых празднованию Дня города Королёв	Начало сентября 2023 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ОРСТ, начальник ООМР, зам. деканов факультетов	Концерт	100

Культурно-просветительское	Организация мероприятия «Неделя первокурсника»	сентябрь 2023 г.	Студенческий совет	Тренинг	200
Физическое	Фестиваль студенческого спорта «От студ. зачёта к знаку отличия ГТО»	Начало сентября 2023 г.	Зам. начальника Управления по воспит. работе	Фестиваль	9
Физическое	Проведение психодиагностического исследования уровня социально-психологической адаптации у студентов 1 курса и психологического климата групп в структурных подразделениях университета	сентябрь - октябрь 2023 г.	Педагоги – психологи структурных подразделений	Социологический опрос	550
Научно-образовательное	Ознакомление студентов первых курсов с историей и традициями «МГОТУ», правилами внутреннего распорядка.	сентябрь 2023 г. декабрь 2023 г.	Кураторы групп первого курса	Встреча	550
Экологическое	Участие студентов «МГОТУ» в экологической акции «Наш лес. Посади своё дерево» по посадке деревьев на территории МО	сентябрь 2023 г.	Зам. деканов факультетов	Акция	50
Физическое	Проведение социально-психологического тестирования студентов МГОТУ и структурных подразделений университета	с сентября - ноябрь 2023 г.	Проректор по МПиВР, ведущий психолог ОСПП, психологи структурных подразделений	Социологический опрос	550
Культурно-просветительское	Участие команды КВН «Сборная города Королёва» в Региональной Подмосковной лиге КВН	сентябрь 2023 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ОРСТ	Конкурс	10

Культурно-просветительское	**Наши традиции.** Отчетный концерт творческих коллективов «МГОТУ»	начало октября 2023 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ОРСТ, начальник ООМР, зам. деканов факультетов	Концерт	200
Гражданско-патриотическое	Участие студентов в мероприятии, посвящённом празднованию дня гражданской обороны	октябрь 2023 г.	Проректор по МПиВР, начальник Управления по воспит. работе	Встреча	100
Физическое	Первенство по баскетболу, волейболу	октябрь 2023 г.	Проректор по внеучебной и воспитательной работе	Спортивные соревнования	50
Научно-образовательное	День открытых дверей Технологического университета и его подразделений	начало октября 2023 г.	Проректор по МПиВР	Встреча	3000
Экологическое	**Наши традиции.** «Закладка Аллеи первокурсников «МГОТУ» - посадка молодых деревьев первокурсниками в структурных подразделениях университета	октябрь 2023 г.	Проректор по МПиВР, кураторы 1 курса	Акция	650
Культурно-просветительское	**Наши традиции.** Организация и проведение игр Лиги КВН «МГОТУ» (Финал Лиги КВН «МГОТУ»)	Конец сентября-октябрь 2023 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ОРСТ	Конкурс	90
Гражданско-патриотическое	Тематические классные часы по истории студенческих трудовых отрядов СССР и России	октябрь-ноябрь 2023	Кураторы студенческих групп	Лекция	100
Физическое	Участие сборной «МГОТУ» по мини-футболу в Чемпионате г.о. Королёв	ноябрь-февраль 2023 г.	Проректор по МПиВР, начальник ОРСТ	Спортивные соревнования	15

Гражданско-патриотическое	Организация и проведение мероприятия, посвящённого «Дню народного единства»	4 ноября 2023 г.	Проректор по МПиВР, начальник ОРСТ, начальник ООМР	Акция	50
Культурно-просветительское	Фестиваль национальных культур	ноябрь 2023 г.	Проректор по МПиВР, начальник управления	Концерт	170
Культурно-просветительское	Кубок ректора по КВН	декабрь 2023 г.	Проректор по ИПиВР, начальник управления	Конкурс	100
Гражданско-патриотическое	Экскурсия по местам боевой славы Подмосковья	декабрь 2023 г.	Проректор по МПиВР, начальник управления	Экскурсия	42
Физическое	Мероприятия, приуроченные Всемирному дню борьбы со СПИДом	1 декабря 2023 г.	Проректор по МПиВР, начальник управления	Акция	200
Гражданско-патриотическое	Организация и проведение мероприятия, посвящённого международному дню инвалидов	3 декабря 2023 г.	Проректор по МПиВР, начальник ОРСТ, начальник ООМР	Концерт	30
Гражданско-патриотическое	Организация и проведение мероприятия, посвящённого международному дню добровольца	декабрь 2023 г.	Проректор по МПиВР, начальник ОРСТ, начальник ООМР,	Встреча	50
Культурно-просветительское	**Наши традиции.** Организация и проведение игр Лиги КВН «МГОТУ» (1 отборочная игра Лиги КВН «МГОТУ»)	декабрь 2023 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ОРСТ	Конкурс	90
Гражданско-патриотическое	Организация и проведение мероприятия, посвящённого дню Конституции Российской Федерации	12 декабря 2023 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ОРСТ	Викторина	200

Культурно-просветительское	**Наши традиции.** Фестиваль студенческого творчества	декабрь 2023 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ОРСТ, начальник ООМР, деканы, зам. деканов факультетов, зам. по УВР колледжа и техникума	Концерт	150
Культурно-просветительское	Участие сборной КВН «МГОТУ» в 35 Международном Фестивале команд КВН «КИВИН-2024»	январь 2024 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ОРСТ	Конкурс	10
Культурно-просветительское	**Наши традиции.** «День студента – Татьянин день»	январь 2024 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ОРСТ, начальник ООМР, деканы	Концерт	292
Научно-образовательное	Церемония награждения «Золотое сечение» (Подведение итогов конкурсов «МГОТУ»: «Студент года», «Преподаватель года», «Студенческая группа года», «Кафедра года», «Куратор/классный руководитель года», «Студенческое признание года», «Научный руководитель года»	январь 2024 г.	Ректорат, Проректор по МПиВР, начальник Управления по воспит. работе, начальник ОРСТ, начальник ООМР, деканы, зав. кафедр	Церемония награждения	50
Культурно-просветительское	Областной праздник студентов «Татьянин День»	январь 2024 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ОРСТ, начальник ООМР	Концерт	50

Гражданско-патриотическое	Мероприятие, посвящённое Дню памяти о россиянах, исполнявших служебный долг за пределами Отечества	15 февраля 2024 г.	Проректор по МПиВР, начальник Управления, зам. нач. управления, начальник ОРСТ	Встреча	70
Культурно-просветительское	Организация зимнего оздоровительного лагеря для студенческого актива «МГОТУ»	февраль 2024г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ОРСТ, начальник ООМР	Учебные сборы	50
Культурно-просветительское	**Наши традиции.** Организация и проведение игр Лиги КВН «МГОТУ» (2-ая отборочная игра Лиги КВН «МГОТУ»)	февраль 2024 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ОРСТ	Конкурс	60
Культурно-просветительское	Участие команды КВН «МГОТУ» в играх и фестивалях Региональной Подмосковной Лиги КВН	март 2024 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ОРСТ	Конкурс	10
Гражданско-патриотическое	Участие студентов «МГОТУ» в мероприятии посвящённому «Дню воссоединения Крыма с Россией»	18 марта 2024 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ОРСТ, начальник ООМР	Акция	50
Физическое	Кубок «МГОТУ» по мини-футболу, посвященный Дню Космонавтики	март 2024 г.	Проректор по МПиВР, начальник ОРСТ	Спортивные соревнования	15
Культурно-просветительское	**Наши традиции.** Конкурс Мистер и Мисс «МГОТУ»	март 2024 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ОРСТ, начальник ООМР	Конкурс	100

Культурно-просветительское	Участие делегации студентов «МГОТУ» в фестивале «Студенческая весна Подмосковья»	март-апрель 2024 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ОРСТ, начальник ООМР	Конкурс	50
Физическое	Кубок города Королёва по мини-футболу	апрель 2024 г.	Проректор по МПиВР, начальник ОРСТ	Спортивные соревнования	15
Гражданско-патриотическое	Мероприятие, посвященное Дню космонавтики	12 апреля 2024 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ОРСТ, начальник ООМР	Встреча	200
Культурно-просветительское	Участие в Центральной Международной Лиге КВН	апрель 2024 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ОРСТ	Конкурс	10
Экологическое	**Наши традиции** Участие в неделе весенних субботников	апрель 2024 г.	Кураторы учебных групп	Акция	170
Гражданско-патриотическое	Встреча обучающихся МГОТУ с ветераном ВОВ	апрель 2024 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ООМР, начальник ОРСТ, зам. деканов факультетов, зам. директоров подразделений по УВР	Встреча	50
Гражданско-патриотическое	**Великие даты России.** Галерея ветеранов «Знаем. Помним. Гордимся!» - выставка портретов ветеранов-участников ВОВ	апрель-май 2024 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ООМР, начальник ОРСТ, деканы факультетов	Выставка	90
Культурно-просветительское	**Наши традиции.** Организация и проведение игр Лиги КВН «МГОТУ» (3-я отборочная игра Лиги КВН	май 2024 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ОРСТ	Конкурс	80

	«МГОТУ»)				
Гражданско-патриотическое	К 79-й годовщине Великой Победы. Акция «Георгиевская лента»	май 2024 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ООМР, начальник ОРСТ, зам. деканов факультетов	Акция	1000
Гражданско-патриотическое	«Вахта Памяти» - торжественный митинг памяти погибшим в годы Великой отечественной войны	май 2024 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ООМР, начальник ОРСТ, зам. деканов факультетов, зам. директоров подразделений по УВР	Акция памяти	1000
Гражданско-патриотическое	К 79-й годовщине Великой Победы. Участие в городском Параде Победы и Параде «Бессмертный полк»	9 мая 2024 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ООМР, начальник ОРСТ	Парад	100
Гражданско-патриотическое	Организация и проведение мероприятия, посвящённого дню славянской письменности и культуры	24 мая 2024 г.	Зам. директора по УВР колледжа, Студенческий совет Классные руководители	Лекция	90
Гражданско-патриотическое	Участие студентов «МГОТУ» в мероприятиях, посвящённых «Международному дню защиты детей»	1 июня 2024 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ООМР, начальник ОРСТ	Встреча	20
Гражданско-патриотическое	Организация и проведение мероприятия, посвящённого «Дню России»	12 июня 2024 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ООМР, начальник ОРСТ	Викторина	70

Гражданско-патриотическое	Участие в городском празднике «День молодежи»	июнь 2024 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ООМР, начальник ОРСТ	Концерт	50
Гражданско-патриотическое	Участие студентов «МГОТУ» в мероприятиях, посвящённых «Дню памяти и скорби - день начала Великой отечественной войны»	22 июня 2024 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ООМР, начальник ОРСТ	Акция	100
Научно-образовательное	**Наши традиции.** Торжественная церемония вручения дипломов выпускникам «МГОТУ»	Начало июля 2024 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ООМР, начальник ОРСТ, деканы, зам. деканов факультетов	Церемония вручения	500
Гражданско-патриотическое	Участие делегации студентов «МГОТУ» в Московском областном молодёжном форуме «Я - гражданин Подмосковья»	июль 2024 г.	Начальник Управления по воспит. работе, начальник ООМР, начальник ОРСТ	Форум	100
Культурно-просветительское	Участие делегации студентов «МГОТУ» в летнем спортивно-оздоровительном лагере студенческого актива	июль-август 2024 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ООМР, начальник ОРСТ	Учебные сборы	50
Научно-образовательное	Участие в дне открытых дверей. Подготовка презентации для выступления	октябрь, ноябрь 2023 г., март, май 2024 г.	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ООМР, начальник ОРСТ	Встреча	20
Научно-образовательное	Участие в работе стипендиальных комиссий в институтах	1 раз в семестр	Проректор по МПиВР, начальник Управления по воспит. работе	Встреча	
Гражданско-патриотическое	Комплекс мероприятий «Подмосковный Королёв –	в течение года	Проректор по МПиВР	Встреча	

