Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования «Академия маркетинга и социально-информационных технологий – ИМСИТ» (г. Краснодар)

Институт информационных технологий и инноваций

Кафедра математики и вычислительной техники

УТВЕРЖДАЮ
Ректор академии, профессор
Р.Л. Агабекян
20 ноября 2023 г.

ОСНОВНАЯ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ВЫСШЕГО ОБРАЗОВАНИЯ

направления подготовки 10.03.01 Информационная безопасность
направленность (профиль) образовательной программы
«Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)»

Квалификация
бакалавр

Краснодар
2023

Основная профессиональная образовательная программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г. № 1427.

Основная профессиональная образовательная программа направления подготовки 10.03.01 Информационная безопасность, направленность (профиль) образовательной программы Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности) для набора 2024 года, рассмотрена и одобрена на заседании кафедры Математики и вычислительной техники 13 октября 2023 г., протокол № 3.

Зав. кафедрой математики и вычислительной
техники, канд. экон. наук Н.П. Исикова

Основная профессиональная образовательная программа утверждена на заседании Научно-методического совета Академии ИМСИТ протокол № 3 от 20 ноября 2023 г.

Председатель Научно-методического Совета Академии ИМСИТ, профессор Н.Н. Павелко

Рецензенты:
Видовский Л.А., д.т.н., профессор, профессор кафедры информационных систем и программирования КубГТУ

Глебов О.В., директор АО «ЮГ-СИСТЕМА ПЛЮС»

СОДЕРЖАНИЕ

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Назначение примерной основной образовательной программы

ОПОП регламентирует цели, ожидаемые результаты, содержание, условия и технологии реализации образовательного процесса, оценку качества подготовки выпускника по данному направлению подготовки и включает в себя: учебный план, календарный учебный график рабочие программы дисциплин (модулей) и другие материалы, обеспечивающие качество подготовки обучающихся, а также программы практик, контрольно-оценочные средства и методические материалы, обеспечивающие реализацию соответствующей образовательной технологии.

Основными пользователями ОПОП являются: руководство, профессорско-преподавательский состав и обучающиеся НАН ЧОУ ВО «Академия маркетинга и социально-информационных технологий – ИМСИТ» (г. Краснодар) (сокращенно НАН ЧОУ ВО Академии ИМСИТ, далее Академия ИМСИТ или академия); государственные экзаменационные комиссии; объединения специалистов и работодателей в сфере профессиональной деятельности соответствующей направленности (профилю) основной профессиональной образовательной программы; уполномоченные государственные органы исполнительной власти, осуществляющие аккредитацию и контроль качества в системе высшего образования.

ОПОП реализуется на русском языке.

1.2 Нормативные документы для разработки ОПОП 10.03.01 Информационная безопасность, направленность (профиль) образовательной программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)»

Нормативную правовую базу разработки ОПОП по направлению подготовки 10.03.01 Информационная безопасность, направленность (профиль) образовательной программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)» составляют:

1) Федеральный закон Российской Федерации: «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ;

2) Федеральный государственный образовательный стандарт высшего профессионального образования (ФГОС ВО) по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г. № 1427.

3) Приказ Минобрнауки РФ «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры» от 05.04.2017 г. № 301;

4) Приказ Министерства образования и науки Российской Федерации «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры» от 29.06.2015г № 636;

5) Приказ Министерства науки и высшего образования РФ и Министерства просвещения РФ от 5 августа 2020 г. N 885/390 «О практической подготовке обучающихся» (вместе с «Положением о практической подготовке обучающихся») (Зарегистрировано в Минюсте России 11.09.2020 N 59778);

6) Приказ Министерства образования и науки Российской Федерации «Об утверждении перечней специальностей и направлений подготовки высшего образования» от 12.09.2013г № 1061;

7) Постановление Правительства РФ от 11 октября 2023 г. N 1678 «Об утверждении Правил применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;

8) Нормативно-методические документы Минпросвещения РФ;

9) Порядок проведения итоговой аттестации по не имеющим государственной аккредитации образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры. Дата утверждения: 28 августа 2019 года, протокол Ученого Совета № 1 (с изменениями и дополнениями от 01.07.2022, протокол Ученого Совета № 10).

10) Устав НАН ЧОУ ВО «Академия маркетинга и социально-информационных технологий – ИМСИТ» и другие локальные акты Академии ИМСИТ.

1.3 Перечень сокращений

ЕКС – единый квалификационный справочник
з.е. – зачетная единица
ОПОП – основная профессиональная образовательная программа

ОТФ – обобщенная трудовая функция

ОПК – общепрофессиональные компетенции

Организация – организация, осуществляющая образовательную деятельность по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность

ПК – профессиональные компетенции

ПООП – примерная основная образовательная программа

ПП – практическая подготовка

ПС – профессиональный стандарт

УГСН – укрупненная группа направлений и специальностей

УК – универсальные компетенции

ФЗ – Федеральный закон

ФГОС ВО – федеральный государственный образовательный стандарт высшего образования

ФУМО – федеральное учебно-методическое объединение

2 ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ВЫПУСКНИКОВ, ОСВОИВШИХ ПРОГРАММУ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

2.1 Общее описание профессиональной деятельности выпускников

Область профессиональной деятельности и сфера профессиональной деятельности, в которых выпускники, освоившие программу бакалавриата, могут осуществлять профессиональную деятельность:

06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере).

В рамках освоения программы бакалавриата выпускники могут готовиться к решению задач профессиональной деятельности следующего типа: эксплуатационный, проектно-технологический, экспериментально-исследовательский, организационно-управленческий.

Перечень основных объектов (или областей знания) профессиональной деятельности выпускников: автоматизированные системы различного назначения, системы обработки данных, средства защиты информации, объекты, на которых осуществляется обработка информации ограниченного доступа.

2.2 Перечень профессиональных стандартов, соотнесенных с ФГОС

Перечень профессиональных стандартов, соотнесенных с федеральным государственным образовательным стандартом по направлению подготовки, приведен в таблице 1.

Таблица 1 – Перечень профессиональных стандартов, соотнесенных с федеральным государственным образовательным стандартом по направлению подготовки 10.03.01 Информационная безопасность

№ п/п	Код профессионального стандарта	Наименование области профессиональной деятельности. Наименование профессионального стандарта
06. Связь, информационные и коммуникационные технологии		
1.	06.030	Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденный приказом Минтруда России от 14 сентября 2022 г. N 536н «Об утверждении профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях» (Зарегистрировано в Минюсте России 18 октября 2022 г. N 70596)
2.	06.032	Профессиональный стандарт «Специалист по безопасности компьютерных

		систем и сетей», утвержденный приказом Минтруда России от 14 сентября 2022 г. N 533н «Об утверждении профессионального стандарта «Специалист по безопасности компьютерных систем и сетей» (Зарегистрировано в Минюсте России 14 октября 2022 г. N 70515)
3.	06.033	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержденный приказом Минтруда России от 14 сентября 2022 г. N 525н «Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах» (Зарегистрировано в Минюсте России 14 октября 2022 г. N 70543)
4.	06.034	Профессиональный стандарт «Специалист по технической защите информации» утвержденный приказом Минтруда России от 9 августа 2022 г. N 474н «Об утверждении профессионального стандарта «Специалист по технической защите информации» (Зарегистрировано в Минюсте России 9 сентября 2022 г. N 70015)

Перечень обобщённых трудовых функций и трудовых функций, имеющих отношение к профессиональной деятельности выпускника программ высшее образование – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, представлен в таблице 2.

Таблица 2 – Перечень обобщённых трудовых функций и трудовых функций,

Код и наименование профессионального стандарта	Обобщенные трудовые функции			Трудовые функции		
	Код	Наименование	Уровень квалификации	Наименование	Код	Уровень (подуровень) квалификации
06.030 Специалист по защите информации в телекоммуникационных системах и сетях	B	Обеспечение защиты от НД и компьютерных атак сооружений и СССЭ (за исключением сетей связи специального назначения) в процессе их эксплуатации	6	Мониторинг функционирования СССЭ, защищенности от НД и компьютерных атак сооружений и СССЭ	B/01.6	6
				Управление функционированием СССЭ, защищенностью от НД и компьютерных атак сооружений и СССЭ	B/02.6	6
				Управление персоналом, обслуживающим сооружения и СССЭ, а также программные, программно-аппаратные (в том числе криптографические) и технические средства и системы их защиты от НД, средства для поиска признаков компьютерных атак в сетях электросвязи	B/03.6	6

06.032 Защита информации в компьютерных системах и сетях	B	Администрирование средств защиты информации в компьютерных системах и сетях	6	Администрирование подсистем защиты информации в операционных системах	B/01.6	6
				Администрирование программно-аппаратных средств защиты информации в компьютерных сетях	B/02.6	6
				Администрирование средств защиты информации прикладного и системного программного обеспечения	B/03.6	6
06.033 Специалист по защите информации в автоматизированных системах	B	Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации	6	Диагностика систем защиты информации автоматизированных систем	B/01.6	6
				Администрирование систем защиты информации автоматизированных систем	B/02.6	6
				Управление защитой информации в автоматизированных системах	B/03.6	6
				Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций	B/04.6	6
				Мониторинг защищенности информации в автоматизированных системах	B/05.6	6
				Аудит защищенности информации в автоматизированных системах	B/06.6	6
				Установка и настройка средств защиты информации в автоматизированных системах	B/07.6	6
				Разработка организационно-распорядительных документов по защите	B/08.6	6

				информации в автоматизированных системах		
				Анализ уязвимостей внедряемой системы защиты информации	B/09.6	6
				Внедрение организационных мер по защите информации в автоматизированных системах	B/10.6	6
06.034 Специалист по технической защите информации	B	Проведение работ по установке и техническому обслуживанию защищенных средств обработки информации	6	Проведение работ по установке, настройке, испытаниям и техническому обслуживанию защищенных технических средств обработки информации	B/01.6	6
				Проведение работ по установке, монтажу, наладке, испытаниям и техническому обслуживанию защищенных программных (программно-технических) средств обработки информации	B/02.6	6
	E	Проведение контроля защищенности информации	6	Проведение специальных исследований на побочные электромагнитные излучения и наводки технических средств обработки информации	E/01.6	6
				Проведение контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок	E/02.6	6
				Проведение контроля защищенности акустической речевой информации от утечки по техническим каналам	E/03.6	6
				Проведение контроля защищенности информации от несанкционированного доступа	E/04.6	6

2.3 Перечень основных задач профессиональной деятельности выпускников

Перечень основных задач профессиональной деятельности выпускников по направлению подготовки 10.03.01 Информационная безопасность, направленность (профиль) программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)» приведен в таблице 3.

Таблица 3 - Перечень основных задач профессиональной деятельности выпускников

Область профессиональной деятельности (по Реестру Минтруда)	Типы задач профессиональной деятельности	Задачи профессиональной деятельности	Объекты профессиональной деятельности (или области знания)
06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере).	эксплуатационный	Эксплуатация автоматизированных систем в защищённом исполнении. Реализация требуемых политик безопасности в автоматизированных системах. Обеспечение защищённости процессов обработки информации в автоматизированных системах.	Системы обработки данных; автоматизированные системы различного назначения; средства защиты информации.
	проектно-технологический	Внедрение решений, направленных на повышения уровня защищённости автоматизированных систем. Сопровождение систем обеспечения информационной безопасности на всех этапах жизненного цикла. Участие в создании технической документации по результатам выполнения работ по обеспечению информационной безопасности.	Автоматизированные системы различного назначения; объекты, на которых осуществляется обработка информации ограниченного доступа
	экспериментально-исследовательский	Определение соответствия достигаемого уровня защищённости требования нормативных документов. Использование инструментальных средств анализа защищённости автоматизированных систем.	Автоматизированные системы различного назначения.
	организационно-управленческий	Организация и выполнение работ по обеспечению информационной безопасности в автоматизированных системах. Подготовка данных для составления обзоров и отчетов по инцидентам информационной безопасности.	Объекты, на которых осуществляется обработка информации ограниченного доступа.

3 ОБЩАЯ ХАРАКТЕРИСТИКА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ, РЕАЛИЗУЕМОЙ В РАМКАХ НАПРАВЛЕНИЯ ПОДГОТОВКИ 10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

3.1 Направленность (профиль) образовательной программы в рамках направления подготовки

Направленность (профиль) программы бакалавриата: «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)», конкретизирует содержание программы бакалавриата в рамках направления подготовки путем ориентации ее на: область профессиональной деятельности и сферу профессиональной деятельности выпускников, и тип задач и задачи профессиональной деятельности выпускников.

3.2 Квалификация, присваиваемая выпускникам образовательной программы

Выпускнику, освоившему образовательную программу по направлению подготовки 10.03.01 Информационная безопасность присваивается квалификация «Бакалавр».

3.3 Объем программы

Объем программы бакалавриата составляет 240 зачетных единиц (далее – з.е.) вне зависимости от формы обучения, применяемых образовательных технологий, реализации программы бакалавриата с использованием сетевой формы, реализации программы бакалавриата по индивидуальному учебному плану.

Объем программы бакалавриата, реализуемый за один учебный год, составляет не более 70 з.е. вне зависимости от формы обучения, применяемых образовательных технологий, реализации программы бакалавриата с использованием сетевой формы, реализации программы бакалавриата по индивидуальному учебному плану (за исключением ускоренного обучения), а при ускоренном обучении – не более 80 з.е.

Зачетная единица эквивалентна 36 академическим часам.

3.4 Формы обучения

Очная, Заочная.

3.5 Срок получения образования

В очной форме обучения, включая каникулы, предоставляемые после

прохождения государственной итоговой аттестации, составляет 4 года;

В заочной форме обучения, включая каникулы, предоставляемые после прохождения государственной итоговой аттестации, составляет 4 года 11 месяцев.

3.6 Требования к уровню подготовки, необходимому для освоения ОПОП

Прием на обучение в НАН ЧОУ ВО Академия ИМСИТ по образовательной программе высшего образования осуществляется в соответствии с «Правилами приема на обучение по образовательным программа высшего образования – программам бакалавриата, программам бакалавриата, программам бакалавриата в НАН ЧОУ ВО Академия ИМСИТ».

К освоению основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность допускаются лица, имеющие образование соответствующего уровня, подтвержденное документами об образовании.

Приветствуется участие абитуриента в профильных предметных олимпиадах; знание базовых ценностей мировой культуры; понимание законов развития природы и общества; обладание интеллектуальными, организаторскими и лидерскими способностями; стремление к личностному росту и профессиональному развитию; способность занимать активную гражданскую позицию; критически оценивать личные достоинства и недостатки.

4 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

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

В результате освоения программы бакалавриата у выпускника должны быть сформированы компетенции, установленные программой бакалавриата.

4.1.1 Универсальные компетенции выпускников и индикаторы их достижения

Программа бакалавриата устанавливает следующие универсальные компетенции и индикаторы их достижения – таблица 4.

Таблица 4 – Универсальные компетенции 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. Анализирует задачу, выделяя ее базовые составляющие. УК-1.2. Определяет и ранжирует информацию, требуемую для решения поставленной задачи. УК-1.3. Осуществляет поиск информации для решения поставленной задачи по различным типам запросов.
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. Формулирует проблему, решение которой напрямую связано с достижением цели проекта. УК-2.2. Определяет связи между поставленными задачами и ожидаемые результаты их решения. УК-2.3. Анализирует план-график реализации проекта в целом и выбирает оптимальный способ решения поставленных задач. УК-2.4. В рамках поставленных задач определяет имеющиеся ресурсы и ограничения, действующие правовые нормы. УК-2.5. Оценивает решение поставленных задач в зоне своей ответственности в соответствии с запланированными результатами контроля, при необходимости корректирует способы решения задач.

Командная работа и лидерство	УК-3. Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	УК-3.1. Определяет свою роль в команде, исходя из стратегии сотрудничества для достижения поставленной цели. УК-3.2. При реализации своей роли в команде учитывает особенности поведения других членов команды. УК-3.3. Анализирует возможные последствия личных действий и планирует свои действия для достижения заданного результата. УК-3.4. Осуществляет обмен информацией, знаниями и опытом с членами команды, оценивает идеи других членов команды для достижения поставленной цели. УК-3.5. Соблюдает установленные нормы и правила командной работы, несет личную ответственность за общий результат.
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. Выбирает стиль делового общения на государственном языке РФ и иностранном языке в зависимости от цели и условий партнерства; адаптирует речь, стиль общения и язык жестов к ситуациям взаимодействия. УК-4.2. Выполняет перевод профессиональных деловых текстов с иностранного языка на государственный язык РФ и с государственного языка РФ на иностранный. УК-4.3. Ведет деловую переписку на государственном языке РФ и иностранном языке с учетом особенностей стилистики официальных и неофициальных писем и социокультурных различий в формате корреспонденции. УК-4.4. Представляет свою точку зрения при деловом общении и в публичных выступлениях.
Межкультурное взаимодействие	УК-5. Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах	УК-5.1. Интерпретирует историю России в контексте мирового исторического развития. УК-5.2. Учитывает при социальном и профессиональном общении историческое наследие и социокультурные традиции различных социальных групп, этносов и конфессий, включая мировые религии, философские и этические учения. УК-5.3. Придерживается принципов недискриминационного взаимодействия при личном и массовом общении в целях выполнения профессиональных задач и усиления социальной интеграции.
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на	УК-6.1. Использует инструменты и методы управления временем при выполнении конкретных задач, проектов, при достижении поставленных целей. УК-6.2. Определяет задачи саморазвития и профессионального роста, распределяет их на долго-, средне- и краткосрочные с обоснованием

	основе принципов образования в течение всей жизни	актуальности и определением необходимых ресурсов для их выполнения. УК-6.3. Использует основные возможности и инструменты непрерывного образования (образования в течение всей жизни) для реализации собственных потребностей с учетом личностных возможностей, временной перспективы развития деятельности и требований рынка труда.
	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 безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных 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 мероприятия 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-8.5. Анализирует современные экологические проблемы и причины их возникновения как показатели нарушения принципов устойчивого развития общества. УК-8.6. Способен выполнять воинский долг и обязанности по защите своей Родины в соответствии с законодательством Российской Федерации.
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 и 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 рынки.
Гражданская позиция	УК-10. Способен формировать нетерпимое отношение к коррупционному поведению	УК-10.1. Анализирует гуманитарные и правовые последствия экстремизма, терроризма и коррупционной деятельности, в том числе собственных действий или бездействий. УК-10.2. Выбирает правомерные формы взаимодействия с гражданами, структурами гражданского общества и органами государственной власти в типовых ситуациях.

4.1.2 Общепрофессиональные компетенции выпускников и индикаторы их достижения

Программа бакалавриата должна устанавливать следующие общепрофессиональные компетенции и индикаторы их достижения – таблица 5.

Таблица 5 – Общепрофессиональные компетенции и индикаторы их достижения

Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции
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. Классифицирует угрозы информационной безопасности в соответствии с нормативными документами. ОПК-1.2. Оценивает угрозы информационной безопасности с точки зрения основных концепций национальной безопасности Российской Федерации. ОПК-1.3. Определяет угрозы информационной безопасности для различных систем.
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. Ищет информацию в глобальной информационной сети Интернет. ОПК-2.2. Подготавливает документы в среде типовых офисных пакетов. ОПК-2.3. Определяет состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств. ОПК-2.4. Применяет технические и программные средств тестирования с целью определения исправности компьютера и оценки его производительности.
ОПК-3. Способен использовать необходимые математические методы для	ОПК-3.1. Использует методы аналитической геометрии и векторной алгебры при решении прикладных задач.

