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.

ПРОГРАММА ИТОГОВОЙ АТТЕСТАЦИИ

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

Квалификация выпускника
«Бакалавр»

Краснодар
2023

Программа итоговой аттестации по основной профессиональной образовательной программе направления подготовки 10.03.01 Информационная безопасность, направленность (профиль) образовательной программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)» рассмотрена и одобрена на заседании кафедры математики и вычислительной техники 13 октября 2023 г., протокол № 3.

Зав. кафедрой, доцент Н.П. Исикова

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

Согласовано:
Проректор по учебной работе, доцент Н.И. Севрюгина

Проректор по качеству образования, доцент К.В. Писаренко

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

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

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Федеральный государственный стандарт (ФГОС ВО) по направлению подготовки 10.03.01 Информационная безопасность утвержденный приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г. № 1427 устанавливает обязательную процедуру прохождения обучающимися итоговой аттестации, которая завершается присвоением квалификации бакалавра.

Итоговая аттестация (ИА) выпускников по направлению подготовки 10.03.01 Информационная безопасность включает:

– выполнение и защиту выпускной квалификационной работы.

Нормативную правовую базу проведения итоговой аттестации выпускников, обучающихся по направлениям подготовки/специальностям высшего образования – программам бакалавриата, программам специалитета, программам магистратуры составляют:

– Федеральный закон «Об образовании в Российской Федерации» от 29 декабря 2012 г. №73-ФЗ;

– Приказ Минобрнауки России от 29.06.2015 г. № 636 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры»;

– Приказ Министерства образования и науки РФ от 05.04.2017 года № 301 «Об утверждении порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»;

– ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность утвержденный приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г. № 1427.

– Нормативно-методические документы Минобрнауки РФ;

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

Вышеуказанные нормативно-правовые акты определяют порядок организации и проведения процедуры ИА, устанавливают оформление и защиту выпускных квалификационных работ, подготовленных обучающимися по направлению подготовки 10.03.01 Информационная безопасность, а также рекомендации для самостоятельной подготовки обучающихся к итоговой аттестации. В соответствии с учебным планом, обучающийся выходят на процедуру ИА по окончании периода своего обучения в рамках (профиля) образовательной программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)».

Процедура ИА позволяет определить успешность овладения выпускником компетенций, предписанных требованиями федерального государственного образовательного стандарта. Успешность прохождения итоговой аттестации является основанием для выдачи выпускнику документа о высшем образовании и приобретенной квалификации образца, установленного Министерством образования и науки Российской Федерации. Сроки проведения итоговой аттестации устанавливаются в соответствии с учебным планом и календарным учебным графиком.

Обучающиеся, не прошедшие процедуру ИА в установленные сроки, отчисляются из академии с выдачей соответствующей справки об обучении, поскольку они не исполнили свои обязанности по добросовестному освоению образовательной программы и выполнению учебного плана.

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Цель и задачи итоговой аттестации

Цель итоговой аттестации в установлении уровня готовности выпускника к выполнению профессиональных задач и определение соответствия его подготовки требованиям ФГОС ВО (СУОС) по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриат).

Задачи итоговой аттестации:

– определить готовность выпускника к видам будущей профессиональной деятельности;

– установить уровень сформированности практических и теоретических знаний, умений и навыков выпускника, соответствующих компетенциям, определенным ФГОС ВО (СУОС) по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриат).

Следует считать выпускника соответствующими требованиям ФГОС ВО, при условии демонстрации выпускником системы знаний, умений и навыков, свидетельствующих о его готовности (способности) решать задачи профессиональной деятельности в типовых ситуациях.

Область профессиональной деятельности и сфера профессиональной деятельности, в которых выпускники, освоившие программу бакалавриата (далее – выпускники), 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).

Профессиональные стандарты, соответствующие профессиональной деятельности выпускников, из числа указанных в приложении к ФГОС ВО: 06.030 Специалист по защите информации в телекоммуникационных системах и сетях, 06.032 Специалист по безопасности компьютерных систем и сетей,

06.033 Специалист по защите информации в автоматизированных системах, 06.034 Специалист по технической защите информации.

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

Задачи профессиональной деятельности:

Эксплуатация автоматизированных систем в защищённом исполнении. Реализация требуемых политик безопасности в автоматизированных системах. Обеспечение защищённости процессов обработки информации в автоматизированных системах.

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.

Определение соответствия достигаемого уровня защищённости требования нормативных документов. Использование инструментальных средств анализа защищённости автоматизированных систем.

Организация и выполнение работ по обеспечению информационной безопасности в автоматизированных системах. Подготовка данных для составления обзоров и отчетов по инцидентам информационной безопасности.

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.

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, тип задач и задачи профессиональной деятельности выпускников.