	космическая столица России»				
Научно-образовательное	Оперативные совещания с заместителями деканов по внеучебной работе	в течение года	Проректор по МПиВР	Встреча	
Научно-образовательное	Участие в конференциях по проблемам организации внеучебной деятельности в высших учебных заведениях РФ	в течение года	Проректор по МПиВР	Конференция	
Научно-образовательное	Участие в работе Совета проректоров по внеучебной работе при РФ	в течение года	Проректор по МПиВР	Совещание	
Научно-образовательное	Проведение встреч ректора «МГОТУ» со студентами	в течение года	Проректор по МПиВР	Встреча	
Гражданско-патриотическое	Организация воспитательной работы со студентами, проживающими в общежитии	в течение года	Проректор по МПиВР, начальник ОРСТ	Встреча	
Гражданско-патриотическое	Педагогическое сопровождение детей, оказавшихся в трудной жизненной ситуации	в течение учебного года	Социальные педагоги, педагоги-психологи структурных подразделений	Родительские собрания	
Гражданско-патриотическое	Собрание с первокурсниками в общежитии. Конкурс на «Лучшую комнату в общежитии»	в течение года	Проректор по МПиВР, начальник ОРСТ	Собрание	
Гражданско-патриотическое	Организация обучения совета студенческого общежития	в течение года	Проректор по МПиВР	Семинар	
Научно-образовательное	Выступления на ректоратах и Учёных советах	в течение года	Проректор по МПиВР	Совещание	

Физическое	Участие сборных команд «МГОТУ» по мини-футболу, волейболу и баскетболу в городских, областных и региональных соревнованиях	в течение года	Проректор по МПиВР, начальник ОРСТ	Спортивные соревнования	
Гражданско-патриотическое	Участие в областных, городских мероприятиях патриотической и гражданской направленности	в течение года	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ООМР, начальник ОРСТ	Акция	
Гражданско-патриотическое	Участие студентов-волонтёров в волонтёрских проектах и программах: «Дружба поколений», «Благодарные внуки», «Четвероногий друг»	в течение года	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ООМР, начальник ОРСТ	Проект	
Научно-образовательное	Участие в конкурсе «World Skills» структурные подразделения университета	в течение учебного года	Зам. директоров по УПР структурных подразделений	Конкурс	
Научно-образовательное	Участие в конкурсах студенческих творческих, научных работ и социальных проектов, проводимых в городе, области, России и на международном уровне	в течение года	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ООМР, начальник ОРСТ	Конкурс	
Гражданско-патриотическое	Встречи с представителями городских молодежных организаций и партий (в рамках работы Дискуссионного Полит-клуба)	в течение года	Проректор по МПиВР	Встреча	
Научно-образовательное	Проведение социологических исследований и мониторинга проблем студенческой жизни	в течение года	Проректор по МПиВР, начальник ОСПП	Социологический опрос	
Научно-образовательное	Подготовка фотоотчётов, презентаций на Учёный совет, Ректорат по мероприятиям,	в течение года	Проректор по МПиВР, специалист по УМР отдела ОМР	Информационно-методические материалы	

	проведённым службой проректора по внеучебной и воспитательной работе				
Научно-образовательное	Подготовка и проведение конкурсов: «Студент года», «Группа года», «Куратор года», «Классный руководитель года»	в течение года	Ректорат, проректор по МПиВР	Конкурс	
Научно-образовательное	Проведение собраний для кураторов учебных групп	в течение года	Проректор по МПиВР	Встреча	
Физическое	Товарищеские встречи по мини-футболу	в течение года	Проректор по МПиВР, начальник ОРСТ	Спортивные соревнования	
Физическое	Товарищеские встречи по волейболу	в течение года	Проректор по МПиВР, начальник ОРСТ	Спортивные соревнования	
Физическое	Товарищеские встречи по баскетболу	в течение года	Проректор по МПиВР, начальник ОРСТ	Спортивные соревнования	
Физическое	Участие в спортивных мероприятиях г.о. Королёв (мини-футбол, баскетбол, волейбол, шахматы)	в течение года	Проректор по МПиВР, начальник ОРСТ	Спортивные соревнования	
Физическое	Организация и проведение спортивных мероприятий, приуроченных к праздничным датам (23 февраля, 8 марта, день физкультурника и др.)	в течение года	Проректор по МПиВР, начальник ОРСТ	Спортивные соревнования	

Гражданско-патриотическое	Участие студентов «МГОТУ» в благотворительных акциях	в течение года	Проректор по МПиВР, начальник Управления по ВР, начальник ООМР, начальник ОРСТ, Студ. совет	Акция	
Гражданско-патриотическое	Экскурсии по «Золотому кольцу России»	в течение года	Проректор по МПиВР	Экскурсия	
Гражданско-патриотическое	Экскурсии по местам боевой Славы Подмосковья	в течение года	Проректор по МПиВР	Экскурсия	
Гражданско-патриотическое	Информационная работа о видах социальной поддержки сиротам в «МГОТУ»; Взаимодействие с отделом опеки и попечительства по г.о. Королёв	в течение года	Проректор по МПиВР, ведущий психолог ОСПП	Информационно-методические материалы	
Физическое	Организация просветительской деятельности по тематикам профилактики и пропаганды здорового образа жизни	в течение года	Проректор по МПиВР, начальник ОСПП	Лекция Акция	
Физическое	Участие в областных, городских межвузовских акциях и конференциях «За здоровый образ жизни»	в течение года	Проректор по МПиВР, начальник ОСПП	Акция	
Физическое	Организация профилактической работы совместно с Королёвским наркологическим диспансером,	в течение года	Проректор по МПиВР, начальник ОСПП	Лекция	

	ФСКН, КВД, КДН и ЗП по г.о. Королёв				
Физическое	Круглые столы «Профилактика зависимого поведения»	в течение года	Проректор по МПиВР, начальник ОСПП	Круглый стол	
Физическое	Участие в спортивном празднике в рамках городского антинаркотического марафона	декабрь	Проректор по МПиВР, начальник ОСПП, начальник ОРСТ	Спортивные соревнования	
Физическое	Организация информационно-пропагандистских мероприятий по профилактике дорожно-транспортных происшествий	в течение года	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ООМР, начальник ОРСТ,	Лекция	
Физическое	Реализация Психологической программы «Пропаганда здорового образа жизни и профилактика алкоголизма и наркомании»	в течение года	Проректор по МПиВР, начальник ОСПП	Лекция	
Физическое	Реализация программы «Социально-психологическая помощь студентам «МГОТУ»	в течение года	Проректор по МПиВР, начальник ОСПП	Лекция	
Научно-образовательное	Работа клуба практической психологии	в течение года каждый четверг	Проректор по МПиВР, начальник ОСПП	Тренинг	

Научно-образовательное	Обновление информации по внеучебной работе на сайте, новости на страничке «Телеграмм», «В контакте».	в течение года	Проректор по МПиВР, начальник Управления по воспит. работе, начальник ООМР, начальник ОРСТ, начальник ОСПП	Информационные материалы	

Проректор по молодежной политике и воспитательной работе **В.Н. Минакова**

Воспитательная работа, проводимая в рамках образовательной программы 10.03.01 Информационная безопасность, реализуется также в культурно-массовых и образовательных мероприятиях, организуемых кафедрой Информационной безопасности, и направленных на формирование профессиональных качеств будущих специалистов.

Культурно-массовые и образовательные мероприятия, запланированные кафедрой Информационной безопасности в 2023-2024 учебном году

Направления воспитательной деятельности	Мероприятие, проводимое кафедрой	Примерная дата проведения в 2023-2024 учебном году
Профессионально-трудовое воспитание	Международный день защитника информации	Ноябрь 2023 г.
Профессионально-трудовое воспитание	Профоринетационная работа в школах, гимназиях и учреждениях СПО регионального научно-образовательного кластера «Северо-Восток»	Ноябрь 2023 г. – Апрель 2024 г.
Научно-образовательное воспитание	Участие студентов в ежегодной Всероссийской научно-практической конференции «Русский космизм: история и современность»	Ноябрь-декабрь 2023 г.
Научно-образовательное воспитание	День открытых дверей. Ежегодное участие студентов в организации и проведении мероприятий по анкетированию	Февраль 2024 г.
Научно-образовательное воспитание	День открытых дверей. Ежегодное участие студентов в организации и проведении мероприятий по анкетированию	Февраль-март 2024 г.
Научно-образовательное, профессионально-трудовое воспитание	Образовательно-познавательные экскурсии на предприятия наукограда Королев. Посещение специализированных выставок по ИБ (ЗИ).	Ноябрь 2023-апрель 2024 г.
Профессионально-трудовое воспитание	Деловая игра «Бизнес на связях» с бизнес-тренером по развитию предпринимателей, автором обучающих курсов. Деловые мероприятия в онлайн и оффлайн	Октябрь 2023-апрель 2024 г.

	форматах	
Культурно – просветительское, гражданско-патриотическое воспитание	Ежегодное посещение исторического музея города студентами - первокурсниками	Март-апрель 2024 года

Приложение 5

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ

Б2.В.01 (У) Ознакомительная практика

Б2.В.02 (У) Учебно-лабораторная практика

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Организация и технологии защиты информации
Уровень высшего образования: бакалавриат
Форма обучения: очная, очно-заочная
Год набора: 2023

Королев
2023

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:

- ознакомительная практика;
- учебно-лабораторная 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) Ознакомительная практика:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;

УК-3. Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде;

УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни;

УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности;

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;

ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;

ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;

Б2.В.02 (У) Учебно-лабораторная практика:

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

Итогом проведения учебной практики является овладение студентами навыков использования контрольно-проверочной аппаратуры, программных продуктов, применяемых в управленческих органах, заполнения организационно-распорядительной 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 России;
- Основы российской государственности;
- 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;
- 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.

Трудоемкость ознакомительной практики составляет 108 часов, 3 зачетные единицы. Проводится после первого курса во 2 и 4 семестре, продолжительностью 2 недели для очной и очно-заочной формы обучения соответственно.

Трудоемкость учебно-лабораторной практики составляет 108 часов, 3 зачетные единицы. Проводится после второго курса в 4 и 6 семестре, продолжительностью 2 недели для очной и очно-заочной формы обучения соответственно.

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 источником 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	9

	системы и управление сертификатами в операционной системе ПК.	
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 межсетевого экрана	18
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 B2C («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. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Гришина Наталия Васильевна. - 2; доп. - Москва; Москва: Издательство "ФОРУМ": ООО "Научно-издательский центр ИНФРА-М", 2015. - 240 с. - ДЛЯ СТУДЕНТОВ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ. - ISBN 978-5-00091-007-8. URL: http://znanium.com/go.php?id=491597.
2. Паршин, К. А. Методы и средства проектирования информационных систем и технологий : учебно-методическое пособие / К. А. Паршин. — Екатеринбург : , 2018. — 129 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/121337 (дата обращения: 28.11.2022).
3. Воробейкина, И. В. Программирование средств защиты информации : учебное пособие / И. В. Воробейкина. — Калининград : БГАРФ, 2021. — 70 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/216425 (дата обращения: 28.11.2022).
4. Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844 (дата обращения: 28.11.2022).
5. Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2021. — 172 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176563 (дата обращения: 28.11.2022).
6. Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
7. Пугин, В. В. Защита информации в компьютерных информационных системах : учебное пособие / В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 119 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182299 (дата обращения: 28.11.2022).
8. Моделирование компьютерных сетей в среде NetCracker Professional 4.1 : методические указания / В. В. Пугин, И. С. Макаров, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 46 с. — Текст : электронный // Лань :

электронно-библиотечная система. — URL: https://e.lanbook.com/book/182305 (дата обращения: 28.11.2022).
9. Воробейкина, И. В. Программирование средств защиты информации : учебное пособие / И. В. Воробейкина. — Калининград : БГАРФ, 2021. — 70 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/216425 (дата обращения: 28.11.2022).
10. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : методические указания / Д. В. Фомин. — Благовещенск : АмГУ, 2017. — 240 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156494 (дата обращения: 28.11.2022).
11. Программно-аппаратные средства защиты информации : учебно-методическое пособие / С. И. Штеренберг, А. М. Гельфанд, Д. В. Рыжаков, Р. А. Фатхутдинов. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2017. — 98 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180093 (дата обращения: 28.11.2022).
12. Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону : Донской ГТУ, 2021. — 228 с. — ISBN 978-5-7890-1878-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/237770 (дата обращения: 28.11.2022).
13. Алѐшкин, А. С. Аппаратные и программные средства поиска уязвимостей при моделировании и эксплуатации информационных систем (обеспечение информационной безопасности) : учебное пособие / А. С. Алѐшкин, С. А. Лесько, Д. О. Жуков. — Москва : РТУ МИРЭА, 2020. — 152 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167600 (дата обращения: 28.11.2022).
14. Иванова, С. М. Теория информации. Хранение и передача данных : учебное пособие / С. М. Иванова, З. В. Ильиченкова. — Москва : РТУ МИРЭА, 2022. — 75 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/256583 (дата обращения: 28.11.2022).
15. Иванова, С. М. Теория информации. Моделирование интеллектуальных систем : учебное пособие / С. М. Иванова, З. В. Ильиченкова. — Москва : РТУ МИРЭА, 2020. — 65 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163804 (дата обращения: 28.11.2022).
16. Алдохина, О. И. Информационно-аналитические системы и сети : учебное пособие / О. И. Алдохина. — Кемерово : КемГИК, [б. г.]. — Часть 1 : Информационно-аналитические системы — 2010. — 148 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/49636 (дата обращения: 28.11.2022).