решения задач профессиональной деятельности	ОПК-3.2. Использует типовые модели и методы математического анализа при решении стандартных прикладных задач. ОПК-3.3. Выполняет типовые расчеты с использованием основных формул дифференциального и интегрального исчисления. ОПК-3.4. Использует расчетные формулы и таблицы при решении стандартных вероятностно-статистических задач. ОПК-3.5. Решает задачи профессиональной области с применением дискретных моделей. ОПК-3.6. Вычисляет теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность).
ОПК-4. Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности	ОПК-4.1. Решает базовые прикладные физические задачи. ОПК-4.2. Анализирует электрические цепи в переходных и установившихся режимах в частотной и временной областях. ОПК-4.3. Анализирует процессы, протекающие в линейных и нелинейных электрических цепях.
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.1. Разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации. ОПК-5.2. Формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации. ОПК-5.3. Формулирует основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации.
ОПК-6. Способен при решении профессиональных задач 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. Разрабатывает модели угроз и модели нарушителя объекта информатизации. ОПК-6.2. Определяет политику контроля доступа работников к информации ограниченного доступа. ОПК-6.3. Формулирует требования, предъявляемые к физической защите объекта и пропускному режиму в организации. ОПК-6.4. Разрабатывает проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации.
ОПК-7. Способен использовать языки программирования и	ОПК-7.1. Разрабатывает с помощью языков высокого уровня алгоритмы решения типовых профессиональных задач.

технологии разработки программных средств для решения задач профессиональной деятельности	ОПК-7.2. Разрабатывает программы для работы с файлами как с источником данных. ОПК-7.3. Отлаживает разработанные программные средства.
ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-8.1. Составляет рефераты по результатам обзора научно-технической литературы, нормативных и методических документов. ОПК-8.2. Систематизирует научную информацию в области информационной безопасности. ОПК-8.3. Использует информационно-справочные системы при поиске информации в области профессиональной деятельности.
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.1. Использует средства криптографической защиты информации в автоматизированных системах. ОПК-9.2. Решает задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов. ОПК-9.3. Организует защиту информации от утечки по техническим каналам на объектах информатизации. ОПК-9.4. Оценивает угрозы информационной безопасности объекта информатизации. ОПК-9.5. Использует средства защиты информации от утечки по техническим каналам и контроля эффективности 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. Реализует требования политик безопасности на объектах информатизации. ОПК-10.2. Конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности. ОПК-10.3. Применяет средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях.
ОПК-11. Способен проводить эксперименты по заданной методике и обработку их результатов	ОПК-11.1. Строит стандартные процедуры принятия решений на основе имеющихся экспериментальных данных. ОПК-11.2. Использует стандартные вероятностно-статистические методы анализа экспериментальных данных. ОПК-11.3. Проводить физический эксперимент. ОПК-11.4. Обрабатывает результаты физического эксперимента.
ОПК-12. Способен проводить подготовку исходных данных для проектирования	ОПК-12.1. Определяет информационную инфраструктуру и информационные ресурсы организации, подлежащие защите.

подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.2. Анализирует показатели качества и критерии оценки систем и отдельных методов и средств защиты информации. ОПК-12.3. Оценивает информационные риски в автоматизированных системах. ОПК-12.4. Разрабатывает основные показатели технико-экономического обоснования соответствующих проектных решений.
ОПК-13. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма	ОПК-13.1. Выявляет существенные черты исторических процессов, явлений и событий. ОПК-13.2. Соотносит общие исторические процессы и отдельные факты. ОПК-13.3. Формулирует собственную позицию по различным проблемам истории.
ОПК-4.1. Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах	ОПК-4.1.1. Определяет подлежащие защите информационные ресурсы автоматизированных систем. ОПК-4.1.2. Составляет комплексы правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе. ОПК-4.1.3. Организует работу персонала автоматизированной системы с учетом требований по защите информации. ОПК-4.1.4. Готовит документы, определяющие правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации.
ОПК-4.2. Способен администрировать операционные системы, системы управления базами данных, вычислительные сети	ОПК-4.2.1. Настраивает операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации. ОПК-4.2.2. Применяет программные средства обеспечения безопасности данных. ОПК-4.2.3. Управляет полномочиями пользователей автоматизированной системы.
ОПК-4.3. Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	ОПК-4.3.1. Осуществляет автономную наладку технических и программных средств системы защиты информации автоматизированной системы. ОПК-4.3.2. Применяет типовые программные средства резервирования и восстановления информации в автоматизированных системах. ОПК-4.3.3. Устраняет известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации.

ОПК-4.4. Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем	ОПК-4.4.1. Применяет инструментальные средства контроля защищенности информации в автоматизированных системах. ОПК-4.4.2. Документирует действия по устранению неисправностей в работе системы защиты информации автоматизированной системы. ОПК-4.4.3. Регистрирует события, связанные с защитой информации в автоматизированных системах.

4.1.3 Обязательные профессиональные компетенции выпускников и индикаторы их достижения

Обязательные профессиональные компетенции включают в программу бакалавриата при их наличии. Обязательные профессиональные компетенции выпускников не установлены в проекте ПООП.

4.2 Профессиональные компетенции выпускников и индикаторы их достижения

В ОПОП установлены профессиональные компетенции и индикаторы их достижения исходя из направленности (профиля) программы бакалавриата, на основе профессиональных стандартов, соответствующих профессиональной деятельности выпускников (таблица 6).

Таблица 6 – Профессиональные компетенции выпускников и индикаторы их достижения

Задача ПД	Объект или область знания	Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции	Основание (ПС)
Тип задач профессиональной деятельности: эксплуатационный				
Эксплуатация автоматизированных систем в защищённом исполнении	06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности	ПК-1 Способен эксплуатировать средства обеспечения информационной безопасности автоматизированных систем.	ПК-1.1 Производит внедрение в состав автоматизированных систем средств обеспечения информационной безопасности. ПК-1.2 Соотносит функционал автоматизированных систем средств обеспечения информационной безопасности с	06.030 Специалист по защите информации в телекоммуникационных системах и сетях.

	объектов информатизации в условиях существования угроз в информационной сфере)		реализуемыми процедурами обеспечения информационной безопасности.	
			ПК-1.3 Выполняет регламентные работы по эксплуатации средств защиты информации. ПК-1.4 Устраняет неисправности при эксплуатации средств защиты информации.	06.034 Специалист по технической защите информации
		ПК-2 Способен реализовывать политики безопасности с использованием инструментальных средств обеспечения информационной безопасности.	ПК-2.1 Формулирует критерии безопасности обработки информации в автоматизированных системах.	06.033 Специалист по защите информации в автоматизированных системах
			ПК-2.2 Выполняет мероприятия для реализации политики информационной безопасности. ПК-2.3 Определяет состав средств, необходимый для управления автоматизированными системами и средствами их защиты от НСД. ПК-2.4 Определяет порядок настройки технических средств для управления автоматизированными системами и средствами их защиты от НСД.	06.030 Специалист по защите информации в телекоммуникационных системах и сетях
			ПК-2.5 Устанавливает программное обеспечение в соответствии с требованиями по защите информации.	06.032 Специалист по безопасности компьютерных систем и сетей
Обеспечение защищённости процессов обработки информации		ПК-3 Способен обеспечивать безопасную обработку данных в	ПК-3.1 Фиксирует возникновение инцидентов информационной безопасности.	06.033 Специалист по защите информации в

в автоматизированных системах		автоматизированных системах.	ПК-3.2 Использует методы и средства резервного копирования информации. ПК-3.3 Устраняет уязвимости в автоматизированной системе. ПК-3.4 Соотносит изменения в конфигурации автоматизированной системы с её защищенностью.	автоматизированных системах
Тип задач профессиональной деятельности: проектно-технологический				
Внедрение решений, направленных на повышения уровня защищённости и автоматизированных систем	06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере)	ПК-4 Способен выполнять работы по проектированию автоматизированных систем в защищенном исполнении.	ПК-4.1 Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных систем. ПК-4.2 Готовит техническую и проектную документацию по вопросам создания и эксплуатации автоматизированных систем. ПК-4.3 Проверяет программы и алгоритмы на предмет соответствия требованиям защиты информации. ПК-4.4 Проводит сравнительный анализ вариантов конфигураций и состава автоматизированных систем. ПК-4.5 Предлагает конфигурации и состав автоматизированной системы.	06.032 Специалист по безопасности компьютерных систем и сетей
Сопровождение систем обеспечения информационной безопасности на всех этапах жизненного		ПК-5 Способен выполнять работы по обеспечению информационной безопасности автоматизированных систем на всех этапах их	ПК-5.1 Проверяет соответствие внедряемых решений и средств для обеспечения информационной безопасности требованиям реализуемой политики безопасности. ПК-5.2 Восстанавливает	06.030 Специалист по защите информации в телекоммуникационных системах и

цикла		жизненного цикла.	работоспособность автоматизированных систем после инцидентов информационной безопасности. ПК-5.3 Проводит операции вывода защищённых автоматизированных систем из эксплуатации.	сетях 06.033 Специалист по защите информации в автоматизированных системах
Участие в создании технической документации по результатам выполнения работ по обеспечению информационной безопасности	06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере)	ПК-6 Способен документально оформлять работы по обеспечению информационной безопасности.	ПК-6.1 Анализирует полноту и нормативным требованиям руководящих документов, описывающих работы по обеспечению информационной безопасности. ПК-6.2 Формирует отчётные и руководящие документы для обеспечения защиты информации в информационной системе в ходе ее эксплуатации. ПК-6.3 Формулирует в соответствии с требованиям руководящих документов состав и содержание процедур контроля обеспеченности уровня защищенности информации. ПК-6.4 Готовит документы для проведения работ по аттестации объектов информатизации и автоматизированных систем.	06.033 Специалист по защите информации в автоматизированных системах

Тип задач профессиональной деятельности: экспериментально-исследовательский				
Определение соответствия достигаемого уровня защищённости и требования нормативных документов	06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере)	ПК-7 Способен определять уровень защищённости автоматизированных систем.	ПК-7.1 Формулирует целевые показатели функционирования защищенных автоматизированных систем. ПК-7.2 Анализирует уязвимости автоматизированных систем в соответствии с нормативными документами. ПК-7.3 Формулирует угрозы информационной безопасности исходя из выявленных характеристик автоматизированной системы.	06.033 Специалист по защите информации в автоматизированных системах
Использование инструментальных средств анализа защищённости автоматизированных систем		ПК-8 Способен выполнять задачи по выявлению уязвимых узлов автоматизированной системы.	ПК-8.1 Разрабатывает методическую, техническую, рекомендательную и отчётную документацию по анализу защищённости автоматизированной системы. ПК-8.2 Осуществляет подбор программных средств тестирования защищённости автоматизированной системы в зависимости от предъявляемым к ней требованиям. ПК-8.3 Использует средств инструментального анализа защищённости программных и аппаратных платформ узлов автоматизированной системы. ПК-8.4 Проводит контроль защищённости и функционирования программно-аппаратных и технических средств автоматизированной	06.030 Специалист по защите информации в телекоммуникационных системах и сетях

			системы.	
Тип задач профессиональной деятельности: организационно-управленческий				
Организация и выполнение работ по обеспечению информационной безопасности в автоматизированных системах	06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере)	ПК-9 Способен организовывать работы по обеспечению информационной безопасности в автоматизированных системах.	ПК-9.1 Формулирование правил работы персонала со средствами защиты информации. ПК-9.2 Распределяет обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему. ПК-9.3 Сопоставляет результат работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации.	06.030 Специалист по защите информации в телекоммуникационных системах и сетях 06.033 Специалист по защите информации в автоматизированных системах
Подготовка данных для составления обзоров и отчетов по инцидентам информационной безопасности		ПК-10 Способен собирать, анализировать и систематизировать информацию по зафиксированным инцидентам информационной безопасности.	ПК-10.1 Соотносит инциденты информационной безопасности с характеристиками систем и средств защиты информации. ПК-10.2 Обосновывает необходимость модернизации системы защиты информации автоматизированной системы. ПК-10.3 Формулирует правила применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности. ПК-10.4 Формулирует правила протоколирования результатов мониторинга безопасности	06.033 Специалист по защите информации в автоматизированных системах

			автоматизированных систем	

В процессе формирования требований из каждого выбранного профессионального стандарта выделена одна или несколько обобщенных трудовых функций (далее – ОТФ), соответствующих профессиональной деятельности выпускников, на основе установленных профессиональным стандартом для ОТФ уровня квалификации и требований раздела «Требования к образованию и обучению» ФГОС ВО. Сводные данные показаны в таблице 7.

Таблица 7 – Соответствие профессиональных компетенций ОТФ

Профессиональный стандарт	Индекс ОТФ	Наименование ОТФ	Компетенции дисциплины	Требования к образованию установленные профстандартом
06.030 Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденный приказом Минтруда России от 14 сентября 2022 г. N 536н «Об утверждении профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях» (Зарегистрировано в Минюсте России 18 октября 2022 г. N 70596)	B	Обеспечение защиты от НД и компьютерных атак сооружений и СССЭ (за исключением сетей связи специального назначения) в процессе их эксплуатации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10	Высшее образование - бакалавриат
06.032 Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей», утвержденный приказом Минтруда России от 14 сентября 2022 г. N 533н «Об утверждении профессионального	B	Администрирование средств защиты информации в компьютерных системах и сетях	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10	Высшее образование - бакалавриат

стандарта «Специалист по безопасности компьютерных систем и сетей» (Зарегистрировано в Минюсте России 14 октября 2022 г. N 70515)				
06.033 Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержденный приказом Минтруда России от 14 сентября 2022 г. N 525н «Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах» (Зарегистрировано в Минюсте России 14 октября 2022 г. N 70543)	B	Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10	Высшее образование - бакалавриат
06.034 Профессиональный стандарт «Специалист по технической защите информации» утвержденный приказом Минтруда России от 9 августа 2022 г. N 474н «Об утверждении профессионального стандарта «Специалист по технической защите информации» (Зарегистрировано в Минюсте России 9 сентября 2022 г. N 70015)	B	Проведение работ по установке и техническому обслуживанию защищенных средств обработки информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10	Высшее образование - бакалавриат
	E	Проведение контроля защищенности информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10	

ОТФ выделены частично в соответствии с требованиями пункта 3.5 ФГОС ВО. Выделение показано в таблице 8.

Таблица 8 – Соответствие профессиональных компетенций трудовым функциям

Индекс	Наименование	Компетенции
06	СВЯЗЬ, ИНФОРМАЦИОННЫЕ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ	
06.030	СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
B	Обеспечение защиты от НД и компьютерных атак сооружений и СССЭ (за исключением сетей связи специального назначения) в процессе их эксплуатации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
B/01.6	Мониторинг функционирования СССЭ, защищенности от НД и компьютерных атак сооружений и СССЭ	ПК-1; ПК-6; ПК-8
ТД.1	Присвоение объекту критической информационной инфраструктуры одной из категорий значимости	ПК-1
ТД.6	Составление отчетов по результатам проверок, в том числе выявление инцидентов, которые могут привести к сбоям или нарушению функционирования или возникновению угроз безопасности информации, циркулирующей в СССЭ	ПК-6; ПК-8
У.1	Использовать установленные федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации формы документов, сопровождающих жизненный цикл объекта критической информационной инфраструктуры	ПК-8
У.2	Использовать средства мониторинга работоспособности и эффективности применяемых программных, программно-аппаратных (в том числе криптографических) и технических средств защиты СССЭ от НД и компьютерных атак	ПК-8
У.3	Проводить контроль функционирования СССЭ, их защищенности от НД и компьютерных атак	ПК-8
У.7	Проводить документационное обеспечение функционирования СССЭ, их защищенности от НД и компьютерных атак	ПК-6
Зн.5	Возможные источники и технические каналы утечки информации	ПК-8
Зн.7	Законодательство Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры	ПК-6

Зн.8	Нормативные правовые акты Президента Российской Федерации, Правительства Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации по вопросам обеспечения информационной безопасности СССЭ	ПК-6
B/02.6	Управление функционированием СССЭ, защищенностью от НД и компьютерных атак сооружений и СССЭ	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
ТД.1	Определение необходимого состава, особенностей размещения и функциональных возможностей СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД и компьютерных атак	ПК-2
ТД.3	Контроль соответствия параметров подсистем защиты СССЭ от НД и компьютерных атак установленным требованиям, обеспечение своевременной корректировки настроек СССЭ, средств и систем их защиты от НД и компьютерных атак в целях реагирования на выявленные нарушения	ПК-10
ТД.4	Установка и настройка программного обеспечения, необходимого для управления СССЭ и средствами их защиты от НД и компьютерных атак	ПК-2; ПК-8
ТД.5	Разработка и организация выполнения мероприятий в соответствии с положениями политики информационной безопасности в сети электросвязи	ПК-2
ТД.6	Проведение отдельных мероприятий в рамках аттестации на предмет соответствия требованиям по защите сооружений и СССЭ от НД и компьютерных атак	ПК-6
У.4	Устанавливать и настраивать параметры сетевых протоколов, реализованных в телекоммуникационном оборудовании	ПК-10
Зн.2	Сетевые протоколы и их параметры настройки	ПК-10
Зн.7	Нормативные правовые акты в области защиты информации ограниченного доступа	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
Зн.8	Национальные, межгосударственные и международные стандарты в области защиты информации	ПК-6
Зн.9	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10

	информационной инфраструктуры	
B/03.6	Управление персоналом, обслуживающим сооружения и СССЭ, а также программные, программно-аппаратные (в том числе криптографические) и технические средства и системы их защиты от НД, средства для поиска признаков компьютерных атак в сетях электросвязи	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
ТД.1	Формирование целей, приоритетов, обязанностей и полномочий персонала, обслуживающего сооружения и СССЭ, средства и системы их защиты от НД, средства для поиска признаков компьютерных атак в сетях электросвязи	ПК-9
ТД.2	Распределение обязанностей и полномочий персонала, обслуживающего сооружения и СССЭ, средства и системы их защиты от НД, средства для поиска признаков компьютерных атак в сетях электросвязи	ПК-9
ТД.3	Проверка уровня квалификации персонала, обслуживающего сооружения и СССЭ, средства их защиты от НД, средства для поиска признаков компьютерных атак в сетях электросвязи, в том числе при приеме на работу	ПК-9
ТД.4	Контроль выполнения персоналом требований инструкций и регламентов по эксплуатации СССЭ, средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи	ПК-9
У.1	Производить постановку задач персоналу по обеспечению защиты СССЭ от НД и компьютерных атак в сетях электросвязи и организовывать их выполнение	ПК-9
У.3	Организовывать перераспределение обязанностей и полномочий персонала, обслуживающего сооружения и СССЭ, средства и системы их защиты от НД, средства для поиска признаков компьютерных атак в сетях электросвязи	ПК-9
Зн.1	Цели и задачи управления персоналом по обеспечению защиты сетей электросвязи от НД и компьютерных атак в сетях электросвязи	ПК-9
Зн.3	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10

	Зн.4	Критерии комплексной оценки квалификации персонала, обслуживающего сооружения и СССЭ, средства и системы их защиты от НД, средства для поиска признаков компьютерных атак в сетях электросвязи	ПК-9
06.032		СПЕЦИАЛИСТ ПО БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
	B	Администрирование средств защиты информации в компьютерных системах и сетях	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
	B/01.6	Администрирование подсистем защиты информации в операционных системах	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
	ТД.1	Определение состава применяемых программно-аппаратных средств защиты информации в операционных системах	ПК-1; ПК-2
	ТД.2	Разработка порядка применения программно-аппаратных средств защиты информации в операционных системах	ПК-2; ПК-9
	ТД.3	Формирование шаблонов установки программно-аппаратных средств защиты информации в операционных системах	ПК-2
	ТД.4	Установка программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации	ПК-2
	ТД.5	Конфигурирование программно-аппаратных средств защиты информации в операционных системах	ПК-2
	ТД.7	Управление антивирусной защитой операционных систем в соответствии с действующими требованиями	ПК-2
	У.1	Формулировать политики безопасности операционных систем	ПК-2
	У.2	Настраивать политики безопасности операционных систем	ПК-2
	У.3	Оценивать угрозы безопасности информации операционных систем	ПК-2
	У.4	Противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем	ПК-2
	У.5	Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах	ПК-2
	У.6	Настраивать антивирусные средства защиты информации в операционных системах	ПК-2
	У.7	Устанавливать обновления программного обеспечения и средств антивирусной защиты	ПК-2
	У.8	Проводить мониторинг функционирования программно-аппаратных средств защиты	ПК-2