17. Дворовенко, О. В. Информационно-аналитические продукты и услуги: практикум по направлению подготовки 51.03.06 «Библиотечно-информационная деятельность», профиль подготовки «Информационно-аналитическая деятельность», квалификация (степень) выпускника: «бакалавр» : учебное пособие / О. В. Дворовенко. — Кемерово : КемГИК, 2021. — 54 с. — ISBN 978-5-8154-0604-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/250628 (дата обращения: 28.11.2022).
18. Барлаков, С. А. Модели и методы в управлении и экономике с применением информационных технологий : учебное пособие / С. А. Барлаков, С. И. Моисеев, В. Л. Порядина. — Санкт-Петербург : Интермедия, 2016. — 264 с. — ISBN 978-5-4383-0135-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103198 (дата обращения: 28.11.2022).
19. Гришаева, С. А. Информационная безопасность в системах менеджмента качества : учебное пособие / С. А. Гришаева. — Москва : МАИ, 2021. — 63 с. — ISBN 978-5-4316-0804-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/256274 (дата обращения: 28.11.2022).
20. Черемухина, Ю. Ю. Системы менеджмента качества : учебное пособие / Ю. Ю. Черемухина. — Москва : РТУ МИРЭА, 2019. — 95 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/171525 (дата обращения: 28.11.2022).
21. Киреева, Н. В. Аудит информационной безопасности : методические указания / Н. В. Киреева, И. С. Поздняк, О. А. Караулова. — Самара : ПГУТИ, 2019. — 21 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223223 (дата обращения: 28.11.2022).
22. Поздняк, И. С. Экспертные системы оценки информационной безопасности : методические указания / И. С. Поздняк, Н. В. Киреева, О. А. Караулова. — Самара : ПГУТИ, 2019. — 23 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223304 (дата обращения: 28.11.2022).
23. Поздняк, И. С. Экпертные системы оценки ИБ : методические указания / И. С. Поздняк, Н. В. Киреева, О. А. Караулова. — Самара : ПГУТИ, 2020 — Часть 2 — 2019. — 15 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/255566 (дата обращения: 28.11.2022).
24. Техническая защита информации : учебное пособие / А. С. Раков, О. Н. Маслов, О. Ю. Губарева [и др.]. — Самара : ПГУТИ, 2020. — 96 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/255575 (дата обращения: 28.11.2022).
25. Рагозин, Ю. Н. Инженерно-техническая защита информации : учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург : Интермедия, 2018. — 168 с. — ISBN 978-5-4383-0161-5. — Текст : электронный // Лань : электронно-

библиотечная система. — URL: https://e.lanbook.com/book/103203 (дата обращения: 28.11.2022).
26. Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2015. — 256 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110328 (дата обращения: 28.11.2022).
27. Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2012. — 374 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/11381 (дата обращения: 28.11.2022).
28. Конкурентная разведка: технологии и противодействие : учебное пособие / В. И. Аверченков, В. В. Спасенников, В. А. Шкаберин, М. Ю. Рытов. — 2-е изд. — Москва : ФЛИНТА, 2017. — 201 с. — ISBN 978-5-9765-2948-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/92919 (дата обращения: 28.11.2022).
29. Прескотт, Д. Е. Конкурентная разведка: Уроки из окопов / Д. Е. Прескотт, С. Х. Миллер ; перевод А. Лисовского. — Москва : Альпина Паблишер, 2016. — 336 с. — ISBN 5-94599-066-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/95696 (дата обращения: 28.11.2022).
30. Романов, В. Г. Социальная инженерия мошенничества : монография / В. Г. Романов, И. В. Романова. — Чита : ЗабГУ, 2021. — 240 с. — ISBN 978-5-9293-2771-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/271808 (дата обращения: 28.11.2022).
31. Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1 : учебное пособие / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 244 с. — ISBN 978-5-9912-0271-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/5178 (дата обращения: 28.11.2022).
32. Милославская, Н. Г. Серия «Вопросы управление информационной безопасностью". Выпуск 5 : учебное пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 166 с. — ISBN 978-5-9912-0275-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/5182 (дата обращения: 28.11.2022).
33. Милославская, Н. Г. Серия «Вопросы управление информационной безопасностью". Выпуск 4 : учебное пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 214 с. — ISBN 978-5-9912-0274-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/5181 (дата обращения: 28.11.2022).
34. Милославская, Н. Г. Серия «Вопросы управление информационной безопасностью". Выпуск 2 : учебное пособие / Н. Г. Милославская, М. Ю.

Сенаторов, А. И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 130 с. — ISBN 978-5-9912-0272-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/5179 (дата обращения: 28.11.2022).
35. Данилова, М. И. Философия и методология науки и техники : учебно-методические пособия / М. И. Данилова. — Краснодар : КубГАУ, 2020. — 28 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223982 (дата обращения: 28.11.2022).
36. Нежметдинова, Ф. Т. Философия и методология науки : учебно-методическое пособие / Ф. Т. Нежметдинова. — Казань : КГАУ, 2017. — 80 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/146613 (дата обращения: 28.11.2022).
37. Щевьёв, А. А. Современная философия и методология науки : учебное пособие / А. А. Щевьёв. — Рязань : РГРТУ, 2017. — 48 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/168300 (дата обращения: 28.11.2022).

Дополнительная литература:

1. Кибербезопасность в условиях электронного банкинга : практическое пособие / под ред. П. В. Ревенкова. - Москва : Прометей, 2020. - 522 с. - ISBN 978-5-907244-61-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1284190 (дата обращения: 28.11.2022).
2. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 320 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: https://doi.org/10.29039/01848-4. - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232287 (дата обращения: 28.11.2022).
3. Тавасиев, А. М. Банковское кредитование : учебник / А.М. Тавасиев, Т.Ю. Мазурина, В.П. Бычков ; под ред. А.М. Тавасиева. — 2-е изд., перераб. — Москва : ИНФРА-М, 2020. — 366 с. — (Среднее профессиональное образование). - ISBN 978-5-16-014239-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1039295 (дата обращения: 28.11.2022).
4. Научные исследования при выполнении магистерских выпускных квалификационных работ : учебное пособие / сост. Ю. А. Андреев, А. А. Мельник, П. В. Ширпнкпн, А. Н. Батуро. - Железногорск : ФГБОУ ВО СПСА ГПС МЧС России, 2020. - 146 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1202011 (дата обращения: 30.11.2022).
5. Менеджмент: выпускная квалификационная работа магистранта : учебное пособие / под общ. ред. д-ра экон. наук, проф. С.Д. Резника, канд. техн. наук, проф. В.В. Двоеглазова. — 4-е изд., перераб. и доп. — Москва : ИНФРА-М, 2022. — 277 с. — (Высшее образование: Магистратура). — DOI 10.12737/1842132. - ISBN 978-5-16-017304-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1842132 (дата обращения: 30.11.2022).

6. Бойко, Г. М. Математические методы и информационные технологии в научных исследованиях : практикум для организации самостоятельной работы адъюнктов, обучающихся дисциплине «Математические методы и информационные технологии в научных исследованиях» направление подготовки 20.07.01 Техносферная безопасность (Адъюнктура) / Г. М. Бойко. - Железногорск : ФГБОУ ВО Сибирская пожарно-спасательная академия ГПС МЧС России, 2021. - 99 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1844131 (дата обращения: 30.11.2022).
7. Землянский, А. А. Управление информационными ресурсами в научно-исследовательской работе : учебное пособие / А. А. Землянский, И. Е. Быстренина. - 2-е изд. - Москва : Дашков и К, 2021. - 110 с. - ISBN 978-5-394-04149-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232484 (дата обращения: 30.11.2022).
8. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016583-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1898839 (дата обращения: 30.11.2022).
9. Конфиденциальное делопроизводство и защищенный электронный документооборот : учебник / Н. Н. Куняев, А. С. Дёмушкин, Т. В. Кондрашова, А. Г. Фабричнов ; под общ. ред. Н. Н. Куняева. - 2-е изд., перераб. и доп. - Москва : Логос, 2020. - 500 с. - (Новая университетская библиотека). - ISBN 978-5-98704-711-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1212394 (дата обращения: 30.11.2022).
10. Раздорожный, А. А. Документирование управленческой деятельности : учеб. пособие / А.А. Раздорожный. — Москва : ИНФРА-М, 2018. — 304 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-011744-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/969585 (дата обращения: 30.11.2022).
11. Информационные технологии в документационном обеспечении управления и архивном деле : учебник для вузов / Н. Н. Кунаев, Т. В. Кондрашова, Е. В. Терентьева, А. Г. Фабричнов / под общ. ред. Н. Н. Куняева. - Москва : Логос, 2020. - 408 с. - ISBN 978-5-98704-786-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1211641 (дата обращения: 30.11.2022).
12. Бондарчук, Н. В. Бизнес-разведка. Практикум : учебное пособие / Н. В. Бондарчук, А. А. Курашова. - Москва : Дашков и К, 2020. - 138 с. - ISBN 978-5-394-03857-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1231982 (дата обращения: 30.11.2022).
13. Бизнес-анализ деятельности организации : учебник / Л.Н. Усенко, Ю.Г. Чернышева, Л.В. Гончарова [и др.] ; под ред. проф. Л.Н. Усенко. — Москва : Альфа-М : ИНФРА-М, 2021. — 560 с. : ил. + Доп. материалы [Электронный ресурс; Режим доступа: http://www.znanium.com]. — (Магистратура). - ISBN 978-5-98281-358-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1245073 (дата обращения: 30.11.2022).

14. Карминский, А. М. Методология создания информационных систем : учебное пособие / А. М. Карминский, Б. В. Черников. - 2-е изд., перераб. и доп. - Москва : ФОРУМ : ИНФРА-М, 2020. - 320 с. : ил. - (Высшее образование). - ISBN 978-5-8199-0494-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1043095 (дата обращения: 30.11.2022).
15. Аверченков, В. И. Аудит информационной безопасности [электронный ресурс] : учеб. пособие для вузов / В. И. Аверченков. – 2-е изд., стереотип. – Москва : Флинта, 2011. – 269 с. - ISBN 978-5-9765-1256-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/453734 (дата обращения: 30.11.2022).
16. Кибербезопасность в условиях электронного банкинга : практическое пособие / под ред. П. В. Ревенкова. - Москва : Прометей, 2020. - 522 с. - ISBN 978-5-907244-61-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1284190 (дата обращения: 30.11.2022).
17. Организация деятельности коммерческого банка : учебник / Е.А. Звонова, М.А. Белецкий, М.Ю. Богачева, О.Ю. Дадашева ; под ред. Е.А. Звоновой — М. : Инфра-М, 2018. — 632 с. — (Высшее образование). - ISBN 978-5-16-005404-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/920530 (дата обращения: 30.11.2022).
18. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2022. — 327 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1035570. - ISBN 978-5-16-015471-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1865598 (дата обращения: 30.11.2022).
19. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 320 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: https://doi.org/10.29039/01848-4. - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232287 (дата обращения: 30.11.2022).
20. Зверева, В. П. Участие в планировании и организации работ по обеспечению защиты объекта : учебник / В.П. Зверева, А.В. Назаров. — Москва : КУРС : ИНФРА-М, 2020. — 320 с. - ISBN 978-5-906818-92-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1055808 (дата обращения: 30.11.2022).
21. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами : монография / А. И. Белоус, В. А. Солодуха. - Москва ; Вологда : Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167736 (дата обращения: 30.11.2022).
22. Баранова, Е. К. Актуальные вопросы защиты информации : монография / А.В. Бабаш, Е.К. Баранова. — Москва : РИОР : ИНФРА-М, 2022. — 111 с. — (Научная мысль). — https://doi.org/10.12737/monography_58dbc380aa3a4. - ISBN 978-5-369-01680-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1878666 (дата обращения: 30.11.2022).

23. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1210523 (дата обращения: 30.11.2022).
24. Рычаго, М. Е. Основы защиты информации : учебное пособие / М. Е. Рычаго, И. В. Ершова, Р. Н. Тихомиров. - Владимир : ВЮИ ФСИН России, 2017. - 68 с. - ISBN 978-5-93035-622-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1864501 (дата обращения: 30.11.2022).
25. Кабашов, С. Ю. Электронное правительство. Электронный документооборот. Термины и определения : учебное пособие / С.Ю. Кабашов. — Москва : ИНФРА-М, 2021. — 320 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-006835-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1132150 (дата обращения: 30.11.2022).
26. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов / Ю. Н. Сычев. - Москва : ИНФРА-М, 2021. - 223 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016533-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1178148 (дата обращения: 30.11.2022).
27. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 223 с. — (Среднее профессиональное образование). - ISBN 978-5-16-015718-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189348 (дата обращения: 30.11.2022).
28. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 223 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/textbook_5cc15bb22f5345.11209330. - ISBN 978-5-16-014397-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189349 (дата обращения: 30.11.2022).
29. Урбанович, П. П. Компьютерные сети : учебное пособие / П. П. Урбанович, Д. М. Романенко. - Москва ; Вологда : Инфра-Инженерия, 2022. - 460 с. - ISBN 978-5-9729-0962-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1902692 (дата обращения: 30.11.2022).
30. Зверева, В. П. Организация и технология работы с конфиденциальными документами : учеб. пособие / В.П. Зверева, А.В. Назаров. — Москва : КУРС: ИНФРА-М, 2018. - 320 с. - (Среднее профессиональное образование). - ISBN 978-5-906818-96-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/754287 (дата обращения: 30.11.2022).
31. Правовое регулирования искусственного интеллекта, роботов и объектов робототехники как условие формирования экономического лидерства в России : монография / Г. Ф. Ручкина, М. В. Демченко, А. В. Попова [и др.] ; под ред. Г.Ф. Ручкиной. - Москва : Прометей, 2021. - 350 с. - ISBN 978-5-00172-197-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1851280 (дата обращения: 30.11.2022).

32. Куняев, Н. Н. Документоведение : учебник / Н. Н. Куняев, Д. Н. Уралов, А. Г. Фабричной ; под ред. проф. Н. Н. Кунаева. - 2-е изд., стер. - Москва : Логос, 2020. - 352 с. - (Новая университетская библиотека). - ISBN 978-5-98704-329-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1211628 (дата обращения: 30.11.2022).
33. Бабаш, А. В. История защиты информации в зарубежных странах : учебное пособие / А.В. Бабаш, Д.А. Ларин. — Москва : РИОР : ИНФРА-М, 2021. — 284 с. — (Высшее образование). — DOI: https://doi.org/10.12737/15090. - ISBN 978-5-369-01844-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1215133 (дата обращения: 30.11.2022).
34. Электронный документооборот и обеспечение безопасности стандартными средствами WINDOWS : учебное пособие / Л.М. Евдокимова, В.В. Корябкин, А.Н. Пылькин, О.Г. Швечкова. - Москва : КУРС, 2023. - 296 с. - ISBN 978-5-906923-24-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1902497 (дата обращения: 30.11.2022).
35. Богульская, Н. А. Модели безопасности компьютерных систем : учебное пособие / Н. А. Богульская, М. М. Кучеров. - Красноярск : Сиб. федер. ун-т, 2019. - 206 с. - ISBN 978-5-7638-4008-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1819309 (дата обращения: 30.11.2022).
36. Беловицкий, К. Б. Основные методы выявления фактов коммерческого шпионажа : учебное пособие / К. Б. Беловицкий. - Москва : Дашков и К, 2021. - 345 с. - ISBN 978-5-394-04261-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1926415 (дата обращения: 30.11.2022).
37. Информационные технологии в документационном обеспечении управления и архивном деле : учебник для вузов / Н. Н. Кунаев, Т. В. Кондрашова, Е. В. Терентьева, А. Г. Фабричнов / под общ. ред. Н. Н. Куняева. - Москва : Логос, 2020. - 408 с. - ISBN 978-5-98704-786-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1211641 (дата обращения: 30.11.2022).
38. Моргунов, А. В. Электронные системы документооборота : учебное пособие / А. В. Моргунов. - Новосибирск : Изд-во НГТУ, 2020. - 74 с. - ISBN 978-5-7782-4269-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1870515 (дата обращения: 30.11.2022).

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;

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).

Приложение 6

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Б2.В.03 (П) Технологическая практика

Б2.О.01 (П) Преддипломная

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Год набора: 2023

Королев
2023

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:

- 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», 4 ЦНИИ МО, ООО»НОВО», НТЦ «ЗАРЯ», ООО «ЦБИ» 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;4 ЦНИИ МО; ООО «ТехЗИ»;ЗАО «КЛИО»; ООО НОВО», НТЦ «ЗАРЯ» «ООО «ЦБИ», 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 (П) Технологическая практика

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

Б2.О.01 (П) Преддипломная практика

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;

ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;
ДОПК-1. Способен проводить анализ функционального процесса объекта информатизации с целью выявления возможных угроз, их вероятных целей, путей реализации и предполагаемого ущерба;
ДОПК-2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;
ДОПК-3. Способен разработать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;
ДОПК-4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами

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 относятся к обязательному разделу ОПОП ВО по направлению подготовки 10.03.01. «Информационная безопасность» и базируется на ранее изученных дисциплинах:

Блок 1. Дисциплины (модули)
Обязательная часть
Б1.О..01 Философия
Б1.О.02 История Росси
Б1.О.03 Основы российской государственности
Б1.О.04 Иностранный язык
Б1.О.05 Безопасность жизнедеятельности
Б1.О.06 Физическая культура
Б1.О.07 Русский язык и культура речи
Б1.О.08 Основы управленческой деятельности
Б1.О.09 Документоведение
Б1.О.10 Экономика предприятия и организация производства

Б1.О.11 Группа учебных дисциплин (модулей) "Математические основы обеспечения информационной безопасности":
Б1.О.11.01 Линейная алгебра и аналитическая геометрия
Б1.О.11.02 Математический анализ

Б1.О.11.03 Теория графов
Б1.О.11.04 Теория информации
Б1.Б.11.05 Теория вероятностей и математическая статистика
Б1.О.11.06 Дискретная математика

Б1.О.12 Группа учебных дисциплин (модулей) "Физико-технические основы обеспечения информационной безопасности":
Б1.О.12.01 Физика
Б1.О.12.02 Электротехника
Б1.О.12.03 Электроника и схемотехника
Б1.Б.13 Группа учебных дисциплин (модулей) "Информационные технологии":
Б1.О.13.01 Информатика
Б1.О.13.02 Языки программирования
Б1.О.13.03 Технологии и методы программирования
Б1.О.13.04 Информационные технологии
Б1.О.13.05 Аппаратные средства вычислительной техники
Б1.О.13.06 Сети и системы передачи информации

Б1.О.14 Группа учебных дисциплин (модулей) "Методы и средства обеспечения информационной безопасности":
Б1.О.14.01 Основы информационной безопасности
Б1.О.14.02 Организационное и правовое обеспечение информационной безопасности
Б1.О.14.03 Основы управления информационной безопасностью
Б1.Б.14.04 Защита информации от утечки по техническим каналам
Б1.О.14.05 Методы и средства криптографической защиты информации
Б1.О.14.06 Программно-аппаратные средства защиты информации
Б1.Б.14.07 Комплексное обеспечение защиты информации объекта информатизации (предприятия)

Б1.О.15 Дисциплины (модули) профиля: "Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)":
Б1.О.15.01 Математическая логика и теория алгоритмов
Б1.О.15.02 Информационные процессы и системы как объекты информационной безопасности
Б1.О.15.03 Конфиденциальное делопроизводство и защищённый электронный документооборот
Б1.О.15.04 Нормативные акты и стандарты по информационной безопасности
Б1.О.15.05 Организация системы обеспечения информационной безопасности (служба ИБ)
Б1.О.15.06 Физическая защита информационных объектов
Б1.О.15.07 Информационно-аналитическая деятельность по обеспечению комплексной безопасности
Б1.О.15.08 Экономика информационной безопасности
Б1.О.15.09 Моделирование процессов и систем защиты информации

Б1.О.16 Элективные курсы по физической культуре и спорту
Б1.О.17 Основы военной подготовки

Часть, формируемая участниками образовательных отношений
Б1.В.01 Дисциплины (модули) образовательной организации:
Б1.В.01.01 Основы исследований информационной безопасности
Б1.В.01.02 Пакеты прикладных программ
Б1.В.01.03 Социально-психологические основы управленческой деятельности
Б1.В.01.04 Основы конкурентной разведки
Б1.В.01.05 История защиты информации в РФ
Б1.В.01.06 Информационная безопасность автоматизированных систем
Б1.В.02 Основы права
Б1.В.03 Безопасность информационных технологий
Б1.В.04 Гуманитарные аспекты (профессиональная этика) информационной безопасности

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 Подготовка объекта информатизации к аттестации по требованиям безопасности информации (ООО «НОВО»)
Б1.В.ДВ.03.04 Аттестация объекта информатизации по требованиям безопасности информации (ООО "ЦБИ")

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 (ООО «НОВО»)
Б1.В.ДВ.04.04 Защита информации от НСД (ООО «ЦБИ»)

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 (ООО «НОВО»)
Б1.В.ДВ.05.04 Контроль защищенности информации от утечки по техническим каналам (ООО "ЦБИ")

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 (ООО «НОВО»)
Б1.В.ДВ.06.04 Средства защиты информации и оценка эффективности защиты от утечки по техническим каналам (ООО "ЦБИ")

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 Технические каналы утечки конфиденциальной информации (ООО «НОВО»)
Б1.В.ДВ.07.04 Технические каналы утечки информации (ООО "ЦБИ")

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 (ООО «НОВО»)
Б1.В.ДВ.08.04 Разработка и сертификация средств защиты информации и технических средств в защищенном исполнении (ООО "ЦБИ")

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 (ООО «НОВО»)
Б1.В.ДВ.09.04 Методы и средства обеспечения защищенности информации от несанкционированного доступа (ООО "ЦБИ")

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 (ООО «НОВО», ООО «ЦБИ»)

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
Обязательная часть

Б2.О.01(П) Преддипломная практика

Часть, формируемая участниками образовательных отношений
Б2.В.01(У) Ознакомительная практика
Б2.В.02(У) Учебно-лабораторная практика
Б2.В.03(П) Технологическая практика

Блок 3. Государственная итоговая аттестация
Б3.Б.01(Д) Подготовка и защита ВКР

ФТД. Факультативные дисциплины
ФТД..01 Технико-экономическое обоснование проекта
ФТД 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.