	информации в операционных системах	
У.9	Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах	ПК-2
У.10	Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах	ПК-2
Зн.1	Архитектура и принципы построения операционных систем	ПК-2
Зн.2	Программные интерфейсы операционных систем	ПК-2
Зн.3	Виды политик управления доступом и информационными потоками применительно к операционным системам	ПК-2
Зн.4	Архитектура подсистем защиты информации в операционных системах	ПК-2; ПК-4
Зн.5	Принципы функционирования средств защиты информации в операционных системах, в том числе использующих криптографические алгоритмы	ПК-2
Зн.6	Состав типовых конфигураций программно-аппаратных средств защиты информации	ПК-2
Зн.7	Требования по составу и характеристикам подсистем защиты информации применительно к операционным системам	ПК-2
Зн.8	Порядок реализации методов и средств антивирусной защиты в операционных системах	ПК-2
Зн.9	Программно-аппаратные средства и методы защиты информации в операционных системах	ПК-1; ПК-2
Зн.10	Принципы работы и правила эксплуатации программно-аппаратных средств защиты информации	ПК-2
Зн.11	Нормативные правовые акты в области защиты информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
Зн.12	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
Зн.13	Организационные меры по защите информации	ПК-1; ПК-2; ПК-3; ПК-5; ПК-6; ПК-7; ПК-8; ПК-10
B/02.6	Администрирование программно-аппаратных средств защиты информации в компьютерных сетях	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
ТД.1	Определение состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях	ПК-1; ПК-2; ПК-4
ТД.2	Разработка порядка применения программно-аппаратных средств защиты информации в компьютерных	ПК-2

	сетях	
ТД.3	Формирование шаблонов конфигурации программно-аппаратных средств защиты информации в компьютерных сетях	ПК-2
ТД.4	Настройка программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации	ПК-2
ТД.5	Управление функционированием программно-аппаратных средств защиты информации в компьютерных сетях	ПК-2
ТД.6	Контроль корректности функционирования программно-аппаратных средств защиты информации в компьютерных сетях	ПК-1
ТД.7	Управление средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями	ПК-2
У.1	Оценивать угрозы безопасности информации в компьютерных сетях	ПК-7
У.2	Настраивать правила фильтрации пакетов в компьютерных сетях	ПК-7
У.3	Обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях	ПК-7; ПК-8
У.4	Конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях	ПК-1
У.5	Выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях	ПК-1
У.6	Проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях	ПК-1
У.7	Производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях	ПК-2
У.8	Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях	ПК-2
Зн.1	Принципы построения компьютерных сетей	ПК-2
Зн.2	Стек сетевых протоколов операционных систем	ПК-2
Зн.3	Стек протоколов сетевого оборудования	ПК-2
Зн.4	Порядок реализации методов и средств межсетевого экранирования	ПК-2
Зн.5	Принципы функционирования сетевых протоколов, включающих	ПК-2

	криптографические алгоритмы	
Зн.6	Виды политик управления доступом и информационными потоками в компьютерных сетях	ПК-2
Зн.7	Источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению	ПК-2
Зн.8	Состав типовых конфигураций программно-аппаратных средств защиты информации и режимов их функционирования в компьютерных сетях	ПК-2
Зн.9	Методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации	ПК-2
Зн.10	Принципы работы и правила эксплуатации применяемых программно-аппаратных средств защиты информации	ПК-2
Зн.11	Программно-аппаратные средства и методы защиты информации в компьютерных сетях	ПК-1; ПК-2
Зн.12	Нормативные правовые акты в области защиты информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
Зн.13	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
Зн.14	Организационные меры по защите информации	ПК-1; ПК-2; ПК-3; ПК-5; ПК-6; ПК-7; ПК-8; ПК-10
B/03.6	Администрирование средств защиты информации прикладного и системного программного обеспечения	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
ТД.1	Определение порядка установки программного обеспечения с целью соблюдения требований по защите информации	ПК-2
ТД.2	Контроль за соблюдением требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение	ПК-2
ТД.3	Формулирование требований к параметрам средств антивирусной защиты для корректной работы программного обеспечения	ПК-2
ТД.4	Выполнение работ по обнаружению вредоносного программного обеспечения	ПК-1
ТД.5	Ликвидация обнаруженного вредоносного программного обеспечения и последствий его функционирования	ПК-1; ПК-3
ТД.6	Формулирование требований к встроенным средствам защиты информации программного обеспечения	ПК-4

У.1	Анализировать угрозы безопасности информации программного обеспечения	ПК-3
У.2	Формулировать правила безопасной эксплуатации программного обеспечения	ПК-3
У.3	Обосновывать правила безопасной эксплуатации программного обеспечения	ПК-3
У.4	Анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия	ПК-4
У.5	Производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации	ПК-4
У.6	Осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения	ПК-10
У.7	Определять порядок функционирования программного обеспечения с целью обеспечения защиты информации	ПК-5
У.8	Анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения	ПК-5
Зн.1	Архитектура подсистем защиты информации в операционных системах	ПК-2; ПК-4
Зн.2	Принципы построения систем управления базами данных	ПК-4
Зн.3	Основные средства и методы анализа программных реализаций	ПК-4
Зн.4	Принципы построения антивирусного программного обеспечения	ПК-4
Зн.5	Виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению	ПК-2
Зн.6	Источники угроз информационной безопасности программного обеспечения и меры по их предотвращению	ПК-3
Зн.7	Уязвимости используемого программного обеспечения и методы их устранения	ПК-1; ПК-3
Зн.8	Виды и формы функционирования вредоносного программного обеспечения	ПК-3
Зн.9	Характерные признаки наличия вредоносного программного обеспечения	ПК-3
Зн.10	Средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения	ПК-3
Зн.11	Принципы функционирования программных средств	ПК-2

		криптографической защиты информации	
	Зн.12	Порядок обеспечения безопасности информации при эксплуатации программного обеспечения	ПК-1
	Зн.13	Нормативные правовые акты в области защиты информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
	Зн.14	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
	Зн.15	Организационные меры по защите информации	ПК-1; ПК-2; ПК-3; ПК-5; ПК-6; ПК-7; ПК-8; ПК-10
06.033		СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
	B	Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
	B/01.6	Диагностика систем защиты информации автоматизированных систем	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
	ТД.1	Обнаружение инцидентов в процессе эксплуатации автоматизированной системы	ПК-3
	ТД.2	Идентификация инцидентов в процессе эксплуатации автоматизированной системы	ПК-3; ПК-10
	ТД.3	Оценка защищенности автоматизированных систем с помощью типовых программных средств	ПК-7; ПК-8
	ТД.4	Устранение последствий инцидентов, возникших в процессе эксплуатации автоматизированной системы	ПК-3; ПК-5; ПК-10
	У.1	Определять источники и причины возникновения инцидентов	ПК-3; ПК-7; ПК-8
	У.2	Оценивать последствия выявленных инцидентов	ПК-7; ПК-10
	У.3	Обнаруживать нарушения правил разграничения доступа	ПК-3; ПК-8
	У.4	Устранять нарушения правил разграничения доступа	ПК-1; ПК-3; ПК-5; ПК-10
	У.5	Осуществлять контроль обеспечения уровня защищенности в автоматизированных системах	ПК-1; ПК-3; ПК-4; ПК-5
	У.6	Использовать криптографические методы и средства защиты информации в автоматизированных системах	ПК-1; ПК-2
	Зн.1	Нормативные правовые акты в области защиты информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
	Зн.2	Национальные, межгосударственные и международные стандарты в области защиты информации	ПК-1; ПК-2; ПК-3; ПК-5; ПК-6; ПК-7; ПК-8; ПК-10

Зн.3	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
Зн.4	Организационные меры по защите информации	ПК-1; ПК-2; ПК-3; ПК-5; ПК-6; ПК-7; ПК-8; ПК-10
Зн.5	Принципы построения средств защиты информации от несанкционированного доступа и утечки по техническим каналам	ПК-4
Зн.6	Критерии оценки защищенности автоматизированной системы	ПК-1; ПК-2; ПК-3; ПК-5; ПК-6; ПК-7; ПК-8; ПК-10
Зн.8	Регламент информирования персонала автоматизированной системы о выявленных инцидентах	ПК-9; ПК-10
Зн.9	Регламент учета выявленных инцидентов	ПК-10
Зн.10	Регламент устранения последствий инцидентов	ПК-10
Зн.11	Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах	ПК-1; ПК-2
B/02.6	Администрирование систем защиты информации автоматизированных систем	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
ТД.1	Установка обновлений программного обеспечения автоматизированной системы	ПК-1; ПК-2; ПК-3; ПК-4
ТД.2	Выполнение установленных процедур обеспечения безопасности информации с учетом требования эффективного функционирования автоматизированной системы	ПК-1; ПК-2
ТД.3	Управление полномочиями доступа пользователей автоматизированной системы	ПК-7
ТД.4	Информирование пользователей о правилах эксплуатации автоматизированной системы с учетом требований по защите информации	ПК-9
ТД.5	Проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий с персоналом на макетах или в тестовой зоне	ПК-9
ТД.6	Внесение изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы	ПК-6; ПК-8
У.1	Создавать, удалять и изменять учетные записи пользователей автоматизированной системы	ПК-9
У.2	Формировать политику безопасности программных компонентов автоматизированных систем	ПК-7

У.3	Устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации	ПК-1; ПК-5
У.4	Использовать криптографические методы и средства защиты информации в автоматизированных системах	ПК-1; ПК-2; ПК-3; ПК-5; ПК-7
У.5	Регистрировать события, связанные с защитой информации в автоматизированных системах	ПК-1; ПК-3; ПК-6; ПК-8; ПК-10
У.6	Анализировать события, связанные с защитой информации в автоматизированных системах	ПК-7; ПК-8; ПК-10
Зн.1	Принципы формирования политики информационной безопасности в автоматизированных системах	ПК-2; ПК-5; ПК-6; ПК-7; ПК-8; ПК-10
Зн.2	Программно-аппаратные средства защиты информации автоматизированных систем	ПК-1; ПК-2
Зн.3	Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах	ПК-1
Зн.4	Методы контроля эффективности защиты информации от утечки по техническим каналам	ПК-5; ПК-7; ПК-10
Зн.5	Критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем	ПК-8; ПК-10
Зн.6	Технические средства контроля эффективности мер защиты информации	ПК-8; ПК-10
Зн.7	Принципы организации и структура систем защиты программного обеспечения автоматизированных систем	ПК-5
Зн.8	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем	ПК-6; ПК-9
Зн.9	Основные меры по защите информации в автоматизированных системах	ПК-2; ПК-4
В/03.6	Управление защитой информации в автоматизированных системах	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
ТД.1	Анализ воздействия изменений конфигурации автоматизированной системы на ее защищенность	ПК-1; ПК-3
ТД.2	Составление комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	ПК-1; ПК-2; ПК-4; ПК-6; ПК-7; ПК-8; ПК-10
ТД.3	Оценка последствий от реализации угроз безопасности информации в автоматизированной системе	ПК-10
ТД.4	Анализ изменения угроз безопасности информации автоматизированной	ПК-1; ПК-3

	системы, возникающих в ходе ее эксплуатации	
У.1	Оценивать информационные риски в автоматизированных системах	ПК-1; ПК-3; ПК-4; ПК-7
У.2	Классифицировать и оценивать угрозы безопасности информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-10
У.3	Определять подлежащие защите информационные ресурсы автоматизированных систем	ПК-1; ПК-2; ПК-3
У.4	Применять нормативные документы по защите от несанкционированного доступа к информации и противодействию технической разведке	ПК-1; ПК-2; ПК-4; ПК-5; ПК-6; ПК-7
У.6	Конфигурировать параметры системы защиты информации автоматизированных систем	ПК-1; ПК-2; ПК-5; ПК-7
У.7	Применять технические средства контроля эффективности мер защиты информации	ПК-8
Зн.1	Основные методы управления защитой информации	ПК-1; ПК-2
Зн.2	Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	ПК-1; ПК-4; ПК-5; ПК-6; ПК-10
Зн.3	Методы защиты информации от несанкционированного доступа и утечки по техническим каналам	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-7; ПК-8; ПК-10
Зн.4	Нормативные правовые акты в области защиты информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
Зн.5	Национальные, межгосударственные и международные стандарты в области защиты информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
Зн.6	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
B/04.6	Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
ТД.1	Обнаружение неисправностей в работе системы защиты информации автоматизированной системы	ПК-1
ТД.2	Устранение неисправностей в работе системы защиты информации автоматизированной системы	ПК-1; ПК-3
ТД.3	Резервирование программного обеспечения, технических средств, каналов передачи данных автоматизированной системы управления на случай возникновения нештатных ситуаций	ПК-1; ПК-3
ТД.5	Восстановление после сбоев и отказов программного обеспечения автоматизированных систем	ПК-5
У.1	Применять типовые программные средства резервирования и восстановления информации в автоматизированных системах	ПК-1; ПК-3
У.3	Классифицировать и оценивать угрозы информационной безопасности	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-10

У.4	Применять программные средства обеспечения безопасности данных	ПК-1; ПК-3
У.5	Документировать действия по устранению неисправностей в работе системы защиты информации автоматизированной системы	ПК-6
Зн.2	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем	ПК-9
Зн.3	Основные информационные технологии, используемые в автоматизированных системах	ПК-4
Зн.4	Принципы построения средств защиты информации от утечки по техническим каналам	ПК-4
Зн.5	Программно-аппаратные средства обеспечения защиты информации автоматизированных систем	ПК-1; ПК-2
Зн.6	Нормативные правовые акты в области защиты информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
Зн.7	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
Зн.8	Организационные меры по защите информации	ПК-1; ПК-2; ПК-3; ПК-5; ПК-6; ПК-7; ПК-8; ПК-10
B/05.6	Мониторинг защищенности информации в автоматизированных системах	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
ТД.1	Выработка рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-7; ПК-8; ПК-10
ТД.2	Выработка рекомендаций для принятия решения о повторной аттестации автоматизированной системы или о проведении дополнительных аттестационных испытаний	ПК-6
ТД.3	Выявление угроз безопасности информации в автоматизированных системах	ПК-4; ПК-7; ПК-8
ТД.4	Принятие мер защиты информации при выявлении новых угроз безопасности информации	ПК-10
ТД.6	Устранение недостатков в функционировании системы защиты информации автоматизированной системы	ПК-1; ПК-3
У.1	Классифицировать и оценивать угрозы информационной безопасности	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-10
У.2	Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах	ПК-4

У.3	Применять нормативные документы по защите информации от несанкционированного доступа и противодействию технической разведке	ПК-1; ПК-2; ПК-4; ПК-5; ПК-6; ПК-7
У.5	Контролировать события безопасности и действия пользователей автоматизированных систем	ПК-6; ПК-8; ПК-9; ПК-10
У.6	Применять технические средства контроля эффективности мер защиты информации	ПК-8
У.7	Документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы	ПК-3; ПК-6
Зн.1	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем	ПК-9
Зн.2	Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	ПК-1; ПК-4; ПК-5; ПК-6; ПК-10
Зн.3	Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах	ПК-1
Зн.4	Программно-аппаратные средства обеспечения защиты информации автоматизированных систем	ПК-1; ПК-2
Зн.5	Методы защиты информации от утечки по техническим каналам	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-7; ПК-8; ПК-10
Зн.6	Нормативные правовые акты в области защиты информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
Зн.7	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
Зн.8	Организационные меры по защите информации	ПК-1; ПК-2; ПК-3; ПК-5; ПК-6; ПК-7; ПК-8; ПК-10
B/06.6	Аудит защищенности информации в автоматизированных системах	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
ТД.1	Оценка информационных рисков безопасности информации в автоматизированной системе	ПК-1; ПК-3; ПК-4; ПК-7
У.1	Классифицировать и оценивать угрозы безопасности информации для объекта информатизации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-10
У.3	Разрабатывать политики безопасности информации автоматизированных систем	ПК-2
У.4	Применять инструментальные средства контроля защищенности информации в автоматизированных системах	ПК-8; ПК-10
Зн.1	Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах	ПК-1
Зн.2	Способы защиты информации от несанкционированного доступа и утечки по техническим каналам	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-7; ПК-8; ПК-10

Зн.3	Методы контроля эффективности защиты информации от несанкционированного доступа и утечки по техническим каналам	ПК-8; ПК-10
Зн.4	Принципы построения систем защиты информации	ПК-4
Зн.5	Нормативные правовые акты в области защиты информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
Зн.6	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
Зн.7	Организационные меры по защите информации	ПК-1; ПК-3; ПК-5; ПК-6; ПК-7; ПК-8; ПК-10
B/07.6	Установка и настройка средств защиты информации в автоматизированных системах	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
ТД.2	Осуществление автономной наладки технических и программных средств системы защиты информации автоматизированной системы	ПК-1; ПК-2
У.1	Администрировать программные средства системы защиты информации автоматизированных систем	ПК-1; ПК-2
У.2	Устранять известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации	ПК-1; ПК-2
У.3	Применять нормативные документы по защите информации от несанкционированного доступа и противодействию технической разведке	ПК-1; ПК-2; ПК-4; ПК-5; ПК-6; ПК-7
У.6	Определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы	ПК-1; ПК-2
Зн.1	Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	ПК-1; ПК-4; ПК-5; ПК-6; ПК-10
Зн.2	Содержание эксплуатационной документации автоматизированной системы	ПК-1; ПК-2; ПК-3; ПК-4
Зн.3	Типовые средства, методы и протоколы идентификации, аутентификации и авторизации	ПК-1; ПК-2; ПК-3
Зн.4	Основные меры по защите информации в автоматизированных системах	ПК-2; ПК-4
Зн.5	Нормативные правовые акты в области защиты информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
Зн.6	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
B/08.6	Разработка организационно-распорядительных документов по защите информации в автоматизированных системах	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
ТД.1	Определение правил и процедур управления системой защиты информации автоматизированной системы	ПК-6; ПК-8; ПК-9; ПК-10

ТД.4	Определение правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации	ПК-5
ТД.5	Определение правил и процедур реагирования на инциденты в автоматизированной системе	ПК-10
У.1	Классифицировать и оценивать угрозы информационной безопасности	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-10
У.2	Применять нормативные документы по защите информации от несанкционированного доступа и противодействию технической разведке	ПК-1; ПК-2; ПК-4; ПК-5; ПК-6; ПК-7
У.3	Определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы	ПК-1; ПК-2
Зн.1	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации	ПК-6; ПК-9
Зн.2	Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	ПК-1; ПК-4; ПК-5; ПК-6; ПК-10
Зн.3	Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах	ПК-1
Зн.4	Принципы построения средств защиты информации от несанкционированного доступа и утечки по техническим каналам	ПК-4
Зн.5	Нормативные правовые акты в области защиты информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
Зн.6	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-8; ПК-9; ПК-10; ПК-6.4
В/09.6	Анализ уязвимостей внедряемой системы защиты информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
У.1	Классифицировать и оценивать угрозы безопасности информации автоматизированной системы	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-10
У.3	Проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-10
У.4	Устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-10
Зн.1	Основные методы и средства криптографической защиты информации	ПК-2
Зн.4	Нормативные правовые акты в области защиты информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
Зн.5	Руководящие и методические документы уполномоченных федеральных органов исполнительной	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10