Трудоемкость производственной технологической практики составляет 108 часов, 3 зачетные единицы. Проводится после третьего курса в 6 семестре для очной и в 8 семестре для очно-заочной формы обучения, продолжительностью 2 недели.

Трудоемкость производственной преддипломной практики составляет 324 часа, 9 зачетных единиц. Проводится после четвертого курса в 8 семестре для очной формы обучения и после пятого курса в 10 семестре для очно-заочной 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 источником 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.	1

	Написание раздела отчета.	
4	Описание организационной структуры предприятия: схема, количество отделов и их название, их функции, подчиненность, взаимодействие. Написание раздела отчета.	1
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	1

	рабочем месте ознакомление с современными средствами вычислительной техники, коммуникаций и связи, используемых в процессе обучения.	
3	Краткая характеристика используемых методов по защите информации и программных продуктов, используемых при отработке практических заданий	2
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 B2C («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 управление 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 инструкций 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

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для прохождения практики (модуля)

Основная литература:

38. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Гришина Наталия Васильевна. - 2; доп. - Москва; Москва: Издательство "ФОРУМ": ООО "Научно-издательский центр ИНФРА-М", 2015. - 240 с. - ДЛЯ СТУДЕНТОВ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ. - ISBN 978-5-00091-007-8. URL: http://znanium.com/go.php?id=491597.

39. Паршин, К. А. Методы и средства проектирования информационных систем и технологий : учебно-методическое пособие / К. А. Паршин. —

Екатеринбург : , 2018. — 129 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/121337 (дата обращения: 28.11.2022).
40. Воробейкина, И. В. Программирование средств защиты информации : учебное пособие / И. В. Воробейкина. — Калининград : БГАРФ, 2021. — 70 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/216425 (дата обращения: 28.11.2022).
41. Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844 (дата обращения: 28.11.2022).
42. Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2021. — 172 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176563 (дата обращения: 28.11.2022).
43. Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
44. Пугин, В. В. Защита информации в компьютерных информационных системах : учебное пособие / В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 119 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182299 (дата обращения: 28.11.2022).
45. Моделирование компьютерных сетей в среде NetCracker Professional 4.1 : методические указания / В. В. Пугин, И. С. Макаров, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 46 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182305 (дата обращения: 28.11.2022).
46. Воробейкина, И. В. Программирование средств защиты информации : учебное пособие / И. В. Воробейкина. — Калининград : БГАРФ, 2021. — 70 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/216425 (дата обращения: 28.11.2022).
47. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : методические указания / Д. В. Фомин. — Благовещенск : АмГУ, 2017. — 240 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156494 (дата обращения: 28.11.2022).
48. Программно-аппаратные средства защиты информации : учебно-методическое пособие / С. И. Штеренберг, А. М. Гельфанд, Д. В. Рыжаков, Р. А. Фатхутдинов. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2017. — 98 с. — Текст : электронный // Лань : электронно-библиотечная

система. — URL: https://e.lanbook.com/book/180093 (дата обращения: 28.11.2022).
49. Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону : Донской ГТУ, 2021. — 228 с. — ISBN 978-5-7890-1878-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/237770 (дата обращения: 28.11.2022).
50. Алѐшкин, А. С. Аппаратные и программные средства поиска уязвимостей при моделировании и эксплуатации информационных систем (обеспечение информационной безопасности) : учебное пособие / А. С. Алѐшкин, С. А. Лесько, Д. О. Жуков. — Москва : РТУ МИРЭА, 2020. — 152 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167600 (дата обращения: 28.11.2022).
51. Иванова, С. М. Теория информации. Хранение и передача данных : учебное пособие / С. М. Иванова, З. В. Ильиченкова. — Москва : РТУ МИРЭА, 2022. — 75 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/256583 (дата обращения: 28.11.2022).
52. Иванова, С. М. Теория информации. Моделирование интеллектуальных систем : учебное пособие / С. М. Иванова, З. В. Ильиченкова. — Москва : РТУ МИРЭА, 2020. — 65 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163804 (дата обращения: 28.11.2022).
53. Алдохина, О. И. Информационно-аналитические системы и сети : учебное пособие / О. И. Алдохина. — Кемерово : КемГИК, [б. г.]. — Часть 1 : Информационно-аналитические системы — 2010. — 148 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/49636 (дата обращения: 28.11.2022).
54. Дворовенко, О. В. Информационно-аналитические продукты и услуги: практикум по направлению подготовки 51.03.06 «Библиотечно-информационная деятельность», профиль подготовки «Информационно-аналитическая деятельность», квалификация (степень) выпускника: «бакалавр» : учебное пособие / О. В. Дворовенко. — Кемерово : КемГИК, 2021. — 54 с. — ISBN 978-5-8154-0604-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/250628 (дата обращения: 28.11.2022).
55. Барлаков, С. А. Модели и методы в управлении и экономике с применением информационных технологий : учебное пособие / С. А. Барлаков, С. И. Моисеев, В. Л. Порядина. — Санкт-Петербург : Интермедия, 2016. — 264 с. — ISBN 978-5-4383-0135-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103198 (дата обращения: 28.11.2022).
56. Гришаева, С. А. Информационная безопасность в системах менеджмента качества : учебное пособие / С. А. Гришаева. — Москва : МАИ, 2021. — 63 с. — ISBN 978-5-4316-0804-9. — Текст : электронный // Лань : электронно-

библиотечная система. — URL: https://e.lanbook.com/book/256274 (дата обращения: 28.11.2022).
57. Черемухина, Ю. Ю. Системы менеджмента качества : учебное пособие / Ю. Ю. Черемухина. — Москва : РТУ МИРЭА, 2019. — 95 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/171525 (дата обращения: 28.11.2022).
58. Киреева, Н. В. Аудит информационной безопасности : методические указания / Н. В. Киреева, И. С. Поздняк, О. А. Караулова. — Самара : ПГУТИ, 2019. — 21 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223223 (дата обращения: 28.11.2022).
59. Поздняк, И. С. Экспертные системы оценки информационной безопасности : методические указания / И. С. Поздняк, Н. В. Киреева, О. А. Караулова. — Самара : ПГУТИ, 2019. — 23 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223304 (дата обращения: 28.11.2022).
60. Поздняк, И. С. Экпертные системы оценки ИБ : методические указания / И. С. Поздняк, Н. В. Киреева, О. А. Караулова. — Самара : ПГУТИ, 2020 — Часть 2 — 2019. — 15 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/255566 (дата обращения: 28.11.2022).
61. Техническая защита информации : учебное пособие / А. С. Раков, О. Н. Маслов, О. Ю. Губарева [и др.]. — Самара : ПГУТИ, 2020. — 96 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/255575 (дата обращения: 28.11.2022).
62. Рагозин, Ю. Н. Инженерно-техническая защита информации : учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург : Интермедия, 2018. — 168 с. — ISBN 978-5-4383-0161-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103203 (дата обращения: 28.11.2022).
63. Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2015. — 256 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110328 (дата обращения: 28.11.2022).
64. Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2012. — 374 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/11381 (дата обращения: 28.11.2022).
65. Конкурентная разведка: технологии и противодействие : учебное пособие / В. И. Аверченков, В. В. Спасенников, В. А. Шкаберин, М. Ю. Рытов. — 2-е изд. — Москва : ФЛИНТА, 2017. — 201 с. — ISBN 978-5-9765-2948-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/92919 (дата обращения: 28.11.2022).
66. Прескотт, Д. Е. Конкурентная разведка: Уроки из окопов / Д. Е. Прескотт, С. Х. Миллер ; перевод А. Лисовского. — Москва : Альпина

Паблишер, 2016. — 336 с. — ISBN 5-94599-066-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/95696 (дата обращения: 28.11.2022).
67. Романов, В. Г. Социальная инженерия мошенничества : монография / В. Г. Романов, И. В. Романова. — Чита : ЗабГУ, 2021. — 240 с. — ISBN 978-5-9293-2771-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/271808 (дата обращения: 28.11.2022).
68. Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1 : учебное пособие / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 244 с. — ISBN 978-5-9912-0271-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/5178 (дата обращения: 28.11.2022).
69. Милославская, Н. Г. Серия «Вопросы управление информационной безопасностью". Выпуск 5 : учебное пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 166 с. — ISBN 978-5-9912-0275-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/5182 (дата обращения: 28.11.2022).
70. Милославская, Н. Г. Серия «Вопросы управление информационной безопасностью". Выпуск 4 : учебное пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 214 с. — ISBN 978-5-9912-0274-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/5181 (дата обращения: 28.11.2022).
71. Милославская, Н. Г. Серия «Вопросы управление информационной безопасностью". Выпуск 2 : учебное пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 130 с. — ISBN 978-5-9912-0272-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/5179 (дата обращения: 28.11.2022).
72. Данилова, М. И. Философия и методология науки и техники : учебно-методические пособия / М. И. Данилова. — Краснодар : КубГАУ, 2020. — 28 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223982 (дата обращения: 28.11.2022).
73. Нежметдинова, Ф. Т. Философия и методология науки : учебно-методическое пособие / Ф. Т. Нежметдинова. — Казань : КГАУ, 2017. — 80 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/146613 (дата обращения: 28.11.2022).
74. Щевьёв, А. А. Современная философия и методология науки : учебное пособие / А. А. Щевьёв. — Рязань : РГРТУ, 2017. — 48 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/168300 (дата обращения: 28.11.2022).

Дополнительная литература:

39. Кибербезопасность в условиях электронного банкинга : практическое пособие / под ред. П. В. Ревенкова. - Москва : Прометей, 2020. - 522 с. - ISBN 978-5-907244-61-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1284190 (дата обращения: 28.11.2022).
40. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 320 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: https://doi.org/10.29039/01848-4. - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232287 (дата обращения: 28.11.2022).
41. Тавасиев, А. М. Банковское кредитование : учебник / А.М. Тавасиев, Т.Ю. Мазурина, В.П. Бычков ; под ред. А.М. Тавасиева. — 2-е изд., перераб. — Москва : ИНФРА-М, 2020. — 366 с. — (Среднее профессиональное образование). - ISBN 978-5-16-014239-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1039295 (дата обращения: 28.11.2022).
42. Научные исследования при выполнении магистерских выпускных квалификационных работ : учебное пособие / сост. Ю. А. Андреев, А. А. Мельник, П. В. Ширпнкпн, А. Н. Батуро. - Железногорск : ФГБОУ ВО СПСА ГПС МЧС России, 2020. - 146 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1202011 (дата обращения: 30.11.2022).
43. Менеджмент: выпускная квалификационная работа магистранта : учебное пособие / под общ. ред. д-ра экон. наук, проф. С.Д. Резника, канд. техн. наук, проф. В.В. Двоеглазова. — 4-е изд., перераб. и доп. — Москва : ИНФРА-М, 2022. — 277 с. — (Высшее образование: Магистратура). — DOI 10.12737/1842132. - ISBN 978-5-16-017304-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1842132 (дата обращения: 30.11.2022).
44. Бойко, Г. М. Математические методы и информационные технологии в научных исследованиях : практикум для организации самостоятельной работы адъюнктов, обучающихся дисциплине «Математические методы и информационные технологии в научных исследованиях» направление подготовки 20.07.01 Техносферная безопасность (Адъюнктура) / Г. М. Бойко. - Железногорск : ФГБОУ ВО Сибирская пожарно-спасательная академия ГПС МЧС России, 2021. - 99 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1844131 (дата обращения: 30.11.2022).
45. Землянский, А. А. Управление информационными ресурсами в научно-исследовательской работе : учебное пособие / А. А. Землянский, И. Е. Быстренина. - 2-е изд. - Москва : Дашков и К, 2021. - 110 с. - ISBN 978-5-394-04149-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232484 (дата обращения: 30.11.2022).
46. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016583-7. - Текст :

электронный. - URL: https://znanium.com/catalog/product/1898839 (дата обращения: 30.11.2022).
47. Конфиденциальное делопроизводство и защищенный электронный документооборот : учебник / Н. Н. Куняев, А. С. Дёмушкин, Т. В. Кондрашова, А. Г. Фабричнов ; под общ. ред. Н. Н. Куняева. - 2-е изд., перераб. и доп. - Москва : Логос, 2020. - 500 с. - (Новая университетская библиотека). - ISBN 978-5-98704-711-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1212394 (дата обращения: 30.11.2022).
48. Раздорожный, А. А. Документирование управленческой деятельности : учеб. пособие / А.А. Раздорожный. — Москва : ИНФРА-М, 2018. — 304 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-011744-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/969585 (дата обращения: 30.11.2022).
49. Информационные технологии в документационном обеспечении управления и архивном деле : учебник для вузов / Н. Н. Кунаев, Т. В. Кондрашова, Е. В. Терентьева, А. Г. Фабричнов / под общ. ред. Н. Н. Куняева. - Москва : Логос, 2020. - 408 с. - ISBN 978-5-98704-786-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1211641 (дата обращения: 30.11.2022).
50. Бондарчук, Н. В. Бизнес-разведка. Практикум : учебное пособие / Н. В. Бондарчук, А. А. Курашова. - Москва : Дашков и К, 2020. - 138 с. - ISBN 978-5-394-03857-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1231982 (дата обращения: 30.11.2022).
51. Бизнес-анализ деятельности организации : учебник / Л.Н. Усенко, Ю.Г. Чернышева, Л.В. Гончарова [и др.] ; под ред. проф. Л.Н. Усенко. — Москва : Альфа-М : ИНФРА-М, 2021. — 560 с. : ил. + Доп. материалы [Электронный ресурс; Режим доступа: http://www.znanium.com]. — (Магистратура). - ISBN 978-5-98281-358-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1245073 (дата обращения: 30.11.2022).
52. Карминский, А. М. Методология создания информационных систем : учебное пособие / А. М. Карминский, Б. В. Черников. - 2-е изд., перераб. и доп. - Москва : ФОРУМ : ИНФРА-М, 2020. - 320 с. : ил. - (Высшее образование). - ISBN 978-5-8199-0494-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1043095 (дата обращения: 30.11.2022).
53. Аверченков, В. И. Аудит информационной безопасности [электронный ресурс] : учеб. пособие для вузов / В. И. Аверченков. – 2-е изд., стереотип. – Москва : Флинта, 2011. – 269 с. - ISBN 978-5-9765-1256-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/453734 (дата обращения: 30.11.2022).
54. Кибербезопасность в условиях электронного банкинга : практическое пособие / под ред. П. В. Ревенкова. - Москва : Прометей, 2020. - 522 с. - ISBN 978-5-907244-61-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1284190 (дата обращения: 30.11.2022).
55. Организация деятельности коммерческого банка : учебник / Е.А. Звонова, М.А. Белецкий, М.Ю. Богачева, О.Ю. Дадашева ; под ред. Е.А.

Звоновой — М. : Инфра-М, 2018. — 632 с. — (Высшее образование). - ISBN 978-5-16-005404-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/920530 (дата обращения: 30.11.2022).
56. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2022. — 327 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1035570. - ISBN 978-5-16-015471-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1865598 (дата обращения: 30.11.2022).
57. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 320 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: https://doi.org/10.29039/01848-4. - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232287 (дата обращения: 30.11.2022).
58. Зверева, В. П. Участие в планировании и организации работ по обеспечению защиты объекта : учебник / В.П. Зверева, А.В. Назаров. — Москва : КУРС : ИНФРА-М, 2020. — 320 с. - ISBN 978-5-906818-92-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1055808 (дата обращения: 30.11.2022).
59. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами : монография / А. И. Белоус, В. А. Солодуха. - Москва ; Вологда : Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167736 (дата обращения: 30.11.2022).
60. Баранова, Е. К. Актуальные вопросы защиты информации : монография / А.В. Бабаш, Е.К. Баранова. — Москва : РИОР : ИНФРА-М, 2022. — 111 с. — (Научная мысль). — https://doi.org/10.12737/monography_58dbc380aa3a4. - ISBN 978-5-369-01680-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1878666 (дата обращения: 30.11.2022).
61. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1210523 (дата обращения: 30.11.2022).
62. Рычаго, М. Е. Основы защиты информации : учебное пособие / М. Е. Рычаго, И. В. Ершова, Р. Н. Тихомиров. - Владимир : ВЮИ ФСИН России, 2017. - 68 с. - ISBN 978-5-93035-622-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1864501 (дата обращения: 30.11.2022).
63. Кабашов, С. Ю. Электронное правительство. Электронный документооборот. Термины и определения : учебное пособие / С.Ю. Кабашов. — Москва : ИНФРА-М, 2021. — 320 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-006835-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1132150 (дата обращения: 30.11.2022).
64. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов / Ю. Н. Сычев. - Москва : ИНФРА-

М, 2021. - 223 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016533-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1178148 (дата обращения: 30.11.2022).
65. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 223 с. — (Среднее профессиональное образование). - ISBN 978-5-16-015718-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189348 (дата обращения: 30.11.2022).
66. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 223 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/textbook_5cc15bb22f5345.11209330. - ISBN 978-5-16-014397-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189349 (дата обращения: 30.11.2022).
67. Урбанович, П. П. Компьютерные сети : учебное пособие / П. П. Урбанович, Д. М. Романенко. - Москва ; Вологда : Инфра-Инженерия, 2022. - 460 с. - ISBN 978-5-9729-0962-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1902692 (дата обращения: 30.11.2022).
68. Зверева, В. П. Организация и технология работы с конфиденциальными документами : учеб. пособие / В.П. Зверева, А.В. Назаров. — Москва : КУРС: ИНФРА-М, 2018. - 320 с. - (Среднее профессиональное образование). - ISBN 978-5-906818-96-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/754287 (дата обращения: 30.11.2022).
69. Правовое регулирования искусственного интеллекта, роботов и объектов робототехники как условие формирования экономического лидерства в России : монография / Г. Ф. Ручкина, М. В. Демченко, А. В. Попова [и др.] ; под ред. Г.Ф. Ручкиной. - Москва : Прометей, 2021. - 350 с. - ISBN 978-5-00172-197-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1851280 (дата обращения: 30.11.2022).
70. Куняев, Н. Н. Документоведение : учебник / Н. Н. Куняев, Д. Н. Уралов, А. Г. Фабричной ; под ред. проф. Н. Н. Кунаева. - 2-е изд., стер. - Москва : Логос, 2020. - 352 с. - (Новая университетская библиотека). - ISBN 978-5-98704-329-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1211628 (дата обращения: 30.11.2022).
71. Бабаш, А. В. История защиты информации в зарубежных странах : учебное пособие / А.В. Бабаш, Д.А. Ларин. — Москва : РИОР : ИНФРА-М, 2021. — 284 с. — (Высшее образование). — DOI: https://doi.org/10.12737/15090. - ISBN 978-5-369-01844-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1215133 (дата обращения: 30.11.2022).
72. Электронный документооборот и обеспечение безопасности стандартными средствами WINDOWS : учебное пособие / Л.М. Евдокимова, В.В. Корябкин, А.Н. Пылькин, О.Г. Швечкова. - Москва : КУРС, 2023. - 296 с. - ISBN 978-5-906923-24-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1902497 (дата обращения: 30.11.2022).

73. Богульская, Н. А. Модели безопасности компьютерных систем : учебное пособие / Н. А. Богульская, М. М. Кучеров. - Красноярск : Сиб. федер. ун-т, 2019. - 206 с. - ISBN 978-5-7638-4008-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1819309 (дата обращения: 30.11.2022).
74. Беловицкий, К. Б. Основные методы выявления фактов коммерческого шпионажа : учебное пособие / К. Б. Беловицкий. - Москва : Дашков и К, 2021. - 345 с. - ISBN 978-5-394-04261-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1926415 (дата обращения: 30.11.2022).
75. Информационные технологии в документационном обеспечении управления и архивном деле : учебник для вузов / Н. Н. Кунаев, Т. В. Кондрашова, Е. В. Терентьева, А. Г. Фабричнов / под общ. ред. Н. Н. Куняева. - Москва : Логос, 2020. - 408 с. - ISBN 978-5-98704-786-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1211641 (дата обращения: 30.11.2022).
76. Моргунов, А. В. Электронные системы документооборота : учебное пособие / А. В. Моргунов. - Новосибирск : Изд-во НГТУ, 2020. - 74 с. - ISBN 978-5-7782-4269-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1870515 (дата обращения: 30.11.2022).

Журналы за последние два года:
«Инсайт. Защита информации»;
«Безопасность информационных технологий»;

Электронные образовательные ресурсы

Электронные ресурсы библиотеки МГОТУ:
http://www.biblioclub.ru/ - Университетская библиотека он-лайн
http://www.diss.rsl.ru/ - Российская государственная библиотека. Библиотека диссертаций
http://online.ebiblioteka.ru/ - универсальная библиотека Ист Вью
Web – ресурсы: www.goveniment.ru - официальный сайт Правительства Российской Федерации
http://www.minfin.ru – Официальный сайт Министерства финансов Российской Федерации
www. mon.gov.ru - официальный сайт Министерства образования Российской Федерации.
http://www.cbr.ru — Официальный сайт Центрального банка России

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 института 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.

1. 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

2. 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;

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).

Приложение 7

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

БЛОК 3. ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ
Б3.01(Д) Подготовка и защита ВКР

МЕОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО НАПИСАНИЮ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Год набора: 2023

Королев
2023

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:

УК-1 Системное и критическое мышление

Способен осуществлять поиск, критический анализ информации, применять системный подход для решения поставленных задач

УК-1.1. Описание сути проблемной ситуации

УК-1.2. Выявление составляющих проблемной ситуации и связей между ними

УК-1.3. Сбор и систематизация информации по проблеме

УК-1.4. Оценка адекватности и достоверности информации о проблемной ситуации

УК-1.5. Выбор методов критического анализа, адекватных проблемной ситуации

УК-1.6. Разработка и обоснование плана действий по решению проблемной ситуации

УК-1.7. Выбор способа обоснования решения (индукция, дедукция, по аналогии) проблемной ситуации;

УК-2 Разработка и реализация проектов

Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

УК-2.1. Формулирование цели, задач, значимости, ожидаемых результатов проекта

УК-2.2. Определение потребности в ресурсах для реализации проекта

УК-2.3. Разработка плана реализации проекта

УК-2.4. Контроль реализации проекта

УК-2.5. Оценка эффективности реализации проекта и разработка плана действий по его корректировке;

УК-3 Командная работа и лидерство

Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде

УК-3.1. Разработка целей команды в соответствии с целями проекта (организации)
УК-3.2. Формирование состава команды, определение функциональных и ролевых критериев отбора участников
УК-3.3. Разработка и корректировка плана работы команды
УК-3.4. Выбор правил командной работы как основы межличностного взаимодействия
УК-3.5. Выбор способов мотивации членов команды с учетом организационных возможностей и личностных особенностей членов команды, в т.ч. лиц с ограниченными возможностями здоровья
УК-3.6. Выбор стиля управления работой команды в соответствии с ситуацией
УК-3.7. Презентация результатов собственной и командной деятельности
УК-3.8. Оценка эффективности работы команды по достигнутому результату;

УК-4 Коммуникации

Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном (ых) языке(ах)

УК-4.1. Поиск источников информации на русском и иностранном языках
УК-4.2. Использование информационно-коммуникационных технологий для поиска, обработки и представления информации
УК-4.3. Составление и корректный перевод академических и профессиональных текстов с иностранного языка на государственный язык РФ и с государственного языка РФ на иностранный
УК-4.4. Выбор психологических способов оказания влияния и противодействия влиянию в процессе академического и профессионального взаимодействия
УК-4.5. Представление результатов академической и профессиональной деятельности на публичных мероприятиях
УК-4.6. Ведение академической и профессиональной дискуссии на государственном языке РФ и/или иностранном языке
УК-4.7. Выбор стиля делового общения применительно к ситуации взаимодействия, ведение деловой переписки