		власти по защите информации	
	Зн.6	Организационные меры по защите информации	ПК-1; ПК-2; ПК-3; ПК-5; ПК-6; ПК-7; ПК-8; ПК-10
	Зн.7	Содержание эксплуатационной документации автоматизированной системы	ПК-1; ПК-2; ПК-3; ПК-4
B/10.6		Внедрение организационных мер по защите информации в автоматизированных системах	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
	ТД.1	Проведение проверки полноты описания в организационно-распорядительных документах на автоматизированную систему действий персонала по реализации организационных мер защиты информации	ПК-6
	ТД.2	Проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий на макетах или в тестовой зоне	ПК-9
	ТД.3	Подготовка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации	ПК-9
	ТД.4	Проведение проверки готовности персонала к эксплуатации системы защиты информации автоматизированной системы	ПК-9
	У.1	Реализовывать правила разграничения доступа персонала к объектам доступа	ПК-2; ПК-9
	У.3	Консультирование персонала автоматизированной системы по комплексу мер (правилам, процедурам, практическим приемам, руководящим принципам, методам, средствам) обеспечения защиты информации	ПК-9
	У.4	Осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации	ПК-9
	Зн.2	Методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и систем защиты автоматизированных систем	ПК-4
	Зн.3	Нормативные правовые акты в области защиты информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
	Зн.4	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
	Зн.5	Организационные меры по защите информации	ПК-1; ПК-2; ПК-3; ПК-5; ПК-6; ПК-7; ПК-8; ПК-10
06.034		СПЕЦИАЛИСТ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
	B	Проведение работ по установке и техническому обслуживанию защищенных средств обработки информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10

B/01.6	Проведение работ по установке, настройке, испытаниям и техническому обслуживанию защищенных технических средств обработки информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
ТД.1	Установка и монтаж защищенных технических средств обработки информации	ПК-2
ТД.2	Настройка защищенных технических средств обработки информации	ПК-1
ТД.4	Техническое обслуживание защищенных технических средств обработки информации	ПК-1
У.1	Производить установку и монтаж защищенных технических средств обработки информации	ПК-2
У.2	Проводить настройку защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами	ПК-2
У.4	Проводить техническое обслуживание защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-технической документацией	ПК-1
У.5	Проводить устранение выявленных неисправностей защищенных технических средств обработки информации и при необходимости организовывать их ремонт	ПК-1
Зн.1	Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и эксплуатации защищенных технических средств обработки информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
Зн.2	Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом высокочастотного облучения основных технических средств и систем и за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах	ПК-6; ПК-8
Зн.3	Способы и средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок	ПК-6; ПК-8

Зн.4	Средства и методики контроля эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок	ПК-6; ПК-8
Зн.5	Технические описания и инструкции по эксплуатации технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок	ПК-6; ПК-8
Зн.6	Проектная документация на систему защиты объекта информатизации (в части защиты объекта от утечки информации за счет побочных электромагнитных излучений и наводок)	ПК-6; ПК-8
Зн.7	Способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах	ПК-6; ПК-8
Зн.8	Методы и средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее	ПК-6; ПК-8
Зн.9	Методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий	ПК-6; ПК-8
Зн.10	Средства и методики контроля защищенности информации от несанкционированного доступа	ПК-6; ПК-8
Зн.11	Технические описания и инструкции по эксплуатации защищенных технических средств обработки информации	ПК-6; ПК-8
Зн.14	Порядок аттестации объектов информатизации на соответствие требованиям безопасности информации	ПК-6
B/02.6	Проведение работ по установке, монтажу, наладке, испытаниям и техническому обслуживанию защищенных программных (программно-технических) средств обработки информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
ТД.1	Установка и монтаж защищенных программных (программно-технических) средств обработки информации	ПК-2
ТД.2	Настройка защищенных программных (программно-технических) средств обработки информации	ПК-1
ТД.4	Техническое обслуживание защищенных программно-технических средств обработки информации	ПК-1
У.1	Производить установку и монтаж защищенных программных (программно-технических) средств обработки информации	ПК-2

	У.2	Проводить настройку защищенных программных (программно-технических) средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами	ПК-2
	У.4	Проводить техническое обслуживание защищенных программно-технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-технической документацией	ПК-1
	У.5	Проводить устранение выявленных неисправностей защищенных программно-технических средств обработки информации и при необходимости организовывать их ремонт	ПК-1
	Зн.1	Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и эксплуатации защищенных программных (программно-технических) средств обработки информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
	Зн.2	Способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах	ПК-6; ПК-8
	Зн.3	Методы и средства защиты информации от несанкционированного доступа и специальных программных воздействий на нее	ПК-6; ПК-8
	Зн.4	Средства и методики контроля защищенности информации от несанкционированного доступа	ПК-6; ПК-8
	Зн.5	Технические описания и инструкции по эксплуатации защищенных программных (программно-технических) средств обработки информации	ПК-6; ПК-8
	Зн.6	Порядок организации технического обслуживания защищенных программно-технических средств обработки информации	ПК-6; ПК-8
	Зн.7	Порядок устранения неисправностей защищенных программно-технических средств обработки информации и организации их ремонта	ПК-6; ПК-8
	Зн.8	Порядок аттестации объектов информатизации на соответствие требованиям безопасности информации	ПК-6
Е		Проведение контроля защищенности информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
	Е/01.6	Проведение специальных исследований на побочные электромагнитные излучения и наводки технических средств обработки информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10

ТД.3	Подготовка отчетных материалов по результатам специальных исследований на побочные электромагнитные излучения и наводки технических средств обработки информации (предписаний на эксплуатацию технических средств и протоколов по результатам специальных исследований технических средств обработки информации)	ПК-6
У.1	Проводить измерение электрической и магнитной составляющей побочных электромагнитных излучений технических средств обработки информации в различных режимах их работы с использованием контрольно-измерительной аппаратуры	ПК-6
У.2	Проводить измерение наводок побочных электромагнитных излучений технических средств обработки информации в различных режимах их работы с использованием контрольно-измерительной аппаратуры	ПК-6
У.3	Рассчитывать радиусы опасных зон побочных электромагнитных излучений и наводок	ПК-6
У.4	Оформлять предписания на эксплуатацию технических средств и протоколы по результатам специальных исследований технических средств обработки информации	ПК-6
Зн.1	Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
Зн.2	Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом высокочастотного облучения основных технических средств и систем и за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах	ПК-6
Зн.3	Средства контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок	ПК-6; ПК-8
Зн.4	Методики проведения специальных исследований на побочные электромагнитные излучения и наводки технических средств обработки	ПК-6; ПК-8

	информации	
Зн.5	Методики расчета радиусов опасных зон побочных электромагнитных излучений и наводок	ПК-6; ПК-8
Зн.6	Отчетные документы, оформляемые по результатам специальных исследований на побочные электромагнитные излучения и наводки технических средств обработки информации	ПК-6; ПК-8
Е/02.6	Проведение контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
ТД.1	Проверка состояния организации работ и выполнения требований по защите информации от утечки за счет побочных электромагнитных излучений и наводок	ПК-6
ТД.3	Подготовка отчетных материалов по результатам контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок (протоколов оценки защищенности информации от утечки за счет побочных электромагнитных излучений и наводок)	ПК-6
У.1	Проверять состояние организации работ и выполнение требований по защите информации от утечки за счет побочных электромагнитных излучений и наводок	ПК-6
У.2	Проводить испытания (с использованием технических средств) с целью проверки защищенности информации от утечки за счет побочных электромагнитных излучений и наводок	ПК-6
У.3	Проводить оценку защищенности информации от утечки за счет побочных электромагнитных излучений и наводок	ПК-6
У.4	Рассчитывать показатели защищенности информации от утечки за счет побочных электромагнитных излучений и наводок	ПК-6
У.5	Оформлять протоколы оценки защищенности информации от утечки за счет побочных электромагнитных излучений и наводок	ПК-6
Зн.1	Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10

Зн.2	Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом высокочастотного облучения основных технических средств и систем и за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах	ПК-6
Зн.3	Способы и средства защиты информатизации от утечки за счет побочных электромагнитных излучений и наводок	ПК-6; ПК-8
Зн.4	Средства и методики контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок	ПК-4; ПК-6
Зн.5	Методики расчета показателей защищенности информации от утечки за счет побочных электромагнитных излучений и наводок	ПК-6; ПК-8
Зн.6	Отчетные документы, оформляемые по результатам контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок	ПК-6
Е/03.6	Проведение контроля защищенности акустической речевой информации от утечки по техническим каналам	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
ТД.1	Проверка состояния организации работ и выполнения требований по защите акустической речевой информации от утечки по техническим каналам	ПК-6
ТД.2	Испытания (с использованием технических средств) с целью проверки защищенности акустической речевой информации от утечки по техническим каналам	ПК-6
ТД.3	Подготовка отчетных материалов по результатам контроля защищенности акустической речевой информации от утечки по техническим каналам (протоколов оценки эффективности защиты акустической речевой информации от утечки по техническим каналам)	ПК-6
У.1	Разрабатывать методики контроля защищенности акустической речевой информации от утечки по техническим каналам	ПК-6
У.2	Проводить контроль защищенности акустической речевой информации от утечки по акустическим, вибрационным и акустооптическим каналам	ПК-6

У.3	Рассчитывать показатели защищенности акустической речевой информации	ПК-6
У.4	Проводить контроль подверженности технических средств акустоэлектрическим и акустоэлектромагнитным преобразованиям	ПК-6
У.5	Проводить оценку защищенности акустической речевой информации от утечки по техническим каналам	ПК-6
У.6	Оформлять протоколы оценки защищенности акустической речевой информации от утечки по техническим каналам	ПК-6
Зн.1	Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
Зн.2	Технические каналы утечки акустической речевой информации (прямые акустические, вибрационные, акустооптические, акустоэлектрические, акустоэлектромагнитные)	ПК-6
Зн.3	Возможности средств акустической речевой разведки	ПК-6
Зн.4	Технические каналы утечки акустической речевой информации, создаваемые за счет возможно внедренных специальных электронных устройств перехвата информации в технические средства и (или) предметы интерьера помещения	ПК-6
Зн.5	Основные характеристики специальных электронных устройств перехвата информации	ПК-6
Зн.6	Способы и средства защиты акустической речевой информации от утечки по техническим каналам	ПК-6
Зн.7	Средства и методики контроля защищенности информации от утечки по акустическим, вибрационным и акустооптическим каналам	ПК-6
Зн.8	Средства и методики контроля подверженности технических средств акустоэлектрическим и акустоэлектромагнитным преобразованиям	ПК-6
Зн.9	Отчетные документы, оформляемые по результатам контроля защищенности акустической речевой информации от утечки по техническим каналам	ПК-10
Е/04.6	Проведение контроля защищенности информации от несанкционированного доступа	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
ТД.1	Проверка состояния организации работ и выполнения требований по защите	ПК-6; ПК-7

	информации от несанкционированного доступа	
ТД.3	Подготовка отчетных материалов по результатам контроля защищенности информации от несанкционированного доступа и специальных воздействий	ПК-6; ПК-7
У.1	Проверять работоспособность средств защиты информации от несанкционированного доступа и специальных воздействий, выполнение правил их эксплуатации	ПК-6
У.2	Анализировать и оценивать технологический процесс обработки информации	ПК-6
У.3	Проводить оценку защищенности информации от несанкционированного доступа и специальных воздействий	ПК-10
У.4	Оформлять отчетные материалы по результатам контроля защищенности информации от несанкционированного доступа и специальных воздействий (протокол контроля защищенности информации от несанкционированного доступа и специальных воздействий)	ПК-6
Зн.1	Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
Зн.2	Способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах	ПК-10
Зн.3	Методы защиты информации от несанкционированного доступа и специальных программных воздействий на нее	ПК-5; ПК-10
Зн.4	Программные (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее	ПК-10
Зн.5	Средства и методики контроля защищенности информации от несанкционированного доступа и специальных программных воздействий	ПК-10
Зн.6	Отчетные документы, оформляемые по результатам контроля защищенности информации от несанкционированного доступа и специальных воздействий (протокол оценки защищенности информации от несанкционированного доступа и специальных воздействий)	ПК-10

Совокупность компетенций, установленных программой бакалавриата, обеспечивает выпускнику способность осуществлять профессиональную деятельность в области 06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере), и решать задачи профессиональной деятельности эксплуатационного, проектно-технологического, экспериментально-исследовательского и организационно-управленческого типа.

Планируемые результаты обучения в результате освоения основной профессиональной образовательной программы высшего образования по направлению подготовки 10.03.01 Информационная безопасность, направленность (профиль) образовательной программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)» показаны в приложении А. Матрица соответствия планируемых результатов освоения образовательной программы и составных частей основной профессиональной образовательной программы высшего образования по направлению подготовки 10.03.01 Информационная безопасность, направленность (профиль) образовательной программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)» приведена в приложении Б.

5 СТРУКТУРА И СОДЕРЖАНИЕ ОПОП

Содержание и организация образовательного процесса при реализации данной ОПОП по направлению подготовки 10.03.01 Информационная безопасность, направленность (профиль) образовательной программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)» регламентируется учебным планом; рабочими программами учебных дисциплин (модулей) и практик; материалами, обеспечивающими качество подготовки и воспитания обучающихся; годовым календарным учебным графиком, а также методическими материалами, обеспечивающими реализацию соответствующих образовательных технологий.

5.1 Объем обязательной части образовательной программы

Согласно требованиям пункта 2.9 ФГОС ВО объем обязательной части, без учета государственной итоговой аттестации, должен составлять не менее 60 процентов общего объема программы бакалавриата. Объем обязательной части, без учета государственной итоговой аттестации, составляет 63 процента общего объема программы бакалавриата, без учета объема государственной итоговой аттестации.

5.2 Типы практики

В Блок 2 «Практика» входят учебная и производственная практики (далее вместе – практики).

Типы учебной практики:

- Учебная практика: Ознакомительная практика
- Учебная практика: Учебно-лабораторная практика

Типы производственной практики:

- Производственная практика: Технологическая практика
- Производственная практика: Эксплуатационная практика
- Производственная практика: Преддипломная практика

5.3 Учебный план и календарный учебный график

5.3.1 Календарный учебный график

В календарном учебном графике указана последовательность реализации ОПОП направлению подготовки 10.03.01 Информационная безопасность,

направленность (профиль) образовательной программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)» по курсам включая теоретическое обучение, экзаменационные сессии, практики (учебная, производственная), подготовку к сдаче и сдача государственного экзамена, выполнение и защиту выпускной квалификационной работы, каникулы.

Основные параметры календарного учебного графика. Учебный год длится с 1 сентября по 31 августа (включая каникулы) и делится на два семестра.

Осенний семестр длится 24 недели (на пятом курсе 25), весенний семестр длится 28 недель (на пятом курсе 24), учебная практика (четвертый семестр 4 недели, шестой семестр – 4 недели, на ЗФО второй курс 4 недели, четвертый – 4 недели), производственная практика (седьмой и восьмой семестры), производственная практика: преддипломная практика (восьмой семестр ОФО, пятый курс ЗФО) – 2 недели, итоговая аттестация (восьмой семестр ОФО, пятый курс ЗФО) – 6 недель (Выполнение и защита выпускной квалификационной работы – 6 недель), каникулы – ОФО – 30 и 4/6 недели, ЗФО – 43 и 5/6 нед.

Трудоемкость учебного года на первом курсе – 60 з.е., на втором 64 з.е, на третьем 65 з.е., на четвертом 60 з.е. (для ЗФО 42 з.е., 42 з.е., 53 з.е., 46 з.е., 57 з.е.). График представлен в Приложении В.

5.3.2 Учебный план

Учебный план – документ, который определяет перечень, трудоемкость, последовательность и распределение по периодам обучения учебных предметов, курсов, дисциплин (модулей), практики, иных видов учебной деятельности и, если иное не установлено настоящим Федеральным законом, формы промежуточной аттестации обучающихся.

Учебный план разработан с учетом требований к условиям реализации образовательных программ, сформулированных в разделе VI ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, направленность (профиль) образовательной программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)».

В учебном плане указывается перечень дисциплин (модулей), практик, аттестационных испытаний государственной итоговой аттестации обучающихся, других видов учебной деятельности с указанием их объема в

зачетных единицах, последовательности и распределения по периодам обучения.

Зачетная единица эквивалентна 36 академическим часам (при продолжительности академического часа 45 минут).

В учебном плане выделяется объем работы обучающихся во взаимодействии с преподавателями (контактная работа обучающихся с преподавателем) (по видам учебных занятий) и самостоятельной работы обучающихся в академических часах.

Для каждой дисциплины (модуля) и практики указывается форма промежуточной аттестации обучающихся.

В учебном плане отображена логическая последовательность освоения дисциплин (модулей) и разделов ОПОП, обеспечивающих формирование необходимых компетенций, указана общая трудоемкость дисциплин (модулей), практик в зачетных единицах, а также их общая и аудиторная трудоемкость в часах.

Структура ОПОП направления подготовки 10.03.01 Информационная безопасность, направленность (профиль) образовательной программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)» включает обязательную часть (базовую) и часть, формируемую участниками образовательных отношений (вариативную).

Программа бакалавриата состоит из следующих блоков:

Блок 1 «Дисциплины (модули)», который включает дисциплины (модули), относящиеся к обязательной части программы, и дисциплины (модули), формируемые участниками образовательных отношений.

Блок 2 «Практика», который включает практики относящиеся к обязательной части программы, и практики, формируемые участниками образовательных отношений.

Блок 3 «Государственная итоговая аттестация», который завершается присвоением квалификации, указанной в перечне специальностей и направлений подготовки высшего образования, утверждаемом Министерством образования и науки Российской Федерации.

Структура ОПОП ВО по направлению подготовки 10.03.01 Информационная безопасность, направленность (профиль) образовательной программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)» представлена в таблице 9.

Таблица 9 – Распределение трудоемкости освоения ОПОП по направлению подготовки 10.03.01 Информационная безопасность, направленность (профиль) образовательной программы «Безопасность автоматизированных систем (по

отрасли или в сфере профессиональной деятельности)» (программа бакалавриата)

Структура программы бакалавриата		Объем программы бакалавриата в з.е. по учебному плану	
		ФГОС ВО (стандарт)	УП ОПОП ВО
Блок 1	Дисциплины (модули)	не менее 201	210
Блок 2	Практика	не менее 18	21
Блок 3	Государственная итоговая аттестация	6-9	9
Объем программы бакалавриата		240	240

К обязательной части программы бакалавриата относятся дисциплины (модули) и практики, обеспечивающие формирование общепрофессиональных компетенций, определяемых ФГОС ВО.

Дисциплины (модули) и практики, обеспечивающие формирование универсальных компетенций, определяемых ФГОС ВО, а также профессиональных компетенций, определяемых Организацией самостоятельно, могут включаться в обязательную часть программы бакалавриата и (или) в часть, формируемую участниками образовательных отношений.

Объем обязательной части, без учета объема государственной итоговой аттестации, должен составлять не менее 60 процентов общего объема программы бакалавриата.