УК-5 Межкультурное взаимодействие

Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах

УК-5.1. Определение целей и задач межкультурного профессионального взаимодействия в условиях различных этнических, религиозных ценностных систем, выявление возможных проблемных ситуаций

УК-5.2. Выбор способов интеграции работников, принадлежащих к разным культурам, в производственную команду
УК-5.3. Выбор способа преодоления коммуникативных, образовательных, этнических, конфессиональных барьеров для межкультурного взаимодействия при решении профессиональных задач
УК-5.4. Выбор способа поведения в поликультурном коллективе при конфликтной ситуации

УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни

УК-6.1. Определение уровня самооценки и уровня притязаний как основы для выбора приоритетов собственной деятельности
УК-6.2. Определение приоритетов собственной деятельности, личностного развития и профессионального роста
УК-6.3. Выбор технологий целеполагания и целедостижения для постановки целей личностного развития и профессионального роста
УК-6.4. Оценка собственных (личностных, ситуативных, временных) ресурсов, выбор способов преодоления личностных ограничений на пути достижения целей
УК-6.5. Оценка требований рынка труда и образовательных услуг для выстраивания траектории собственного профессионального роста
УК-6.6. Оценка собственного ресурсного состояния, выбор средств коррекции ресурсного состояния
УК-6.7. Оценка индивидуального личностного потенциала, выбор техник самоорганизации и самоконтроля для реализации собственной деятельности;

УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности

УК-7.1. Выбирает здоровье - сберегающие технологии для поддержания здорового образа жизни с учетом физиологических особенностей организма
УК-7.2. Планирует свое рабочее и свободное время для оптимального сочетания физической и умственной нагрузки и обеспечения работоспособности
УК-7.3. Соблюдает и пропагандирует нормы здорового образа жизни в различных жизненных ситуациях и в профессиональной деятельности

УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении черезвычайных ситуаций и военных конфликтов

УК-8.1. Анализирует факторы вредного влияния на жизнедеятельность

элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений);
УК-8.2. Идентифицирует опасные и вредные факторы в рамках осуществляемой деятельности;
УК-8.3. Выявляет проблемы, связанные с нарушениями техники безопасности на рабочем месте; предлагает мероприятиях по предотвращению чрезвычайных ситуаций;
УК-8.4. Разъясняет правила поведения при возникновении чрезвычайных ситуаций природного и техногенного происхождения; оказывает первую помощь, описывает способы участия в восстановительных мероприятиях.

УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности

УК-9.1. Понимает базовые принципы функционирования экономики и экономического развития, цели формы участия государства в экономике;
УК-9.2. Применяет методы личного экономического и финансового планирования для достижения текущих и долгосрочных финансовых целей, использует финансовые инструменты для управления личными финансами (личным бюджетом), контролирует собственные экономические и финансовые риски
УК-9.3. Умеет разрабатывать основные показатели технико-экономического обоснования соответствующих проектных решений;
УК-9.4. Умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите.

УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности

УК-10.1 Анализирует действующие правовые нормы, обеспечивающие борьбу с экстремизмом, терроризмом и коррупцией в различных областях жизнедеятельности, а также способы профилактики коррупции и формирования нетерпимого отношения к ней
УК-10.2. Планирует, организует и проводит мероприятия, обеспечивающие формирование гражданской позиции и предотвращение экстремизма, терроризма и коррупции в обществе
УК-10.3 Соблюдает правила общественного взаимодействия на основе нетерпимого отношения к экстремизму, терроризму и коррупции

ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

ОПК-1.1. Знает понятия информации и информационной безопасности;

ОПК-1.2. Знает место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики;

ОПК-1.3. Знает источники и классификацию угроз информационной безопасности;

ОПК-2. Способен применять информационно – коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;

ОПК-2.1. Знает классификацию современных компьютерных систем и программного обеспечения, типовые структуры и принципы организации компьютерных сетей; назначение, функции и обобщённую структуру операционных систем; назначение и основные компоненты систем баз данных;

ОПК-2.2. Знает классификацию современных компьютерных систем и архитектуру их основных типов;

ОПК-2.3. Знает структуру и принципы работы современных и перспективных микропроцессоров;

ОПК-3. Способен использовать совокупность необходимых математических методов для решения задач профессиональной деятельности;

ОПК-3.1. Знает основные понятия теории пределов и непрерывности функций одной и нескольких действительных переменных;

ОПК-3.2. Знает основные методы дифференциального исчисления функций одной и нескольких действительных переменных;

ОПК-3.3. Знает основные методы интегрального исчисления функций одной и нескольких действительных переменных;

ОПК-4. Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности;

ОПК-4.1. Знает основополагающие принципы механики;

ОПК-4.2. Знает основные положения теории колебаний и волн, оптики;

ОПК-4.3. Умеет решать типовые задачи кодирования и декодирования;

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие

деятельность по защите информации в сфере профессиональной деятельности;

ОПК-5.1. Знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации;

ОПК-5.2. Знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации;

ОПК-5.3. Умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав;

ОПК-6. Способен при решении задач профессиональной деятельности организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ОПК-6.1.1 знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;

ОПК-6.1.2 знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях;

ОПК-6.1.3 знает систему организационных мер, направленных на защиту информации ограниченного доступа

ОПК-6.1.4 знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа

ОПК-6.1.5 знает основные угрозы безопасности информации и модели нарушителя объекта информатизации

ОПК-6.2.1 умеет разрабатывать модели угроз и модели нарушителя объекта информатизации

ОПК-6.2.2 умеет разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации

ОПК-6.2.3 умеет определить политику контроля доступа работников к информации ограниченного доступа

ОПК-6.2.4 умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации

ОПК-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности;

ОПК-7.1.1 знает основные принципы построения компьютера, формы и способы представления данных в персональном компьютере

ОПК-7.1.2 знает области и особенности применения языков программирования высокого уровня

ОПК-7.1.3 знает язык программирования высокого уровня (структурное, объектно-ориентированное программирование)

ОПК-7.2.1 умеет работать с интегрированной средой разработки программного обеспечения

ОПК-7.2.2 умеет разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач

ОПК-7.2.3 умеет разрабатывать программы для работы с файлами как с источником данных

ОПК-7.3.1 владеет навыками разработки, документирования, тестирования и отладки программ

ОПК-7.1.4 знает базовые структуры данных

ОПК-7.1.5 знает основные алгоритмы сортировки и поиска данных

ОПК-7.1.6 знает основные комбинаторные и теоретико-графовые алгоритмы

ОПК-7.1.7 знает общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения

ОПК-7.2.4 умеет применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач;

ОПК-7.3.2 владеет навыками разработки алгоритмов решения типовых профессиональных задач;

ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;

ОПК-8.1.1 знает принципы и порядок работы информационно-справочных систем

ОПК-8.1.2 знает способы поиска и обработки информации, методы работы с научной информацией, принципы и правила построения суждений и оценок

ОПК-8.2.1 умеет обобщать, анализировать и систематизировать научную информацию в области информационной безопасности

ОПК-8.2.2 умеет различать факты, интерпретации, оценки и аргументированно отстаивать свою позицию в процессе коммуникации

ОПК-8.2.3 умеет пользоваться информационно-справочными системами

ОПК-8.3.1 владеет навыком составления и оформления реферата по результатам обзора научно-технической литературы, нормативных и методических документов

ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;

ОПК-9.1.1 знает принципы построения систем и сетей электросвязи;

ОПК-9.1.2 знает современные виды информационного взаимодействия и обслуживания телекоммуникационных сетей и систем;

ОПК-9.2.1 умеет проводить анализ показателей эффективности сетей и систем телекоммуникаций и качества предоставляемых услуг;

ОПК-9.1.3 знает основные понятия и задачи криптографии, математические модели криптографических систем

ОПК-9.1.4 знает основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и криптографические протоколы

ОПК-9.1.5 знает национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения

ОПК-9.2.2 умеет применять математические модели для оценки стойкости СКЗИ

ОПК-9.2.3 умеет использовать СКЗИ в автоматизированных системах

ОПК-9.1.6 знает классификацию и количественные характеристики технических каналов утечки информации;

ОПК-9.1.7 знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;

ОПК-9.1.8 знает организацию защиты информации от утечки по техническим каналам на объектах информатизации;

ОПК-9.2.9 умеет пользоваться нормативными документами в области технической защиты информации;

ОПК-9.2.4 умеет анализировать и оценивать угрозы информационной безопасности объекта информатизации;

ОПК-9.3.1 владеет методами и средствами технической защиты информации.

ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;

ОПК-10.1.1 знает программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях

ОПК-10.2.1 умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности

ОПК-10.1.2 знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности

ОПК-10.1.3 знает принципы формирования политики информационной безопасности организации

ОПК-11. Способен проводить эксперименты по заданной методике и обработку их результатов;

ОПК-11.1.1 знает теоретические основы теории погрешностей;

ОПК-11.2.1 умеет проводить физический эксперимент, обрабатывать его результаты

ОПК-11.2.2 умеет использовать стандартные вероятностно-статистические методы анализа экспериментальных данных;

ОПК-11.2.3 умеет строить стандартные процедуры принятия решений на основе имеющихся экспериментальных данных;

ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем и средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений

ОПК-12.1.1 знает принципы формирования политики информационной безопасности в информационных системах;

ОПК-12.1.2 знает принципы организации информационных систем в соответствии с требованиями по защите информации;

ОПК-12.1.3 знает требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации;

ОПК-12.1.4 знает основные этапы процесса проектирования и общие требования к содержанию проекта;

ОПК-12.2.1 умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;

ОПК-12.2.2 умеет анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;

ОПК-12.2.3 умеет формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения;

ОПК-12.2.4 умеет оценивать информационные риски в автоматизированных системах;

ОПК-12.2.5 умеет разрабатывать основные показатели технико-экономического обоснования соответствующих проектных решений;

ОПК-13. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире, в том числе для формирования гражданской позиции и развития патриотизма.

ОПК-13.1.1 знает основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире;

ОПК-13.1.2 знает ключевые события истории России и мира, выдающихся деятелей России;

ОПК-13.2.1 умеет соотносить общие исторические процессы и отдельные факты, выявлять существенные черты исторических процессов, явлений и событий;

ОПК-13.2.2 умеет формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории;

ДОПК-2.1. Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба

ДОПК-2.1.1.1 знает технологии обеспечения информационной безопасности, способы их организации и оптимизации

ДОПК-2.1.1.2 знает технологии проектирования и построения информационных систем

ДОПК-2.1.2.1 умеет классифицировать информационные системы по назначению, структуре, типу

ДОПК-2.1.3.1 владеет навыками выявления и устранения угроз информационной безопасности

ДОПК-2.1.1.3 знает стратегии обеспечения информационной безопасности, способы их организации и оптимизации

ДОПК-2.1.1.4 знает определения рисков информационной безопасности применительно к объекту информатизации с заданными характеристиками

ДОПК-2.1.1.5 знает методы и подходы к реализации системы управления безопасностью автоматизированных информационных систем

ДОПК-2.1.2.2 умеет обосновывать решения по обеспечению информационной безопасности объектов в профессиональной сфере деятельности

ДОПК-2.1.3.2 владеет навыками реализации политики информационной безопасности

ДОПК-2.1.1.6 знает методы анализа процессов для определения актуальных угроз

ДОПК-2.1.1.7 знает особенности работы решений по защите информации в информационных процессах и системах

ДОПК-2.1.2.3 умеет представлять процессы в формализованном виде на языках моделирования

ДОПК-2.1.3.3 владеет навыками применения современных программно-аппаратных средств моделирования информационных процессов и систем ЗИ

ДОПК-2.1.3.4 владеет навыками оценки адекватности моделей и анализа результатов моделирования

ДОПК-2.1.1.8 знает принципы обеспечения информационной безопасности объекта информатизации

ДОПК-2.1.1.9 знает методы хранения, обработки и передачи и получения информации из открытых информационных систем

ДОПК-2.1.2.4 умеет делать выводы по результатам проведённого анализа, выявляя потенциальные угрозы ИБ

ДОПК-2.1.3.5 владеет навыками применения автоматизированных средств сбора и анализа информации, основанных на технологиях OSINT и data mining

ДОПК-2.1.3.6 владеет навыками анализа надежности защиты информационных систем

ДОПК-2.1.1.10 знает основные категории требований к программным и программно-аппаратным средствам защиты информации

ДОПК-2.1.1.11 знает требования по защите автоматизированных систем от НСД

ДОПК-2.1.2.5 умеет делать обоснованный выбор существующих средств защиты информации для нейтрализации определенного вида угроз

ДОПК-2.1.2.7 владеет навыками выбора и применения современных аппаратных и программных средств технической защиты информации

ДОПК-2.1.3.8 владеет навыками эффективного использования средств автоматического контроля и обнаружения возможных каналов утечки сведений, представляющих государственную, военную, служебную и коммерческую тайну

ДОПК-2.1.1.12 знает основы администрирования вычислительных сетей

ДОПК-2.1.1.13 знает основы организации систем управления БД

ДОПК-2.1.1.14 знает принципы организации операционных систем в защищённом исполнении

ДОПК-2.1.2.6 умеет настраивать политики безопасности наиболее распространенных операционных систем

ДОПК-2.1.2.7 умеет выявлять и устранять сбои в работе ос, систем электронного документооборота и основных СУБД

ДОПК-2.1.3.8 владеет навыками установки и администрирования основных операционных систем и систем электронного документооборота

ДОПК-2.2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;

ДОПК-2.2.1.1 знает подходы к построению подсистем фиксации и реагирования на инциденты информационной безопасности

ДОПК-2.2.1.2 знает принципы разработки организационных и технических мер по сбору, анализу и мониторингу событий безопасности

ДОПК-2.2.2.1 умеет анализировать эффективность применения мер по обеспечению ЗИ и разрабатывать предложения по совершенствованию структуры мер и повышению эффективности.

ДОПК-2.2.2.2 умеет реагировать на инциденты информационной безопасности

ДОПК-2.2.3.1 владеет навыками классификации информационных систем и средств вычислительной техники по требованиям регуляторов ИБ

ДОПК-2.2.1.3 знает как проводится анализ журналов событий средств защиты информации

ДОПК-2.2.1.4 знает основные этапы расследования компьютерных преступлений в соответствии с нормативными требованиями

ДОПК-2.2.2.3 умеет сопоставлять основные структурно-функциональные характеристики информационных систем с требованиями руководящих документов

ДОПК-2.2.3.2 владеет навыками сравнения и анализа существующих средств защиты информации

ДОПК-2.2.3.3 владеет навыками нахождения наиболее подходящего решения применительно к заданным характеристикам информационной системы

ДОПК-2.2.1.5 знает руководящие документы в области классификации современных информационных систем и средств вычислительной и техники

ДОПК-2.2.1.6 знает основы нормативно-правовых актов в области защиты информации конфиденциального характера

ДОПК-2.2.1.7 знает как формируется организационно-распорядительная и эксплуатационная документация по обеспечению безопасности информационных систем

ДОПК-2.2.2.4 умеет классифицировать информацию и автоматизированные системы, определять основные требования к ее защите

ДОПК-2.2.3.4 владеет навыками работы с нормативно-правовыми актами, навыками ориентации в них и поиска необходимой информации

ДОПК-2.3. Способен разработать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;

ДОПК-2.3.1.1 знает государственные нормативные документы в области организации проведения и сопровождения аттестации объекта информатизации

ДОПК-2.3.1.2 знает отечественные и зарубежные стандарты в области информационной безопасности

ДОПК-2.3.1.3 знает как разрабатывать технические задания на создание подсистем информационной безопасности открытых информационных систем

ДОПК-2.3.2.1 умеет организовывать проведение и сопровождать аттестацию объекта информатизации в соответствии с требованиями нормативных документов

ДОПК-2.3.3.1 владеет навыками внедрения и контроля исполнения требования локальных нормативных документов по обеспечению ИБ

ДОПК-2.3.1.4 знает правовые нормы, инструкции и стандарты в области организации документооборота

ДОПК-2.3.1.5 знает правовые основы организации защиты государственной тайны и конфиденциальной информации

ДОПК-2.3.2.2 умеет разрабатывать инструкции по организации защищённого документооборота и контролировать их исполнение

ДОПК-2.3.3.2 владеет навыками установки, настройки и использования современных систем электронного документооборота в защищённом исполнении

ДОПК-2.3.1.6 знает как разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации

ДОПК-2.3.1.7 знает актуальные нормативно-правовые акты и методические документы в области обеспечения информационной безопасности персональных данных

ДОПК-2.3.1.8 знает правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны в соответствии с доктриной ИБ РФ

ДОПК-2.3.2.3 умеет формировать требования к системам защиты информации в информационных системах персональных данных с учетом специфики их эксплуатации в различных сферах жизнедеятельности

ДОПК-2.3.3.3 владеет навыками проведения лицензирования в области защиты информации

ДОПК-2.3.3.4 владеет навыками работы с нормативно-правовыми актами

ДОПК-2.4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами

ДОПК-2.4.1.1 знает стандарты и критерии в области аудита ИБ

ДОПК-2.4.1.2 знает требования законодательства по обеспечению безопасности персональных данных

ДОПК-2.4.1.3 знает как составляются политики информационной безопасности в информационной системе персональных данных

ДОПК-2.4.2.1 умеет определять объекты аудита, критерии и область их действия

ДОПК-2.4.3.1 владеет навыками составления отчётов по результатам выполненного аудита

ДОПК-2.4.1.4 знает принципы организации процесса аудита

ДОПК-2.4.1.5 знает теоретическую базу разработки политик безопасности

ДОПК-2.4.2.2 умеет применять инструментальные средства мониторинга и аудита безопасности

ДОПК-2.4.2.3 умеет составлять программу аудита ИБ

ДОПК-2.4.3.2 владеет навыками проведения аудита ИБ со сбором данных

ДОПК-2.4.1.6 знает теоретическую базу и средства для проведения мониторинга защищенности информационной системы

ДОПК-2.4.1.7 знает принципы администрирования подсистем информационной безопасности

ДОПК-2.4.2.4 умеет разрабатывать методики анализа рисков

ДОПК-2.4.2.5 умеет собирать и анализировать свидетельства аудита

ДОПК-2.4.3.3 владеет навыками по формулированию выводов и заключения по полученным результатам

ДОПК-2.4.1.8 знает порядок аттестации объектов информатизации

ДОПК-2.4.1.9 знает порядок проведения сертификационных испытаний средств защиты информации

ДОПК-2.4.2.6 умеет формализовать задачи анализа безопасности информационных систем

ДОПК-2.4.3.4 владеет навыками выбора и обоснования критериев оценки защищенности открытых информационных систем

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;

ПК-1.1. Нормативно-правовые акты и стандарты в области ИБ и принципы проведения диагностики системы ЗИ;

ПК-1.2. Выявлять и оценивать источники и последствия инцидентов ИБ (ЗИ);

ПК-1.3. Выполнять обнаружение, идентификацию и устранение инцидентов ИБ (ЗИ).

ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;

ПК-2.1. Руководящие и методические документы принципы организации по проведению экспериментальной деятельности в области ЗИ;

ПК-2.2. Применять действующую нормативную базу выбирать целесообразные потребные средства и определять структуру системы ЗИ в ходе проведения экспериментов;

ПК-2.3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ.

ПК-3. способностью осуществлять управление с разработкой организационно-распорядительных документов и реализацию организационных мер по ЗИ в АС;

ПК-3.1. Основные нормативно-правовые акты, методы управления деятельностью, угрозы ИБ и нарушители систем безопасности информации;

ПК-3.2. Оценивать информационные риски разрабатывать предложения по совершенствованию СУ (ИБ) и применять средства контроля эффективности ЗИ;

ПК-3.3. Анализировать воздействие на защищаемую систему информации, оценивать последствия и вырабатывать предложения по ее совершенствованию;

ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

ПК-4.1. Знать нормативно-методические, руководящие и методические документы, организационные меры, критерии оценки защищенности и регламенты обеспечения работоспособности систем ЗИ;

ПК-4.2. Определять и оценивать источники, причины и последствия возникающих инцидентов выявлять и устранять нарушения в области ИБ (ЗИ);

ПК-4.3. Принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации.

ПК-5. Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений

ПК-5.1.1 Документационное обеспечение по разработке проектных решений по ЗИ, принципы и особенности организации проектно-технологической деятельности;

ПК-5.2.2 Участвовать в разработке проектных документов на создание подсистемы ИБ с разработкой модели проектируемых систем ЗИ и осуществлять технико-экономическое обоснование;

ПК-5.3.3 Анализировать защищенность информационной инфраструктуры с формированием системы требований по ЗИ и участвовать в обосновании критериев эффективности функционирования проектируемых систем ИБ (ЗИ)

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.

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-исследователь- ской 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.

Объем 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 объём 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 чёткие 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 7.2);

Задание на выполнение выпускной квалификационной работы (приложение 7.3);

Результаты нормоконтроля ВКР (приложение 7.6);

Содержание (оглавление) работы;

Введение;
Основная часть;
Заключение;
Глоссарий (образец оформления, приложение 7.5);
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 7.7) 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 7.2).

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 7.8) 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 7.9 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 7.10.

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 7.11.

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 7.12.

Защита ВКР проходит в торжественной обстановке, публично, на открытом заседании аттестационной комиссии. Идентификация выпускников на итоговых аттестационных испытаниях проводится традиционно: визуально и по паспортам.

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

---

* 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).

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.

Приложение 7.1

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.

Приложение 7.2
Образец титульного листа

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки
_____

ДОПУСК К ЗАЩИТЕ:

Приказ №
от «____»_____201__г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
БАКАЛАВРА

Тема:
_____
_____
_____

Студент(ка): _____ / _____ /
Ф. И. О. подпись
Факультет _____ Группа _____

Научный руководитель: _____ / _____ /
Ф. И. О. подпись

Дата представления работы «____» _____ 201__г.

Королёв 202__ г.

ПРИЛОЖЕНИЕ 7.3

З А Д А Н И Е
на выполнение выпускной квалификационной работы
бакалавра

Студент(ка)
_____
фамилия, имя, отчество
форма обучения _____, группа _____,
очная/заочная
направление подготовки _____

1. Тема
_____
_____
2. Дата выдачи темы «_____»_____202__г.
3. Календарный график выполнения
_____
_____
_____
4. Содержание пояснительной записки
_____
_____
_____
5. Срок представления студентом законченной выпускной квалификационной работы бакалавра: «___» _____ 202 __г.

Научный руководитель
_____
Ф.И.О., ученая степень, должность, место работы
_____
_____

Научный руководитель _____

(подпись)
Студент(ка) _____

(подпись)

Приложение 7.4

Унифицированные требования к оформлению выпускных квалификационных работ бакалавра

№ п.п.	Объект унификации	Параметры унификации
1	Формат листа бумаги	А4
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

Приложение 7.5

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

Приложение 7.6

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	Объем введения	3-5 стр. машинописного текста	
9	Объем основной части	60-80 стр. машинописного текста	
10	Объем заключения	2-3 стр. машинописного текста	
11	Нумерация страниц	Сквозная, в нижней части листа, посередине. На	

		титульном 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 _____ _____

фамилия, имя, отчество подпись

С результатами нормоконтроля ознакомлен:
выпускник

подпись

ПРИЛОЖЕНИЕ 7.7

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

Приложение 7.8

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. _____
7. _____
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.

Приложение 7.9

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.

ПРИЛОЖЕНИЕ 7.10

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. Объём 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).

Приложение 7.11

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 А.В.Степанов
ПЕЧАТЬ
(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)

Приложение 7.12

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).

Лист регистрации изменений

Номер изменения	Номер листа			Дата внесения изменения	Основание для введения изменения	Всего листов в документе	Подпись ответственного за внесение изменений
	измененного	нового	изъятого				