В рамках обязательной части Блока 1 «Дисциплины (модули)» программы бакалавриата реализуются следующие дисциплины (модули):

Б1.О.01 История России

Б1.О.02 Иностранный язык

Б1.О.03 Философия

Б1.О.04 Безопасность жизнедеятельности

Б1.О.05 Информатика

Б1.О.06 Математический анализ

Б1.О.07 Физическая культура и спорт

Б1.О.08 Введение в направление подготовки и планирование профессиональной карьеры

Б1.О.09 Аналитическая геометрия

Б1.О.10 Основы российской государственности

Б1.О.11 Основы программирования

Б1.О.12 Линейная алгебра и функция нескольких переменных

Б1.О.13 Интегралы и дифференциальные уравнения

Б1.О.14 Дискретная математика

Б1.О.15 Теория вероятностей и математическая статистика

Б1.О.16 Физика

Б1.О.17 Основы информационной безопасности

Б1.О.18 Электротехника

Б1.О.19 Элементы алгебры и теории чисел

Б1.О.20 Структуры и алгоритмы обработки данных

Б1.О.21 Вычислительные методы

Б1.О.22 Электроника и схемотехника

Б1.О.23 Экономика

Б1.О.24 Основы военной подготовки

Б1.О.25 Теория информации

Б1.О.26 Аппаратные средства вычислительной техники

Б1.О.27 Методы и средства криптографической защиты информации

Б1.О.28 Экология

Б1.О.29 Интеллектуальные системы и технологии

Б1.О.30 Организационное и правовое обеспечение информационной безопасности

Б1.О.31 Сети и телекоммуникации

Б1.О.32 Метрология и электрорадиоизмерения

Б1.О.33 Безопасность систем баз данных

Б1.О.34 Администрирование сетей

Б1.О.35 Защита информации от утечки по техническим каналам

Б1.О.36 Безопасность операционных систем

Б1.О.37 Безопасность компьютерных сетей

Б1.О.38 Технологии программирования

Б1.О.39 Программно-аппаратные средства защиты информации

Б1.О.40 Основы управления информационной безопасностью

Б1.О.ДЭ.01.01 Физическая культура и спорт: общая физическая подготовка

Б1.В.01 Русский язык и культура речи

Б1.В.02 Право

Б1.В.03 Системы охраны и инженерной защиты информации

Б1.В.04 Защита информационных процессов в компьютерных системах

Б1.В.05 Методы защиты программного обеспечения

Б1.В.06 Проектирование защищенных автоматизированных систем

Б1.В.07 Порядок проведения аттестации объектов информатизации

Б1.В.08 Комплексная защита объектов информатизации

Б1.В.ДЭ.01.01 Социальные и этические вопросы в информационной сфере

Б1.В.ДЭ.02.01 Иностранный язык в профессиональной деятельности

Б1.В.ДЭ.03.01 Исследование операций

Б1.В.ДЭ.04.01 Специализированные вычислительные устройства защиты информации

Б1.В.ДЭ.05.01 Экономика защиты информации

Б1.В.ДЭ.06.01 Теория систем и системный анализ

Б1.В.ДЭ.07.01 Организация и управление службой защиты информации

Набор дисциплин (модулей) соответствующих профилю направленности становится обязательным для освоения обучающимся. Обучающимся обеспечивается возможность освоения дисциплин (модулей) по выбору, доля таких дисциплин составляет 25,5 % от объема части, формируемой участниками образовательных отношений Блока 1 «Дисциплины (модули)».

В Блок 2 Практика входят учебная и производственная практики (далее вместе – практики).

Типы учебной практики:

Б2.О.01(У) Учебная практика: Ознакомительная практика

Б2.О.02(У) Учебная практика: Учебно-лабораторная практика

Типы производственной практики:

Б2.О.03(П) Производственная практика: Технологическая практика

Б2.О.04(П) Производственная практика: Эксплуатационная практика

Б2.О.05(П) Производственная практика: Преддипломная практика

В Блок 3 «Государственная итоговая аттестация» входит:

Б3.01(Д) Выполнение и защита выпускной квалификационной работы

Обучающимся обеспечивается возможность освоения факультативных дисциплин, объем таких дисциплин составляет 9 з.е:

ФТД.01 Основы национальной безопасности

ФТД.02 Гуманитарные аспекты информационной безопасности

ФТД.03 История информационного противоборства

ФТД.04 Нейрокомпьютерные системы

Учебный план по направлению подготовки 10.03.01 Информационная безопасность, направленность (профиль) образовательной программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)» (программа бакалавриата) представлен в Приложении Г.

5.4 Рабочие программы учебных курсов, предметов, дисциплин (модулей) и практик

По каждой из дисциплин, включенных в учебный план, разработана рабочая программа.

Рабочая программа дисциплины (модуля) включает в себя:

- наименование дисциплины (модуля);
- перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы;
- указание места дисциплины (модуля) в структуре образовательной программы;
- объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся;
- содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий;
- перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю);
- контрольно-оценочные средства для проведения промежуточной аттестации обучающихся по дисциплине (модулю);
- перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);
- перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля);
- методические указания для обучающихся по освоению дисциплины (модуля);
- перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости);
- описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

В рабочей программе каждой дисциплины сформулированы конечные результаты обучения в органичной увязке с осваиваемыми знаниями, умениями и приобретаемыми компетенциями в целом по ОПОП с учетом направленности (профиля) программы «Безопасность автоматизированных систем (по отрасли

или в сфере профессиональной деятельности)». Разработка рабочих программ осуществляется в соответствии с локальными актами академии.

Рабочие программы всех учебных дисциплин (модулей) как базовой части, так и части, формируемой участниками образовательных отношений учебного плана, включая элективные дисциплины (по выбору), разработаны и хранятся на кафедрах-разработчиках и являются составной частью ОПОП направлению подготовки 10.03.01 Информационная безопасность, направленность (профиль) образовательной программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)».

Практика – вид учебной деятельности, направленной на формирование, закрепление, развитие практических навыков и компетенции в процессе выполнения определенных видов работ, связанных с будущей профессиональной деятельностью.

Программа практики включает в себя:

указание вида практики, способа (при наличии) и формы (форм) ее проведения;

перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы;

указание места практики в структуре образовательной программы;

указание объема практики в зачетных единицах и ее продолжительности в неделях либо в академических или астрономических часах;

содержание практики;

указание форм отчетности по практике;

фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике;

перечень учебной литературы и ресурсов сети «Интернет», необходимых для проведения практики;

перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости);

описание материально-технической базы, необходимой для проведения практики.

Краткое содержание рабочих программ дисциплин (модулей) и практик приведены в таблице 10.

Таблица 10 – Краткое содержание рабочих программ дисциплин (модулей) и практик

Индекс	Наименование и краткое содержание дисциплины (модулей) и практик	Компетенции	Объем, з.е.
Б1.О.01	История (история России, всеобщая история) Тема 1. Методология и теория исторической̆ науки. Россия в мировом историческом процессе Тема 2. Место средневековья во всемирно-историческом процессе. История России с древнейших времен до конца XVII века. Основные этапы становления российской̆ государственности Тема 3. Мировая история: переход к новому времени. XVIII век в западноевропейской̆ и российской̆ истории. Модернизация и просвещение. Особенности российской̆ модернизации Тема 4. Основные тенденции развития всемирной̆ истории в XIX веке. Российская империя в XIX столетии. Проблемы модернизации страны Тема 5. Место XX века во всемирно-историческом процессе. Россия в начале XX века. Революция или реформа? Тема 6. Социально-экономическое и политическое развитие страны в первое десятилетие советской̆ власти. Тема 7. Советское общество в 30-е годы Тема 8. Вторая мировая война и Великая Отечественная война советского народа. Послевоенный̆ мир 45 – 1953 гг Тема 9. Советское общество 50-х – 80-х годов. От первых попыток либерализации системы к глобальному кризису. Тема 10. От попыток перестройки системы к смене модели общественного развития. Современная Россия.	УК-5	4
Б1.О.02	Иностранный язык Английский язык – базовый уровень. Раздел 1. A Course of Business English Learning Раздел 2. Practice in Writing Business Letters Раздел 3. Communicate in English Раздел 4. Лексические основы чтения текстов по экономике Раздел 5. A Course of Basic English Revision Раздел 6. (выборочно) Раздел 7. Спецкурс “Programming” Английский язык – средний уровень. Раздел 1. Лексические основы чтения текстов по экономике Раздел 2. Грамматические основы чтения специального текста Раздел 3. Business Correspondence in English Раздел 4. English Business Communication Раздел 5. Taking Computer for granted Английский язык – продвинутый уровень Раздел 1. The language of small business, 1 часть Раздел 2. The language of small business, 2 часть Раздел 3. Грамматические основы чтения специального текста. Раздел 4. Business Correspondence in English Раздел 5. Business Vocabulary in Fiction Раздел 6. English Business Communication Раздел 7. Taking Computer for granted Немецкий язык Раздел 1. Лексические основы чтения текстов по экономике Раздел 2. Грамматические основы чтения специального текста	УК-4	12

	Раздел 3. Kommunikation in Deutsch Раздел 4. Deutsch. Business kursus Раздел 5. Деловая корреспонденция Раздел 6. Спецкурс Французский язык Раздел 1. Экономическая деятельность и общество Раздел 2. Микро и макроэкономика Раздел 3. Развитие навыков устной и письменной речи на базе темы № 16 Раздел 4. Рыночная экономика Раздел 5. Роль производства в экономике Раздел 6. Факторы производства Раздел 7. Спецкурс на французском языке		
Б1.О. 03	Философия Тема 1 Предмет философии и ее основной вопрос. Тема 2 Философия Древнего мира. Тема 3 Развитие философии от средневековья до Нового времени Тема 4 Немецкая классическая философия Тема 5 Основные направления современной. Тема 6 Русская философия и ее опыт в поиске смысла бытия Тема 7 Философское понимание мира: бытие и материя как исходные категории Тема 8 Проблема познание в философии Тема 9 Сознание, его происхождение и сущность Тема 10 Природа и общество Тема 11 Основы социальной философии Тема 12 Философии истории Тема 13 Культура и цивилизация Тема 14 Философское учение о личности. Общественный прогресс и глобальные проблемы современности.	УК-5	3
Б1.О. 04	Безопасность жизнедеятельности Тема 1. Основные положения и принципы обеспечения безопасности Тема 2.Безопасность жизнедеятельности и окружающая природная среда Тема 3. БЖ и производственная среда Тема 4. Психологические основы безопасности Тема 5. Основы здорового образа жизни Тема 6. ЧС классификация и причины возникновения Тема 7. Чрезвычайные ситуации техногенного характера Тема 8. Первая помощь пострадавшим в условиях чрезвычайных ситуаций	УК-8	3
Б1.О. 05	Информатика Раздел I. Программные средства компьютерной обработки информации Тема 1. Введение. Понятие информации. Тема 2. Современные операционные среды компьютерной обработки информации. Тема 3. Основные виды и устройства обработки данных. Тема 4. Обработка текстовых файлов. Тема 5. Структурный анализ регулярных выражений. Раздел II. Основные алгоритмы обработки информации Тема 1. Базовые алгоритмы сортировки данных. Тема 2. Сортировки с помощью обмена. Улучшение прямых методов сортировок. Тема 3. Метод Шелла. Сортировки методом слияния. Тема 4. Поразрядная сортировка. Хеширование. Тема 5. Метод быстрой сортировки. Тема .6. Базовые методы поиска. Раздел III. Системы счисления и кодирование информации Тема 1. Основные понятия и виды систем счисления. Тема 2. Смешанные системы счисления. Тема 3. Перевод записей целых и вещественных чисел между системами счисления. Тема 4. Алгоритм перевода периодической десятичной дроби в р-ичную. Тема 5. Двоичная	ОПК-2	4

	арифметика. Кодирование символьной информации.		
Б1.О. 06	Математический анализ Тема 1. Введение в математический анализ. Тема 2. Дифференциальное исчисление функций одной переменной. Тема 3. Интегральное исчисление функций одной переменной. Тема 4. Определенный интеграл и его приложение. Тема 5. Числовые и функциональные ряды. Тема 6. Дифференциальное исчисление функций многих переменных. Тема 7.Интегральное исчисление функций многих переменных. Тема 8. Элементы теории функций комплексной переменной.	ОПК-3	5
Б1.О. 07	Физическая культура и спорт Раздел I. Теоретический раздел Тема 1. Физическая культура в общекультурной и профессиональной подготовке студентов. Тема 2. Биологические основы физической культуры Тема 3. Физическая подготовка в системе физического воспитания Тема 4. Врачебный контроль и самоконтроль занимающихся физической культурой и спортом. Тема 5. Основы здорового образа жизни. Физическая культура в обеспечении здоровья. Тема 6. Основы методики самостоятельных занятий физическими упражнениями. Тема 7. Профессионально-прикладная физическая подготовка. Раздел II. Практический раздел Тема 8.1. Общая и специальная физическая подготовка (ОФП). Тема 8.2 Общая и специальная физическая подготовка (ОФП). Тема 8.3. Общая и специальная физическая подготовка (ОФП).	УК-7	2
Б1.О. 08	Введение в направление подготовки и планирование профессиональной карьеры Тема 1. Введение. Основы информационной безопасности. Тема 2. Основные понятия и определения в области деятельности «информационная безопасность». Тема 3. Комплексность реализациями системы обеспечения защиты информации в Российской Федерации. Тема 4. Особенности работы специалиста в области технической средства защиты информации. Тема 5. Роль специалиста в области информационной безопасности. Тема 6. Стратегия и практика развития компетенций. Тема 7. Введение в планирование карьеры. Тема 8. Модели успешного профессионального поведения. Тема 9. Технология целеполагания.	УК-6; УК-10	3
Б1.О. 09	Аналитическая геометрия Тема 1. Математический анализ. Функции многих переменных. Тема 2. Математический анализ. Функция одной переменной. Тема 3. Элементы линейной алгебры и аналитической геометрии.	ОПК-3	4
Б1.О. 10	Основы российской государственности Тема 1. Россия: цифры и факты Тема 2. Россия: испытания и герои Тема 3. Цивилизационный подход: возможности и ограничения. Тема 4. Философское осмысление России как цивилизации. Тема 5. Мировоззрение и идентичность. Тема 6. Мировоззренческие принципы (константы) российской цивилизации. Тема 7. Конституционные принципы и разделение властей Тема 8. Стратегическое планирование: национальные	УК-5	2

	проекты и государственные программы Тема 9. Актуальные вызовы и проблемы развития России Тема 10. Сценарии развития российской цивилизации		
Б1.О.11	Основы программирования Тема 1. Введение в программирование. Тема 2. Структуры данных. Тема 3. Модульное программирование. Тема 4. Конструирование и верификация программ.	ОПК-7	6
Б1.О.12	Линейная алгебра и функция нескольких переменных Тема 1. Комплексные числа и многочлены. Тема 2. Элементы матричного анализа. Тема 3. Линейная алгебра и функции нескольких переменных. Системы линейных уравнений. Тема 4. Элементы векторной алгебры.	ОПК-3	4
Б1.О.13	Интегралы и дифференциальные уравнения Тема 1. Определение и свойства определенного интеграла. Тема 2. Несобственные интегралы первого и второго рода. Тема 3. Кратные интегралы. Криволинейные интегралы первого и второго рода. Тема 4. Дифференциальные уравнения. Тема 5. Системы дифференциальных уравнений.	ОПК-3	4
Б1.О.14	Дискретная математика Раздел 1. Элементы теории множеств. Раздел 2. Основные понятия комбинаторики и ее конфигурации. Раздел 3. Элементы теории графов и сетей. Раздел 4. Переключательные функции.	ОПК-3	3
Б1.О.15	Теория вероятностей и математическая статистика Тема 1. Случайные события. Тема 2. Случайные величины. Тема 3. Статистическое оценивание Тема 4. Проверка статистических гипотез Тема 5. Дисперсионный анализ Тема 6. Корреляционный анализ Тема 7. Регрессионный анализ (двумерная модель)	ОПК-3	3
Б1.О.16	Физика Тема 1. Основы механики и молекулярной физики. Тема 2. Термодинамика и электричество. Тема 3. Магнитные волны. Тема 4. Элементы квантовой физики.	ОПК-4; ОПК-11	8
Б1.О.17	Основы информационной безопасности Тема 1. Введение. Базовые понятия. Тема 2. Конфиденциальность. Классификация угроз. Тема 3. Угрозы информационной безопасности. Классы нарушителей. Оценка риска. Тема 4. Персональные данные. Защита авторских прав. Тема 5. Выявление контрафактной продукции. Тема 6. Криптографические методы защиты.	УК-1; ОПК-1; ОПК-9	2
Б1.О.18	Электротехника Тема 1. Введение. Основные определения, законы и методы расчета электрических цепей. Тема 2. Линейные цепи синусоидального тока. Тема 3. Передаточная функция и частотные характеристики линейных электрических цепей. Тема 4. Основы теории четырехполюсников и электрических фильтров. Тема 5. Переходные процессы в линейных электрических цепях. Тема 6. Электрические цепи с нелинейными элементами и магнитные цепи.	ОПК-4	4
Б1.О.19	Элементы алгебры и теории чисел Тема 1. Теорема деления с остатком. Делимость и её свойства. Простые числа. Тема 2. Каноническое представление целых	ОПК-3	2

	чисел. НОД. Тема 3. Взаимно простые числа и их свойства. НОК. Свойства НОК, НОД. Тема 4. Сравнения и их свойства. Системы сравнений первой степени. Тема 5. Сравнения второй степени. Непрерывные дроби. Тема 6. Группы, кольца, поля. Их свойства. Тема 7. Элементы теории многочленов. Тема 8. Эллиптические кривые над полем. Точки эллиптической кривой и их свойства. Тема 9. Эллиптические кривые над конечными полями. Действия над точками эллиптической кривой.		
Б1.О. 20	Структуры и алгоритмы обработки данных Раздел 1. Структуры данных. Раздел 2. Алгоритмы.	ОПК-3; ОПК-7	4
Б1.О. 21	Вычислительные методы Тема 1. Основы теории погрешностей. Тема 2. Методы решения систем линейных уравнений. Тема 3. Численные методы решения нелинейных уравнений. Тема 4. Математическая обработка результатов эксперимента. Интерполяция и аппроксимация функций. Тема 5. Численное интегрирование. Тема 6. Приближенное решение дифференциальных уравнений. Тема 7. Методы численной оптимизации.	ОПК-3	3
Б1.О. 22	Электроника и схемотехника Тема 1. Введение. Общие сведения об элементной базе электронной техники. Тема 2. Полупроводники и электронно-дырочный переход. Тема 3. Биполярные транзисторы. Тема 4. Полевые транзисторы. Тема 5. Оптоэлектронные устройства. Тема 6. Полупроводниковые элементы интегральных микросхем.	ОПК-4	4
Б1.О. 23	Экономика Раздел 1. Микроэкономика. Раздел 2. Макроэкономика.	УК-2; УК-9	4
Б1.О. 24	Основы военной подготовки Тема 1. Общевоинские уставы Вооруженных Сил Российской Федерации, их основные требования и содержание. Тема 2. Внутренний порядок и суточный наряд. Тема 3. Общие положения Устава гарнизонной и караульной службы Тема 4. Строевые приемы и движение без оружия Тема 5. Основы, приемы и правила стрельбы из стрелкового оружия. Тема 6. Назначение, боевые свойства, материальная часть и применение стрелкового оружия, ручных противотанковых гранатометов и ручных гранат Тема 7. Выполнение упражнений учебных стрельб из стрелкового оружия Тема 8. Вооруженные Силы Российской Федерации их состав и задачи. Тактико-технические характеристики (ТТХ) основных образцов вооружения и техники ВС РФ. Тема 9. Основы общевойскового боя. Тема 10.Основы инженерного обеспечения. Тема 11. Организация воинских частей и подразделений, вооружение, боевая техника вероятного противника Тема 12. Ядерное, химическое, биологическое, зажигательное оружие. Тема 13. Радиационная, химическая и биологическая защита Тема 14. Местность как элемент боевой обстановки. Измерения и ориентирование на местности без карты, движение по азимутам. Тема 15. Медицинское обеспечение войск (сил), первая медицинская помощь при ранениях, травмах и особых случаях.	УК-8	3

Б1.О.25	Теория информации Тема 1. Введение. Задачи и постулаты прикладной теории информации. Тема 2. Вопросы измерения информации в сетях электросвязи. Тема 3. Дискретизация и квантования сигналов в сетях электросвязи. Тема 4. Кодирование информации в сетях электросвязи. Тема 5. Основы передачи информации в сетях электросвязи.	ОПК-3	3
Б1.О.26	Аппаратные средства вычислительной техники Тема 1. Введение в дисциплину. Математические основы вычислительной техники. Тема 2. Принципы построения вычислительной техники. Тема 3. Функциональная и структурная организация вычислительной техники. Тема 4. Основы микропроцессорной техники.	ОПК-2	5
Б1.О.27	Методы и средства криптографической защиты информации Тема 1. Введение в криптологию. Тема 2. Классификация криптоалгоритмов. Тема 3. Потоковые шифраторы. Тема 4. Блочные криптоалгоритмы. Тема 5. Ассиметричные криптоалгоритмы. Тема 6. Алгоритмы обмена ключами. Тема 7. Применение программных систем шифрования. Тема 8. Стеганография. Тема 9. Криптоанализ и криптостойкость.	ОПК-9	3
Б1.О.28	Экология Тема 1. Введение. Тема 2. Человек и биосфера. Основы учения о биосфере и ее эволюции. Тема 3. Экосистемы. Тема 4. Сообщества и популяции. Тема 5. Организм и среда. Тема 6. Глобальные экологические проблемы современности. Тема 7. Загрязнение атмосферы, гидросферы, литосферы. Тема 8. Рациональное природопользование и охрана окружающей среды. Тема 9. Социально-экономические аспекты экологии.	УК-8	2
Б1.О.29	Интеллектуальные системы и технологии Раздел 1. Новые информационные технологии. Раздел 2. Понятие интеллектуальной информационной системы. Раздел 3. Тенденции развития интеллектуальных информационных систем.	УК-1; ОПК-1	3
Б1.О.30	Организационное и правовое обеспечение информационной безопасности Тема 1. Информационная безопасность в системе национальной безопасности России. Тема 2. Информация, информационные системы как объект правового регулирования информационной безопасности. Тема 3. Правовая основа допуска и доступа персонала к защищаемым сведениям. Тема 4. Правовые проблемы, связанные с защитой прав обладателей собственности на информацию и распоряжением информацией. Тема 5. Правовые основы защиты коммерческой тайны. Тема 6. Компьютерная информация – как объект информатизации. Тема 7. Лицензирование в области защиты информации. Тема 8. Сертификация в области защиты информации. Тема 9. Система правовой ответственности за утечку информации и утрату носителей информации. Тема 10. Правовые основы деятельности подразделений защиты информации. Тема 11. Правовые основы защиты личной тайны.	УК-10; ОПК-5; ОПК-6; ОПК-8; ОПК-4.1	2

	Тема 12. Правовые основы защиты персональных данных.		
Б1.О.31	Сети и телекоммуникации Раздел 1. Сравнение параметров кабельных и беспроводных сетей. Раздел 2. Функции сетевого и транспортного уровней. Раздел 3. Прикладной уровень.	УК-1; ОПК-2; ОПК-9	5
Б1.О.32	Метрология и электрорадиоизмерения Тема 1. История метрологии, основные понятия, системы единиц физических величин. Тема 2. Основы теории погрешностей. Тема 3. Метрологические характеристики средств измерений. Тема 4. Технические измерения. Тема 5. Проверка и аттестация средств измерений. Тема 6. Метрологическое обеспечение производства.	ОПК-4; ОПК-11	4
Б1.О.33	Безопасность систем баз данных Тема 1. Понятия и определения реляционной модели. Тема 2. Проектирование реляционных баз данных. Тема 3. Манипулирование реляционными базами данных. Реляционная алгебра. Тема 4. Клиент-серверная архитектура современных реляционных СУБД и АИС. Тема 5. Понятие безопасности БД. Угрозы безопасности БД. Тема 6. Меры защиты БД и СУБД. Тема 7. Методы и механизмы обеспечения целостности информации в реляционных базах данных. Тема 8. Обработка транзакций. Тема 9. Управление параллельностью работы транзакций. Тема 10. Реализация ограничений в базах данных. Тема 11. Методы и механизмы обеспечения конфиденциальности информации в системах баз данных. Тема 12. Использование криптографических методов защиты информации в системах баз данных. Тема 13. Защита баз данных от «внедрения в SQL». Тема 14. Методы и механизмы обеспечения доступности баз данных и СУБД. Тема 15. Резервирование серверов СУБД. Тема 16. Верификация баз данных и проведение аудита в СУБД. Тема 17. Мониторинг активности пользователей на уровне СУБД. Тема 18. Распределенные базы данных	УК-1; УК-3; ОПК-4.2	5
Б1.О.34	Администрирование сетей Тема 1. Принципы администрирование сетей. Тема 2. Администрирование пользователей. Тема 3. Сетевые службы. Тема 4. Администрирование сетей на основе Astra Linux SE.	ОПК-4.2	3
Б1.О.35	Защита информации от утечки по техническим каналам Тема 1. Технические средства разведки. Общие сведения. Тема 2. Радиоэлектронная разведка. Тема 3. Оптическая разведка. Тема 4. Акустическая разведка. Тема 5. Компьютерная разведка. Тема 6. Средства технической разведки. Тема 7. Противодействие техническим разведкам. Тема 8. Радиоэлектронное противодействие и радиомаскировка. Тема 9. Противодействие акустической разведке. Тема 10. Противодействие видовой разведке. Тема 11. Защита от внедряемых на объекты разведывательных устройств. Тема 12. Технические средства защиты информации.	ОПК-9; ОПК-12	4
Б1.О.36	Безопасность операционных систем Тема 1. Организация сетей на базе Microsoft Windows Server.	ОПК-4.2	7

	Тема 2. Управление объектами службы каталогов Active Directory. Тема 3. Архитектура и режимы функционирования средств защиты информации Astra Linux Special Edition. Тема 4. Дискреционное и мандатное управление доступом в Astra Linux Special Edition. Тема 5 Аудит в Astra Linux Special Edition. Тема 6. Red Book: настройка безопасной конфигурации для Astra Linux Special Edition 1.7.		
Б1.О.37	Безопасность компьютерных сетей Тема 1. Типы сетевых атак. Механизмы и методы проведения сетевых атак в стеке протоколов TCP/IP. Обзор методов защиты. Тема 2. Обеспечение безопасности уровня сетевого доступа. Тема 3. Ограничение маршрутной информации, фильтрация трафика ICMP, ARP Spoofing, DHCP Spoofing, фрагментация. Тема 4. Перехват и сбор трафика. Тема 5. Межсетевые экраны.	ОПК-9; ОПК-10; ОПК-4.4	3
Б1.О.38	Технологии программирования Раздел 1 Программное обеспечение Раздел 2 Структурное программирование Раздел 3 Объектно-ориентированное программирование Раздел 4 Компонентно-ориентированное программирование	УК-1; ОПК-7	6
Б1.О.39	Программно-аппаратные средства защиты информации Тема 1. Введение. Основные понятия. Требования руководящих документов по защите информации. Тема 2. Модели разграничения доступа. Тема 3. Идентификация и аутентификация пользователей. Тема 4. Программно-аппаратные средства шифрования. Тема 5. Электронная подпись.	ОПК-10; ОПК-12; ОПК-4.1; ОПК-4.3	4
Б1.О.40	Основы управления информационной безопасностью Тема 1. Основные понятия информационной безопасности. Тема 2. Угрозы информационной безопасности в информационных системах. Тема 3. Оценочные стандарты в информационной безопасности. Тема 4. Стандарты управления информационной безопасностью. Тема 5. Создание СУИБ на предприятии. Тема 6. Методики и технологии управления рисками. Тема 7. Разработка корпоративной методики анализа рисков. Тема 8. Современные методы и средства анализа и управление рисками информационных систем компаний. Тема 9. Правовые меры обеспечения информационной безопасности	ОПК-1; ОПК-5; ОПК-6; ОПК-12; ОПК-4.1	2
Б1.О.ДЭ.01.01	Физическая культура и спорт: общая физическая подготовка Гимнастика Легкая атлетика Спортивные игры Общая физическая подготовка (ОФП) – юноши Прикладные виды аэробики – девушки	УК-7	
Б1.В.01	Русский язык и культура речи Раздел 1. Язык как средство общения (коммуникативный аспект изучения). Лексическая стилистика. Раздел 2. Фразеологическая стилистика. Стилистика словообразования. Раздел 3. Стилистика частей речи Раздел 4. Синтаксическая стилистика Раздел 5. Культура и техника речи. Риторика и культура речи.	УК-4	3

Б1.В.02	Право Тема 1 Государство и право, их роль в жизни общества Правоотношение. Норма права, источники права, система права Тема 2 Права и свободы человека и гражданина Конституция Российской Федерации – основной закон государства Особенности федеративного устройства Система органов государственной власти РФ Тема 3 Понятие гражданского правоотношения его структура. Субъекты гражданских правоотношений. Понятие права собственности и его защита. Общие положения о договорах Наследственное право. Тема 4 Трудовой договор: порядок заключения, основания прекращения Правовое регулирование трудовых отношений Тема 5 Семейное право Основы семейного права. Тема 6 Основы административной ответственности. Основы уголовной ответственности	УК-10	3
Б1.В.03	Системы охраны и инженерной защиты информации Тема 1. Введение. Задачи дисциплины «Системы охраны и инженерной защиты информации». Тема 2. Угрозы информационной безопасности информации и объекты защиты. Тема 3. Демаскирующие признаки объектов защиты. Классификация демаскирующих признаков. Тема 4. Источники и носители информации. Тема 5. Принципы и способы добывания информации. Тема 6. Основы противодействия техническим средствам разведки. Тема 7. Технические каналы утечки информации (электромагнитные каналы, электрические каналы, параметрические каналы, вибрационные каналы). Тема 8. Каналы утечки речевой информации. Тема 9. Каналы утечки информации при передаче по каналам связи. Тема 10. Технические каналы утечки видовой информации. Тема 11. Несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники. Тема 12. Звукоизоляция помещений.	УК-3; ПК-2; ПК-9; ПК-10	4
Б1.В.04	Защита информационных процессов в компьютерных системах Тема 1. Введение в дисциплину. Характеристика информационных систем и информационных процессов. Тема 2. Основы принципы защиты информационных процессов в компьютерных системах. Тема 3. Стандарты по защите информации и информационных процессов. Тема 4. Организация и средства защиты информационных процессов в компьютерных системах.	ПК-1; ПК-2	4
Б1.В.05	Методы защиты программного обеспечения Тема 1. Защита программного обеспечения. Тема 2. Методы защиты от исследования программ. Тема 3. Организационно-технические принципы защиты. Тема 4. Методы и средства защиты программ от компьютерных вирусов. Тема 5. Методы защиты программного обеспечения от внедрения на этапе его эксплуатации и сопровождения программных закладок. Тема 6. Методы и средства обеспечения целостности и достоверности используемого программного кода. Тема 7. Основные подходы к защите программ от несанкционированного копирования.	УК-3; ПК-4; ПК-5; ПК-7	5

Б1.В.06	Проектирование защищенных автоматизированных систем Тема 1. Понятие автоматизированной системы (АС). Тема 2. Основные аспекты построения системы информационной безопасности. Тема 3. Мероприятия по защите информации. Тема 4. Требования к архитектуре АС для обеспечения безопасности ее функционирования. Тема 5. Оценочные стандарты и технические спецификации. Тема 6. Критерии оценки безопасности информационных технологий. Тема 7. Требования руководящих документов ФСТЭК России к АС. Тема 8. Описание информационной системы и особенностей ее функционирования. Тема 9. Перечень потенциальных источников атак и определение их возможностей (модель нарушителя). Тема 10. Определение уровня защищенности данных в АС. Тема 11. Описание угроз безопасности информации (модель угроз безопасности информации). Тема 12. Методы выбора системы защиты информации.	ПК-3; ПК-4	6
Б1.В.07	Порядок проведения аттестации объектов информатизации Тема 1. Введение. Основные понятия в области технической защиты информации. Тема 2. Концептуальные основы защиты информации. Система документов по технической защите информации. Тема 3. Органы по технической защите информации в РФ. Тема 4. Лицензирование деятельности в области ТЗИ. Тема 5. Объект информатизации. Классификация объектов защиты. Тема 6. Общий порядок сертификации средств защиты информации. Тема 7. Порядок сертификации во ФСТЭК России. Тема 8. Аттестация объекта информатизации по требованиям безопасности информации. Тема 9. Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники.	ПК-6	4
Б1.В.08	Комплексная защита объектов информатизации Тема 1. Теория информационной безопасности и методология защиты информации. Тема 2. Правовое обеспечение информационной безопасности. Тема 3. Защита и обработка конфиденциальных документов. Тема 4. Организационное обеспечение информационной безопасности. Тема 5. Инженерно-техническая защита информации. Тема 6. Инженерно-техническая защита информации. Тема 7. Криптографические методы и средства обеспечения информационной безопасности. Тема 8. Программно-аппаратная зашита информации и защита информационных процессов в компьютерных системах. Тема 9. Комплексная зашита информации на предприятии.	ПК-5; ПК-7; ПК-8; ПК-10	5
Б1.В.ДЭ.01.01	Социальные и этические вопросы в информационной сфере Раздел 1 Вопросы развития информационных технологий во взаимосвязи с этическими проблемами, нормами и социальными процессами. Раздел 2 Этические проблемы формирования глобального информационного пространства.	УК-5	2
Б1.В.ДЭ.02.01	Иностранный язык в профессиональной деятельности Раздел 1. Лингвистический материал Раздел 2. Социокультурные и профессиональные знания Раздел 3. Сферы делового общения и грамматическая тематика	УК-4	3

Б1.В.ДЭ.03.01	Исследование операций Раздел 1. Введение. Общая характеристика и особенности исследования операций. Раздел 2. Линейные оптимизационные модели и линейное программирование. Раздел 3. Нелинейное программирование. Раздел 4. Дискретное программирование и линейные целочисленные модели. Раздел 5. Динамическое программирование.	УК-1	3
Б1.В.ДЭ.04.01	Специализированные вычислительные устройства защиты информации Тема 1. Стандарты безопасности. Тема 2. Защищенная автоматизированная система. Тема 3. Защита информации на машинных носителях. Тема 4. Криптографические средства защиты информации. Тема 5. Защита информации в электронных платежных системах.	ПК-1	3
Б1.В.ДЭ.05.01	Экономика защиты информации Тема 1. Введение. Основные понятия и содержание дисциплины «Экономика защиты информации». Тема 2. Экономические проблемы информационных ресурсов и защиты информации. Тема 3. Экономика информации, неопределенности и риска. Тема 4. Ценообразование на информационные продукты и услуги. Себестоимость информационных продуктов и услуг. Тема 5. Экономическая безопасность фирмы. Тема 6. Оценка эффективности создания и функционирования системы защиты информации. Страхование, как способ и метод защиты вложений.	ПК-9; ПК-10	2
Б1.В.ДЭ.06.01	Теория систем и системный анализ Тема 1. Цели и закономерности целеобразования. Тема 2. Измерения и шкалы. Тема 3. Модели и моделирование. Тема 4. Понятие системы. Тема 5. Конструктивные свойства систем. Тема 6. Функциональные свойства систем. Тема 7. Системы в организации. Тема 8. Классификация систем. Тема 9. Системы управления. Тема 10. Методы формализованного представления систем. Тема 11. Методы неформализованного представления систем. Тема 12. Методики системного анализа.	УК-1	3
Б1.В.ДЭ.07.01	Организация и управление службой защиты информации Тема 1. Структура службы информационной безопасности. Тема 2. Функции основных групп службы безопасности. Тема 3.Цели и задачи службы информационной безопасности. Тема 4. Организационные основы и принципы деятельности службы информационной безопасности. Тема 5. Лицензирование видов деятельности службы безопасности. Тема 6. Управление службой защиты информации. Тема 7. Организация информационно-аналитической работы. Тема 8. Организация работы с персоналом предприятия.	ПК-9	3
Б2.О.01(У)	Учебная практика: Ознакомительная практика Цели: 1. закрепление, расширение, углубление и систематизация знаний, полученных при изучении обязательных дисциплин базовой части учебного плана; 2. подготовка к выполнению самостоятельных и курсовых работ	ОПК-2; ОПК-8; ОПК-4.2; ОПК-4.4	6

	в последующих семестрах; 3. обеспечение возможности применения студентами теоретических знаний для решения практических задач; 4. развитие организаторских способностей студентов; 5. формирование и развитие практических навыков в профессиональной сфере использования технологий и технических средств, применяемых в области информационной безопасности; 6. развитие у обучающихся компетенций, а также формирования опыта самостоятельной исследовательской и аналитической деятельности в изучении практического материала; 7. формирование общего представления студентов о будущей профессиональной деятельности и развитие интереса к профессии. Задачи: 1. формирование общепрофессиональных компетенций, установленных ФГОС ВО и закрепленных учебным планом за учебной ознакомительной практикой; 2. освоение современных технологий и технических средств, применяемых в области информационной безопасности; 3. совершенствование навыков подготовки, представления и защиты информационных, проектных, аналитических, руководящих и отчетных документов по результатам профессиональной деятельности и практики.		
Б2.О. 02(У)	Учебная практика: Учебно-лабораторная практика Цели: 1. Получение профессиональных умений и опыта профессиональной деятельности в области проектирования и реализации технологий информационной безопасности. Задачи: 1. Формирование общепрофессиональных компетенций, установленных ФГОС ВО и закрепленных учебным планом за учебной практикой (учебно-лабораторным практикумом). 2. Освоение современных технологий и технических средств, применяемых в области информационной безопасности. 3. Совершенствование навыков подготовки, представления и защиты информационных, проектных, аналитических, руководящих и отчетных документов по результатам профессиональной деятельности и практики. 4. Развитие исполнительских и лидерских навыков обучающихся.	ОПК-3; ОПК-4; ОПК-7; ОПК-9; ОПК-11	6
Б2.О. 03(П)	Производственная практика: Технологическая практика Цели: 1. Получение профессиональных умений и опыта профессиональной деятельности в области реализации технологий информационной безопасности. Задачи: 1. Формирование профессиональных компетенций, установленных ФГОС ВО и закрепленных учебным планом за производственной проектно-технологической практикой. 2. Освоение современных технологий и технических средств, применяемых в области информационной безопасности.	ОПК-6; ОПК-9; ОПК-10; ОПК-12; ОПК-4.1; ОПК-4.3; ПК-1; ПК-2; ПК-3; ПК-6	3

	3. Совершенствование навыков подготовки, представления и защиты информационных, проектных, аналитических, руководящих и отчетных документов по результатам профессиональной деятельности и практики. 4. Развитие исполнительских и лидерских навыков обучающихся.		
Б2.О. 04(П)	Производственная практика: Эксплуатационная практика Цели: 1. Получение профессиональных умений и опыта профессиональной деятельности в области проектирования и реализации технологий информационной безопасности. Задачи: 1. Формирование общепрофессиональных компетенций, установленных ФГОС ВО и закрепленных учебным планом за производственной эксплуатационной практикой. 2. Освоение современных технологий и технических средств, применяемых в области информационной безопасности. 3. Совершенствование навыков подготовки, представления и защиты информационных, проектных, аналитических, руководящих и отчетных документов по результатам профессиональной деятельности и практики. 4. Развитие исполнительских и лидерских навыков обучающихся.	ОПК-1; ОПК-5; ОПК-6; ОПК-9; ОПК-10; ОПК-12; ОПК-4.1; ОПК-4.3	3
Б2.О. 05(П)	Производственная практика: Преддипломная практика Цели: 1. Получение профессиональных умений и опыта профессиональной деятельности в области проектирования и реализации технологий информационной безопасности. Задачи: 1. Формирование общепрофессиональных компетенций, установленных ФГОС ВО и закрепленных учебным планом за производственной эксплуатационной практикой. 2. Освоение современных технологий и технических средств, применяемых в области информационной безопасности. 3. Совершенствование навыков подготовки, представления и защиты информационных, проектных, аналитических, руководящих и отчетных документов по результатам профессиональной деятельности и практики. 4. Развитие исполнительских и лидерских навыков обучающихся.	УК-1; ОПК-2; ОПК-3; ОПК-4; ОПК-5; ОПК-6; ОПК-8; ОПК-9; ОПК-10; ОПК-12; ОПК-4.1; ОПК-4.2; ОПК-4.3; ОПК-4.4; ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10	3
Б3.01 (Д)	Выполнение и защита выпускной квалификационной работы Включает в себя требования к выпускной квалификационной	УК-1; УК-2;	9

	работе и порядку их выполнения, критерии оценки защиты выпускной квалификационной работы.	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; ОПК-4.1; ОПК-4.2; ОПК-4.3; ОПК-4.4; ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10	
ФТД.01	Основы национальной безопасности Раздел 1. Теоретико-методологические основы национальной безопасности Раздел 2. Организационно-правовые основы обеспечения безопасности (национальной безопасности)	УК-1; УК-2; УК-10	2
ФТД.02	Гуманитарные аспекты информационной безопасности Тема 1. Доктрина информационной безопасности Российской Федерации. Тема 2. Безопасность личности, общества и государства: дифференциация и взаимосвязь уровней информационной безопасности. Тема 3. Объективные и субъективные аспекты информационной безопасности в условиях социальной турбулентности. Тема 4. Экзистенциально-личностное измерение безопасности и информационная безопасность личности, духовная	УК-5; УК-6	3

	безопасность личности. Тема 5. Цивилизационные аспекты национально-информационной безопасности. Тема 6. Виртуальные девиантные сообщества и деструктивный контент социальных сетей		
ФТД.03	История информационного противоборства Тема 1. История возникновения органов защиты информации. Тема 2. Защита государственных интересов в XII – XVI вв. Тема 3. Защита государственных интересов в XVI – XVIII вв. Тема 4. Защита государственных интересов в XIX веке. Тема 5. Защита государственных интересов в 1900-1917 гг. Тема 6. Защита государственных интересов в период создания Советской власти, НЭПа и 1928 – 1941 годах. Тема 7. Защита государственных интересов в период великой отечественной войны. Тема 8. Система безопасности СССР и России в XX – XXI веках.	УК-5	2
ФТД.04	Нейрокомпьютерные системы Раздел 1. Основные понятия ИНС. Модели искусственных нейронов и методы их обучения. Раздел 2. Типы искусственных нейронных сетей. Раздел 3. Перспективы развития и применения ИНС и нейрокомпьютерных систем.	УК-1	2

Копии рабочих программ дисциплин (модулей) и практик представлены в Приложении Д.

5.5 Фонды оценочных средств для промежуточной аттестации по дисциплинам (модулям) и практикам

Разработаны фонды оценочных средств, с помощью которых проводится оценка сформированности всех без исключения компетенций, перечисленных в образовательной программе, на этапе промежуточной аттестации. Такими оценочными средствами являются тесты, экзаменационные вопросы и вопросы для зачета, всевозможные задачи, задания, кейсы и прочие средства, соотнесенные с компетенциями, перечисленными в образовательной программе, через индикаторы (показатели) достижения компетенций.

Рекомендуемая структура оценочного средства:

1 Паспорт оценочных средств

2 Оценочные средства для проведения текущего контроля обучающихся

3 Спецификация оценочного средства

4 Оценочные средства для проведения промежуточной аттестации обучающихся

5 Демонстрационный вариант по дисциплине

6 Эталон ответов на Демонстрационный вариант оценочного средства по

дисциплине

Фонд оценочных средств для проведения промежуточной аттестации по дисциплинам (модулям) и практикам учебного плана по направлению 10.03.01 Информационная безопасность, направленность (профиль) программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)» приведены в приложении Е.

5.6 Программы итоговой аттестации

Государственная итоговая аттестация, завершающая освоение основной профессиональной образовательной программы высшего образования (программы бакалавриата), является итоговой аттестацией обучающихся по программе бакалавриата.

Государственная итоговая аттестация проводится государственными экзаменационными комиссиями в целях определения соответствия результатов освоения обучающимися программы бакалавриата требованиям федерального государственного образовательного стандарта, выявления подготовленности выпускника к профессиональной деятельности. К государственной итоговой аттестации допускаются обучающиеся, в полном объеме выполнившие учебный план или индивидуальный учебный план по программе бакалавриата.

Целью государственной итоговой аттестации (в дальнейшем – ГИА) является установление степени соответствия уровня качества подготовки выпускника высшего учебного заведения к выполнению профессиональных задач требованиям федерального государственного образовательного стандарта высшего образования (ФГОС ВО), основной профессиональной образовательной программы (ОПОП) по направлению подготовки 10.03.01 Информационная безопасность, также определение степени овладения выпускниками необходимыми компетенциями.

Задачи государственной итоговой аттестации: комплексная оценка уровня подготовки выпускников Образовательной организации, которая:

- строится с учетом изменений в содержании и организации профессиональной подготовки выпускников, описываемых в рамках деятельностной парадигмы образования;
- оценивает уровень сформированности у выпускника необходимых компетенций, степени владения выпускником теоретическими знаниями, умениями и практическими навыками для профессиональной деятельности;
- учитывает возможность продолжения образования обучающимся на более высоких ступенях.

Общая трудоемкость государственной итоговой аттестации по направлению подготовки бакалавров 10.03.01 Информационная безопасность составляет 6 зачетных единиц (З.Е.), и включает в себя подготовку к процедуре защиты и защиту выпускной квалификационной работы (6 З.Е.).

Порядок и сроки проведения итоговых аттестационных испытаний устанавливаются на основании Положения о порядке проведения государственной итоговой аттестации по образовательным программам высшего образования в Образовательной организации, а также в соответствии с графиком учебного процесса по направлению подготовки бакалавров 10.03.01 Информационная безопасность.

Продолжительность государственной итоговой аттестации составляет 4 недели – выполнение и защита выпускной квалификационной работы.

Содержание итоговой аттестации является выпускная квалификационная работа (ВКР).

Выполнение и защита выпускной квалификационной работы бакалавра завершает подготовку обучающегося и показывает его готовность к основным видам профессиональной деятельности.

В процессе выполнения работы обучающемуся предоставляется возможность под руководством опытных специалистов углубить и систематизировать теоретические и практические знания, полученные в процессе освоения учебного плана, закрепление навыков самостоятельной исследовательской работы и творчески применить их в решении конкретных практических задач. Обучающиеся должны активно использовать знания из области менеджмента, экономики, статистики, организации коммерческой деятельности, маркетинга, рекламы, финансов и других смежных дисциплин, формирующих его как работы бакалавра по данному направлению.

Подготовка к выполнению выпускной квалификационной работы (ВКР) начинается с младших курсов, когда обучающиеся, выполняя рефераты по дисциплинам общей подготовке, курсовые и междисциплинарные работы по дисциплинам, учатся критически мыслить, делать выводы, обобщения. Преподаватели кафедры заранее ориентируют обучающихся на выбор таких тем курсовых работ, которые могут стать частью выпускных квалификационных работ.

Раскрывая сущность вопросов по избранной теме, выпускник должен показать и развить навыки самостоятельных исследований по проблемам менеджмента деловой организации, ее конкурентоспособности, а также по оптимизации организационной структуры, производственного процесса организации, инновационной ее деятельности, управления трудовыми ресурсами и др. Сформированные при написании курсовых работ

исследования получают логическое завершение в выпускной квалификационной работе работы бакалавра.

Таким образом, выпускная квалификационная работа бакалавра является формой оценки уровня его профессиональной квалификации.

Выпускная квалификационная работа бакалавра призвана выявить способность выпускников на основе полученных знаний самостоятельно решать конкретные практические аспекты в области управления организацией, подтвердить наличие профессиональных компетенций.

Основными целями выпускной квалификационной работы бакалавра являются:

– систематизация, закрепление и расширение теоретических и практических знаний обучающихся по дисциплинам направления 10.03.01 Информационная безопасность.

В соответствии с поставленными целями выпускник в процессе выполнения выпускной квалификационной работы бакалавра должен решить следующие задачи:

– обосновать актуальность выбранной темы и ее значение в решении проблем Интеллектуальных систем в гуманитарной сфере;

– изучить теоретические положения, нормативно-техническую и правовую документацию, статистические материалы, справочную, специальную и научную литературу по избранной теме и изложить свою точку зрения по относящимся к ней дискуссионным вопросам;

– провести анализ деятельности деловой организации и оценку её экономических показателей, показателей в области Информационной безопасности;

– использовать специальные программы обеспечения как инструмент обработки информации;

– провести анализ действующей системы;

– сформулировать выводы и разработать аргументированные предложения по повышению информационной безопасности информационной системы/интеллектуальной системы;

– оформить выпускную квалификационную работу в соответствии с требованиями Методических указаний по написанию выпускной квалификационной работы в Образовательной организации.

Обучающийся несет полную ответственность за самостоятельность и достоверность проведенного исследования в рамках выпускной

квалификационной работы. Все использованные в работе материалы и положения из опубликованной научной и учебной литературы, других информационных источников обязательно должны иметь на них ссылки.

По результатам защиты выпускной квалификационной работы Государственная экзаменационная комиссия решает вопрос о присвоении выпускнику соответствующей квалификации.

Тематика выпускных квалификационных работ должна быть актуальной, соответствовать современному состоянию и перспективам развития науки и техники.

ВКР выполняется на тему, которая соответствует области, объектам и видам профессиональной деятельности по направлению 10.03.01 Информационная безопасность (уровень бакалавриат).

Тематика ВКР определяется выпускающей кафедрой и утверждается уполномоченным органом Организации. Тематика ВКР должна соответствовать как современному уровню развития науки, так и современным потребностям общественной практики и формироваться с учетом предложений работодателей по данному направлению подготовки. При выборе тематики выпускных квалификационных работ рекомендуется учитывать реальные задачи экономики, социальной сферы, науки и практики в соответствии с направлениями научной деятельности Образовательной организации, работодателей.

Обучающийся имеет право выбора темы из предложенной тематики ВКР, подав заявление на выпускающую кафедру. ВКР может быть выполнена на тему, предложенную организацией-работодателем, в соответствии со стандартом направления подготовки и профилем. В этом случае работодатель на официальном бланке оформляет заявку с предложением определенной темы (направления) исследования.

Обучающийся имеет право предложить свою тему ВКР вместе с обоснованием целесообразности ее разработки при условии соответствия темы стандарту направления подготовки и профилю. Обучающийся, желающий выполнить выпускную квалификационную работу на тему, не предусмотренную примерным перечнем, должен обосновать свой выбор и получить согласие научного руководителя и разрешение заведующего профильной кафедры. Изменение или корректирование (уточнение) темы ВКР допускается в исключительных случаях по просьбе руководителя ВКР с последующим ее утверждением на заседании выпускающей кафедры.

Руководство и консультирование, требования к объему, структуре и оформлению ВКР, рецензирование ВКР и процедура защиты ВКР установлены положением о подготовке и защите ВКР обучающимися Академии ИМСИТ.

Выпускная квалификационная работа бакалавра выполняется на фактических материалах конкретной организации – как правило, объекта прохождения производственной / преддипломной практики, на основе глубокого изучения теоретических вопросов, относящихся к избранной теме работы, детального анализа практических материалов по основным направлениям деятельности объекта исследования. Обучающийся самостоятельно выбирает тему выпускной квалификационной работы исходя из ее актуальности, научного или практического интереса, наличия достаточного фактического и статистического материала.

Требования к структуре и содержанию выпускной квалификационной работы определяется Методическими указаниями по написанию выпускной квалификационной работы в Образовательной организации.

Выпускная квалификационная работа бакалавра должна иметь структуру, которая согласуется с научным руководителем:

– титульный лист;

– содержание;

– введение;

– основную часть, состоящую, как правило, не менее чем из трех разделов (теоретического, обзорного по заявленной проблематике; аналитического, организационно-экономического по рассматриваемой проблеме; практического, с рассмотрением реальной практики, опыта функционирования объекта исследования);

– заключение, включающее выводы и предложения (рекомендации);

– список используемых источников;

– приложения (при необходимости).

Основными требованиями к работе являются:

– четкость и логическая последовательность изложения материала;

– краткость и точность формулировок, исключающая возможность неоднозначного их толкования;

– конкретность изложения полученных результатов, их анализа и теоретических положений;

– обоснованность выводов, рекомендаций и предложений.

Содержание ВКР должно соответствовать названию темы.

Работа считается выполненной в полном объеме в том случае, если в ней

нашли отражение все проблемы и вопросы, предусмотренные заданием на выполнение выпускной квалификационной работы.

На каждом этапе работы над ВКР обучающийся должен продемонстрировать практически весь спектр компетенций, а руководитель имеет возможность оценить уровень их достижения и зафиксировать в своем отзыве.

Защита выпускной квалификационной работы проводится на открытых заседаниях экзаменационной комиссии с участием не менее двух третей ее состава при обязательном присутствии председателя комиссии и его заместителя.

Результаты защиты выпускной квалификационной работы определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и объявляются в тот же день после обсуждения членами Государственной экзаменационной комиссии и оформления в установленном порядке Протоколами заседания экзаменационной комиссии.

Оценку результатов выполнения ВКР производят члены экзаменационной комиссии.

Объектами оценки являются: ВКР; иллюстративный материал, выставляемый обучающимся на защиту ВКР; доклад обучающегося на заседании государственной экзаменационной комиссии; ответы обучающегося на вопросы, заданные членами комиссии в ходе защиты ВКР.

Критериями оценки ВКР являются:

– научный уровень доклада, степень освещенности в нем вопросов темы исследования, значение сделанных выводов и предложений для организации;

– использование специальной научной литературы, нормативных актов, материалов производственной практики;

– творческий подход к разработке темы;

– правильность и научная обоснованность выводов;

– стиль изложения;

– оформление выпускной квалификационной работы (ВКР);

– степень профессиональной подготовленности, проявившаяся как в содержании выпускной квалификационной работы бакалавра, так и в процессе её защиты;

– чёткость и аргументированность ответов обучающегося на вопросы, заданные ему в процессе защиты;

– оценки руководителя в отзыве и рецензента.

Результаты защиты выпускной квалификационной работы оцениваются по 4-х балльной системе:

Система оценки защиты выпускной квалификационной работы:

5 Отлично - структура ВКР соответствует заданию и отличается глубоко раскрытыми разделами. Обучающийся показывает глубокое и систематическое знание всего программного материала исчерпывающе, последовательно, четко и логически стройно излагает материал ВКР, умеет тесно увязывать теорию с практикой, не затрудняется с ответом при видоизменении вопросов, задаваемых членами государственной экзаменационной комиссии, использует в ответе материал монографической литературы, правильно обосновывает принятые в представленной ВКР решения, демонстрирует свободное владение научным языком и терминологией соответствующей научной области

4 Хорошо - структура ВКР соответствует заданию кафедры и раскрыта в требуемом объеме. Обучающийся показывает знание всего программного материала, свободно излагает материал ВБР, умеет увязывать теорию с практикой, но испытывает затруднения с ответом при видоизмененные вопросы, задаваемые членами государственной экзаменационной комиссии, принятые в представленной ВКР решения обоснованы, но присутствуют в проведенных расчетах неточности, демонстрирует владение научным языком и терминологией соответствующей научной области, но затрудняется с ответом при видоизменении заданий, при обосновании принятого решения возникают незначительные затруднения в использовании изученного материала.

3 Удовлетворительно - структура ВКР соответствует заданию. Обучающийся имеет фрагментарные знания материала, изложенного в ВКР, показывает знания важнейших разделов теоретического курса освоенных дисциплин и содержания лекционных курсов, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения в ответах на вопросы, задаваемые членами государственной экзаменационной комиссии.

2 Неудовлетворительно - обучающийся не владеет представленным материалом, допускает существенные ошибки, неуверенно, с большими затруднениями поясняет представленные в ВКР расчеты, демонстрирует неспособность отвечать на вопросы, задаваемые членами государственной экзаменационной комиссии.

На основании результатов государственного экзамена и защиты выпускной квалификационной работы делается заключение об уровне

освоения выпускником ОПОП и готовности к выполнению определенным в ОПОП видам профессиональной деятельности.

Для выпускников из числа инвалидов и лиц с ограниченными возможностями здоровья ГИА может проводиться с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких выпускников. При проведении ГИА для выпускников с индивидуальными особенностями обеспечивается соблюдение следующих общих требований: использование специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего выпускникам необходимую техническую помощь, обеспечение доступа в здания и помещения, где проходит ГИА, и другие условия, без которых невозможно или затруднено проведение ГИА.

При проведении ГИА обеспечивается соблюдение следующих общих требований: возможность выбора способа проведения ГИА; проведение ГИА для обучающихся-инвалидов и лиц с ограниченными возможностями здоровья в одной аудитории совместно с обучающимися, не имеющими ограниченных возможностей здоровья, если это не создает трудностей для обучающихся при прохождении государственной итоговой аттестации; присутствие в аудитории ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь с учетом их индивидуальных особенностей на основании письменного заявления; пользование необходимыми обучающимся техническими средствами при прохождении ГИА с учетом их индивидуальных особенностей.

Продолжительность прохождения ГИА по отношению к установленной продолжительности его сдачи увеличивается по письменному заявлению обучающегося с ограниченными возможностями здоровья: продолжительность выступления обучающегося при защите выпускной квалификационной работы – не более чем на 0,5 часа.

Материально-техническое обеспечение государственной итоговой аттестации предусматривает наличие аудитории для сдачи государственного экзамена и защиты выпускной квалификационной работы. Государственный экзамен должен проходить в аудиториях, предусматривающих наличие рабочих мест для председателя и членов государственной экзаменационной комиссии и рабочих мест для обучающихся, допущенных на государственный экзамен. Для защиты выпускной квалификационной работы также требуется аудитория, предусматривающая наличие рабочих мест для председателя и членов государственной экзаменационной комиссии, рабочего места для студента, компьютерной техники с необходимым лицензионным программным

обеспечением, мультимедийного проектора, экрана, щитов для размещения наглядного материала.

Порядок подачи и рассмотрения апелляций установлен положением Академии ИМСИТ об апелляционной комиссии по результатам итоговой аттестации.

Программа аттестации и требования к ВКР приведена в приложении Ж.

5.7 Образовательные технологии

Реализация ОПОП направлению подготовки 10.03.01 Информационная безопасность, направленность (профиль) программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)» предусматривает использование широкого спектра новых образовательных и информационно-коммуникационных технологий.

Все учебно-методические материалы по ОПОП разработаны:

1) по определенной структуре теоретической и практической части, позволяющей быстро менять содержание дисциплины адекватно современному состоянию науки и практики,

2) с возможностью использования широкого спектра учебных элементов, мотивирующих обучающихся к самостоятельному, инициативному и творческому освоению учебного материала в процессе познавательной деятельности, таких как:

- использование в лекционных курсах презентаций, элементов практики и тренинга, за счет включения наглядных примеров решения актуальных задач;

- выполнение на практических и семинарских занятиях индивидуальных и групповых заданий с использованием персональных компьютеров, информационных технологий;

- выполнение на практических и лабораторных занятиях индивидуальных и групповых проектов, решение творческих задач;

- самостоятельная разработка обучающимися технических и инновационных проектов в различных областях автоматизации обработки информации и управления; подготовка презентаций обучающимися как результата работы (индивидуально и в группах) по решению ситуационных задач, деловых игр; ведение открытых дискуссий по актуальным проблемам информатизации;

3) с возможностью использования балльно-рейтинговой оценки обучающегося. Совокупность образовательных технологий, применяемая при освоении дисциплин ОПОП для подготовки бакалавров по направлению подготовки 10.03.01 Информационная безопасность, направленность (профиль)

программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)», обусловлена как множеством формируемых компетенций выпускников, так и применением различных моделей обучения для достижения эффективного результата обучения (формирования соответствующей компетенции).

Модели обучения включают следующие методы:

– словесные, наглядные, практические (по способу предъявления учебной информации);

– репродуктивные, частично-поисковые, поисковые, исследовательские (по степени самостоятельности обучающегося в процессе обучения);

– объяснительно-иллюстративные, программированные, эвристические, проблемные, модельные (по степени информированности обучающегося о процессе обучения);

– Case study, метод проектов и другие.

Формы обучения, применяемые при освоении дисциплин ОПОП для подготовки бакалавров по направлению подготовки 10.03.01 Информационная безопасность, направленность (профиль) программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)», включают: лекции, семинары, практические и лабораторные работы, самостоятельные работы, курсовые работы, курсовые проекты, конференции, проекты и другие формы.

Применяемые при освоении дисциплин ОПОП ВО для подготовки бакалавров по направлению подготовки 10.03.01 Информационная безопасность, направленность (профиль) программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)» образовательные технологии обладают следующими характеристиками:

<u>общесистемными:</u>

- научность содержания, предполагающая построение содержания образования с учетом основных принципов педагогики, психологии, кибернетики, теории высшей нервной деятельности;

- открытость, предусматривающая возможность реализации любого способа управления учебной деятельностью;

- воспитывающий характер, заключающийся в сочетании процессов обучения и воспитания;

- креативность, предполагающая обеспечение подготовки бакалавров с творческим потенциалом, способных самостоятельно ставить и решать проблемы;

- надежность работы и системная целостность, заключающаяся в адекватной реакции на любые ответы и вопросы обучающихся;

- научная организация дизайна образовательной среды, предусматривающая обеспечение максимальной информативности при минимальной утомляемости обучающихся.

методологическими:

- целенаправленность, предусматривающая обеспечение обучающегося постоянной информацией о ближайших и отдаленных целях образования, степени достижения этих целей;

- обеспечение мотивации, предполагающей стимулирование постоянной высокой мотивации обучающихся, подкрепляемой целенаправленностью, активными формами работы, высокой наглядностью результатов, своевременной обратной связью;

- обеспечение обучения в сотрудничестве, заключающемся в совместной деятельности в процессе обучения обучающихся и преподавателя; обеспечение систематической обратной связи, обеспечивающую не только информацией об ошибках или отсутствии положительного результата, но и методах и средствах ее устранения;

- обоснованность оценивания, предполагающая применение кроме результатов контроля дополнительных показателей, в частности, характер ошибок, активность участия, степень сложности исследуемых проблем и т.д.;

- педагогическая гибкость, предполагающая возможность самостоятельного решения обучающимся о выборе учебной стратегии; возможность возврата назад, предполагающая отмену обучающимся ошибочных действий при самостоятельной работе.

структурные и организационные:

- структурная целостность, предусматривающая представление учебного материала в виде укрупненных дидактических единиц, сохраняющих логику, главные идеи и взаимосвязи осваиваемой учебной дисциплины;

- наличие входного контроля, предусматривающего диагностику уровня знаний обучающегося перед началом работы с целью обеспечения индивидуализации образования и оказания требуемой первоначальной помощи;

- индивидуализация образования, предполагающая многоуровневую организацию учебного материала, банк заданий разного уровня сложности;

- наличие развитой системы помощи, заключающейся в многоуровневости и достаточности системы помощи, позволяющей освоить метод, способ решения задач или проблем и учитывающей характер обучающегося;

- наличие интеллектуального ядра, предполагающего систему анализа причин ошибок обучающегося, комментарии, помогающие ему понять ошибки и сделать правильные выводы; возможность документирования процесса образования и его результатов.

6 УСЛОВИЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ ПО ОПОП

Требования к условиям реализации программы бакалавриата:

6.1 Требования к условиям реализации программы бакалавриата включают в себя общесистемные требования, требования к материально-техническому и учебно-методическому обеспечению, требования к кадровым и финансовым условиям реализации программы бакалавриата, а также требования к применяемым механизмам оценки качества образовательной деятельности и подготовки обучающихся по программе бакалавриата.

6.2. Общесистемные требования к реализации программы бакалавриата.

6.2.1 Академия ИМСИТ располагает на праве собственности и ином законном основании материально-техническим обеспечением образовательной деятельности (помещениями и оборудованием) для реализации программы бакалавриата по Блоку 1 «Дисциплины (модули)» и Блоку 3 «Государственная итоговая аттестация» в соответствии с учебным планом.

6.2.2 Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде академии из любой точки, в которой имеется доступ к информационно- телекоммуникационнойсети«Интернет» (далее – сеть «Интернет»), как на территории академии, так и вне ее. Условия для функционирования электронной информационно- образовательной среды могут созданы с использованием ресурсов Академии ИМСИТ и ООО «ЗНАНИУМ», ООО «КноРус медиа», ООО «Айбукс». Электронная информационно-образовательная среда Академии ИМСИТ (https://www.imsit.ru/ru/elibraries/elibraries.html) обеспечивает:

доступ к учебным планам, рабочим программам дисциплин (модулей), практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), практик;

формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы;

в случае реализации программы бакалавриата с применением электронного обучения, дистанционных образовательных технологий электронная информационно-образовательная среда Организации дополнительно обеспечивает: фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения программы бакалавриата.

проведение учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения,

дистанционных образовательных технологий; взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети«Интернет». В настоящее время электронное обучение не используется;

Функционирование электронной информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий (LMS Moodle, сайт академии на хостинге sweb.ru) и квалификацией работников, ее использующих и поддерживающих. Функционирование электронной информационно-образовательной среды должно соответствует законодательству Российской Федерации.

Перечень электронно-библиотечных систем и информационных ресурсов, используемых в процессе обучения по направлению подготовки 10.03.01 Информационная безопасность, направленность (профиль) программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)» представлен в таблице 6.1.

Таблица 6.1 - Электронные библиотечные системы и электронные ресурсы, используемые при подготовке по направлению подготовки 10.03.01 Информационная безопасность, направленность (профиль) программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)»

№	Наименование электронного ресурса	Принадлежи ость	Ссылка на ресурс	Наименование организации-владельца, реквизиты договора на использование	Доступность
1	2	3	4	5	6
1.	Web-ресурс «Электронная образовательная среда»	собственный	http://eios.imsit.ru	НАН ЧОУ ВО «Академия маркетинга и социально-информационных технологий – ИМСИТ» (г. Краснодар)	С любых компьютеров имеющих доступ к сети интернет по паролю
2.	Коллекция CD и DVD в фонде научной библиотеке Академии ИМСИТ	собственный	Компакт-диски (CD- ROM и DVD-ROM	НАН ЧОУ ВПО «Академия маркетинга и социально-информационных технологий»»	Полная коллекция - в электронном читальном зале научной библиотеки
3.	«Электронно-библиотечная система ZNANIUM.COM»	сторонний	http://znanium.com/	ООО «ЗНАНИУМ». Договор № 1398 эбс от 28.09.2023 г. Строк действия с 28.09.2023 до 27.09.2024 г.	С любых компьютеров имеющих доступ к сети интернет по паролю
4.	ЭБС «Айбукс.ру/ibo	сторонний	http://ibooks.ru/	ООО «ЗНАНИУМ». Договор № 1398 эбс от	С любых компьютеров

	oks.ru»			28.09.2023 г. Строк действия с 28.09.2023 до 27.09.2024 г.	имеющих доступ к сети интернет по паролю
5.	ЭБС «Айбукс.ру/ibooks.ru»	сторонний	http://ibooks.ru/	ООО «Айбукс». Договор № 27-01/23К от 27.01.2023 г. Срок действия с 27.01.2023 г. по 26.01.2024 г.	С любых компьютеров имеющих доступ к сети интернет по паролю
6.	Электронные Периодические издания	сторонний	http://elibrary.ru	ООО «Научная электронная библиотека» (г. Москва). Лицензионное соглашение № 7241 от 24.02.12 г.	С любых компьютеров имеющих доступ к сети интернет
7.	Электронно-библиотечная система BOOK.ru	сторонний	https://www.book.ru/	ООО «КноРус медиа». Договор №18511468 от 08 Сентября 2023 г. Срок действия с 10.09.2023 до 09.09.2024 г.	С любых компьютеров имеющих доступ к сети интернет
8.	Техническая документация Windows для разработчиков и ИТ-специалистов	сторонний	https://docs.microsoft.com/ru-RU/windows/	Microsoft. Режим доступа – свободный.	С любых компьютеров имеющих доступ к сети интернет по паролю
9.	Справочный центр Astra Linux	сторонний	https://wiki.astralinux.ru/	ООО «РусБИТех-Астра». Договор №А-2023-3968-ВУЗ от 08 августа 2023 г.	С любых компьютеров имеющих доступ к сети интернет по паролю
10	База знаний Astra.	сторонний	https://wiki.astralinux.ru/kb	ООО «РусБИТех-Астра». Договор №А-2023-3968-ВУЗ от 08 августа 2023 г.	С любых компьютеров имеющих доступ к сети интернет по паролю
11	Код Безопасности	сторонний	https://www.securitycode.ru/	ООО «Код Безопасности». Договор КБ/04085/1/11 от 14.02.2022 г.	С любых компьютеров имеющих доступ к сети интернет по паролю
12	Федеральная Служба по Техническому и Экспортному Контролю	сторонний	https://fstec.ru/	ФСТЭК России. Режим доступа – свободный.	С любых компьютеров имеющих доступ к сети интернет по паролю
13	Справочно-правовая база «Консультант Плюс»	сторонний	Локальная сеть Академии ИМСИТ	Консультант-Плюс в г. Краснодаре Договор о сотрудничестве № ИП-2 от 24.05.2007 г. действует по настоящее время	С компьютеров академии
14	Web-ресурс «Официальный сайт Академии ИМСИТ»	собственный	https://imsit.ru	НАН ЧОУ ВО «Академия маркетинга и социально-информационных технологий – ИМСИТ» (г. Краснодар)	С любых компьютеров имеющих доступ к сети интернет

6.2.3 Сетевая форма при реализации программы бакалавриата не используется. При реализации программы бакалавриата в сетевой форме требования к реализации программы бакалавриата должны обеспечиваться

совокупностью ресурсов материально-технического и учебно-методического обеспечения, предоставляемого организациями, участвующими в реализации программы бакалавриата в сетевой форме.

6.3 Требования к материально-техническому и учебно-методическому обеспечению программы бакалавриата (приложение И).

6.3.1 Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой бакалавриата, оснащенные оборудованием и техническими средствами обучения, состав которых определяется в рабочих программахдисциплин (модулей). Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательнуюсреду Академии ИМСИТ. Допускается замена оборудования его виртуальными аналогами.

6.3.2 Академия ИМСИТ обеспечена необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства (состав определен в рабочих программах дисциплин (модулей) и подлежитпри необходимости обновляется).

6.3.3 Библиотечный фонд, на ряду с электронными изданиями, укомплектован печатными изданиями из расчета не менее 0,25 экземпляра каждого из изданий, указанных в рабочих программах дисциплин (модулей), практик, на одного обучающегося из числа лиц, одновременно осваивающих соответствующуюдисциплину(модуль), проходящих соответствующую практику.

6.3.4 Обучающимся должен обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, состав которых определяется в рабочих программах дисциплин (модулей) и обновляется при необходимости.

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

6.4 Требования к кадровым условиям реализации программы бакалавриата (приложение К).

6.4.1 Реализация программы бакалавриата обеспечивается педагогическими работниками Академии ИМСИТ, а также лицами, привлекаемыми академией к реализации программы бакалавриата на иных условиях.

6.4.2 Квалификация педагогических работников академии отвечает квалификационным требованиям, указанным в квалификационных справочниках и (или) профессиональных стандартах(приналичии).

6.4.3 Более 70 процентов численности педагогических работников академии, участвующих в реализации программы бакалавриата, и лиц, привлекаемых 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).

6.4.4 Более 5 процентов численности педагогических работников академии, участвующих в реализации программы бакалавриата, и лиц, привлекаемых 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 (имеют стаж работы в данной профессиональной сфере не менее 3 лет).

6.4.5 Не менее 60 процентов численности педагогических работников академии и лиц, привлекаемых к образовательной деятельности 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).

6.4.6 В реализации программы бакалавриата принимают участие два педагогических работника Организации, имеющих ученую степень или ученое звание по научной специальности 05.13.19 "Методы и системы защиты информации, информационная безопасность" или по научной специальности, соответствующей направлениям подготовки кадров высшей квалификации по программам подготовки научно-педагогических кадров в адъюнктуре, входящим в укрупненную группу специальностей и направлений подготовки 10.00.00 «Информационная безопасность».

6.5 Требования к финансовым условиям реализации программы бакалавриата.

6.5.1 Финансовое обеспечение реализации программы бакалавриата должно осуществляться в объеме не ниже значений базовых нормативов затрат на оказание государственных услуг по реализации образовательных программ высшего образования – программ бакалавриата и значений корректирующих

коэффициентов к базовым нормативам затрат, определяемых Министерством Просвещения Российской Федерации.

6.6 Требования к применяемым механизмам оценки качества образовательной деятельности и подготовки обучающихся по программе бакалавриата.

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

6.6.2 В целях совершенствования программы бакалавриата Организация 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 Организации. 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.

6.6.3 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.

6.6.4 Внешняя оценка качества образовательной деятельности и подготовки обучающихся по программе бакалавриата может осуществляться 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, освоивших программу бакалавриата, отвечающими требованиям профессиональных стандартов (при наличии), требованиям рынка труда к специалистам соответствующего профиля.

7 ХАРАКТЕРИСТИКИ СОЦИАЛЬНО-КУЛЬТУРНОЙ СРЕДЫ НАН ЧОУ ВО АКАДЕМИИ ИМСИТ, ОБЕСПЕЧИВАЮЩИЕ РАЗВИТИЕ ОБЩЕКУЛЬТУРНЫХ (СОЦИАЛЬНО - ЛИЧНОСТНЫХ КОМПЕТЕНЦИЙ) КОМПЕТЕНЦИЙ ВЫПУСКНИКОВ ПО НАПРАВЛЕНИЮ 10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НАПРАВЛЕННОСТЬ (ПРОФИЛЬ) ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ «БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ (ПО ОТРАСЛИ ИЛИ В СФЕРЕ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)»

Социально-культурная среда формируется в соответствии с концепцией воспитательной работы в академии, программой по оздоровлению участников образовательного процесса и пропаганде здорового образа жизни в НАН ЧОУ ВО Академии ИМСИТ.

Цель социально-культурной среды - подготовка разносторонне развитой и профессионально ориентированной личности, способной конкурировать на рынке труда, обладающей высокой культурой, социальной активностью, мировоззренческим потенциалом, интеллигентностью, качествами гражданина, способностями к профессиональному, интеллектуальному и социальному творчеству, владеющей устойчивыми профессиональными умениями и навыками.

Задачи социально-культурной среды:

— создание оптимальных социокультурных и образовательных условий для социального и профессионального становления личности социально активного, жизнеспособного, гуманистически ориентированного, высококвалифицированного специалиста;

— формирование и развитие личностных качеств, необходимых для эффективной профессиональной деятельности;

— формирование гражданской позиции и патриотического сознания, правовой и политической культуры;

— формирование ориентации на общечеловеческие ценности и высокие гуманистические идеалы культуры;

— воспитание нравственных качеств, интеллигентности;

— формирование и развитие умений и навыков управления коллективом в различных формах самоуправления обучающихся;

— формирование и развитие чувства академического корпоративизма и солидарности, стремления к здоровому образу жизни, воспитание нетерпимого отношения к антиобщественному поведению.

Профессионалъно-творческая и трудовая составляющая среды – организованный и контролируемый образовательный процесс приобщения

обучающихся к профессиональному труду в ходе их становления как субъектов трудовой деятельности, увязанный с овладением квалификацией и воспитанием профессиональной этики.

Основные формы реализации:

— организация научно-исследовательской работы обучающихся;

— проведение выставок научно-исследовательских работ;

— проведение межвузовских и международных конкурсов на лучшие научно-исследовательские и выпускные квалификационные работы;

— проведение конкурсов на получение грантов на уровнях НАН ЧОУ ВО Академии ИМСИТ и Краснодарского края на лучшие научно-исследовательские, инновационные проекты;

— проведение конкурсов на лучшую группу, лучшего обучающегося; привлечение обучающихся к научно-исследовательской деятельности;

— прочие формы.

Духовно-нравственная составляющая среды – формирование нравственного сознания и моральных качеств личности, умений и навыков соответствующего поведения в различных жизненных ситуациях, ответственности человека не только перед самим собой, но и перед другими людьми.

Основные формы реализации:

— вовлечение обучающихся в деятельность творческих коллективов, досуговых мероприятий, кружков, секций, поддержание и инициирование их деятельности;

— организация выставок творческих достижений обучающихся, сотрудников, ППС;

— развитие досуговой, клубной деятельности, поддержка молодежной творческой субкультуры;

— организация и проведение культурно-массовых мероприятий («Посвящение в студенты», «Две звезды», «Мисс и Мистер ИМСИТ», «КВН», «Звездопад талантов» и т.п.);

— участие в спортивных мероприятиях академии;

— анализ социально-психологических проблем обучающихся и организация психологической поддержки;

— другие формы.

Патриотическая составляющая среды – воспитание любви к Родине и преданности Отечеству, стремления и желания служить его интересам и готовность к его защите.

Основные формы реализации:

— изучение проблем отечественной истории, российской культуры и

философии, литературы и искусства, достижений российской науки и техники;

— научно-исследовательская деятельность по историко-патриотической тематике, итоги которой находят отражение в научных статьях и докладах на научных конференциях различного уровня;

— организация субботников и других мероприятий для воспитания бережливости и чувства причастности к НАН ЧОУ ВО Академии ИМСИТ, факультету, группе;

— курирование групп младших курсов старшекурсниками;

— проведение общеакадемических конкурсов, формирующих у молодых людей интерес к истории НАН ЧОУ ВО Академии ИМСИТ, города Краснодара, Краснодарского края (конкурсы сочинений, конкурс патриотической направленности и др.);

— проведение профориентационной работы в школах и других имиджевых мероприятий силами обучающихся,

— читательские конференции, обзоры литературы, организация выставок, проведение мероприятий с активом обучающихся;

— организация встреч с ветеранами Великой Отечественной войны;

— публикация материалов, раскрывающих проблемы духовно-нравственных ориентиров обучающихся, отражающие историю нашей страны, города и НАН ЧОУ ВО Академии ИМСИТ, место и роль коллектива в этом процессе.

Правовая составляющая среды – воспитание уважения к Конституции Российской Федерации и другим российским законам. Воспитание уважения к суду и государственным институтам России.

Основные формы реализации:

— развитие самоуправления обучающихся;

— организация и проведение городских, региональных семинаров по гражданско-правовому и патриотическому образованию и воспитанию;

— участие в программах государственной молодежной политики всех уровней;

— развитие волонтерской деятельности;

— прочие формы.

Эстетическая составляющая среды – развитие творческих способностей, личное формирование умений творчески мыслить и творчески подходить к решению любых практических задач, а также формирование установок на положительное восприятие ценностей отечественного, национального искусства.

Основные формы реализации: развитие системы творческих клубов и коллективов; другие формы.

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

Основные формы реализации:

— физическое воспитание и валеологическое образование обучающихся;

— организация летнего отдыха обучающихся;

— организация работы спортивных секций, спартакиад;

— проведение социологических исследований жизнедеятельности обучающихся;

— профилактика наркомании, алкоголизма и других вредных привычек;

— профилактика правонарушений;

— пропаганда здорового образа жизни, занятий спортом, проведение конкурсов, их стимулирующих.

Экологическая составляющая среды – формирование мировоззрения, основанного на объективном единстве человека с природой, представлении о целостной картине мира; накопление опыта, приобретение ценностных ориентиров, инженерных навыков в сфере сохранения природы и окружающей среды, обеспечение экологической безопасности человека.

Основные формы реализации:

— развитие и совершенствование деятельности экологического общества обучающихся;

— участие НАН ЧОУ ВО Академии ИМСИТ в традиционных городских акциях;

— прочие формы.