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

Программа бакалавриата должна устанавливать следующие универсальные компетенции:

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции выпускника
Системное и критическое мышление	УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач
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
Командная работа и лидерство	УК-3. Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде
Коммуникация	УК-4. Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)
Межкультурное взаимодействие	УК-5. Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни
	УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и 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
Экономическая культура, в том числе финансовая грамотность	УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности
Гражданская позиция	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности

Программа бакалавриата должна устанавливать следующие общепрофессиональные 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-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;

ОПК-3. Способен использовать необходимые математические методы для решения задач профессиональной деятельности;

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

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;

ОПК-6. Способен при решении 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-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности;

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

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

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

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

ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для 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.

В дополнение к указанным общепрофессиональным компетенциям программа бакалавриата должна устанавливать общепрофессиональные компетенции, соответствующие выбранной направленности (профилю) программы бакалавриата, установленной в соответствии с пунктом 1.14 ФГОС ВО:

направленность (профиль) Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности):

ОПК-4.1. Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах;

ОПК-4.2. Способен администрировать операционные системы, системы управления базами данных, вычислительные сети;

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-4.4. Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем.

Профессиональные компетенции, устанавливаемые программой бакалавриата, сформированы на основе профессиональных стандартов, соответствующих профессиональной деятельности выпускников (06.030 Специалист по защите информации в телекоммуникационных системах и сетях, 06.032 Специалист по безопасности компьютерных систем и сетей, 06.033 Специалист по защите информации в автоматизированных системах, 06.034 Специалист по технической защите информации), а также проектов примерных профессиональных образовательных программ.

Профессиональные компетенции, обеспечивающие выпускнику способность решать задачи эксплуатационного типа:

ПК-1 Способен эксплуатировать средства обеспечения информационной безопасности автоматизированных систем.

ПК-2 Способен реализовывать политики безопасности с использованием инструментальных средств обеспечения информационной безопасности.

ПК-3 Способен обеспечивать безопасную обработку данных в автоматизированных системах.

Профессиональные компетенции, обеспечивающие выпускнику способность решать задачи проектно-технологического типа:

ПК-4 Способен выполнять работы по проектированию автоматизированных систем в защищенном исполнении.

ПК-5 Способен выполнять работы по обеспечению информационной безопасности автоматизированных систем на всех этапах их жизненного цикла.

ПК-6 Способен документально оформлять работы по обеспечению информационной безопасности.

Профессиональные компетенции, обеспечивающие выпускнику способность решать задачи экспериментально-исследовательского типа:

ПК-7 Способен определять уровень защищённости автоматизированных систем.

ПК-8 Способен выполнять задачи по выявлению уязвимых узлов автоматизированной системы.

Профессиональные компетенции, обеспечивающие выпускнику способность решать задачи организационно-управленческого типа:

ПК-9 Способен организовывать работы по обеспечению информационной безопасности в автоматизированных системах.

ПК-10 Способен собирать, анализировать и систематизировать информацию по зафиксированным инцидентам информационной безопасности.

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.

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	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

в телекоммуникационных системах и сетях» (Зарегистрировано в Минюсте России 18 октября 2022 г. N 70596)				
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)	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
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	B	Проведение работ по установке и техническому обслуживанию защищенных средств обработки	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10	Высшее образование - бакалавриат

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)		информации		
	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 приведенной ниже таблицей:

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	ПК-8

	функционирования СССЭ, их защищенности от НД и компьютерных атак	
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
В/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 информационной инфраструктуры	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10
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 информации в операционных системах	ПК-2
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 сетях	ПК-2
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	ПК-2

	оборудования	
Зн.4	Порядок реализации методов и средств межсетевого экранирования	ПК-2
Зн.5	Принципы функционирования сетевых протоколов, включающих криптографические алгоритмы	ПК-2
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	ПК-3

		программного обеспечения	
	Зн.11	Принципы функционирования программных средств криптографической защиты информации	ПК-2
	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
B/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 системы, возникающих в ходе ее	ПК-1; ПК-3

	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	ПК-4

	информации	
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	ПК-10

	автоматизированной системе	
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 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.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	ПК-2

	информации	
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	ПК-1

		эксплуатации и эксплуатационно-технической документацией	
	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	ПК-6

	информации)	
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 информации	ПК-6; ПК-8
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	ПК-6

	методом высокочастотного облучения основных технических средств и систем и за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах	
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
E/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 информации от несанкционированного доступа	ПК-6; ПК-7
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	ПК-6

	технологический процесс обработки информации	
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.

1.2 Место итоговой аттестации в структуре ОПОП

Итоговая аттестация, завершающая освоение основной профессиональной образовательной программы, является обязательной итоговой аттестацией обучающихся. Итоговая аттестация относится к базовой части Блоку 3 «Государственная итоговая аттестация» в структуре основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность и завершается присвоением квалификации «Бакалавр».

1.3 Объем итоговой аттестации

Общая трудоемкость ИА составляет 324 часа (9 з.е.) в том числе: 324 часа (9 з.е.) на выполнение и защиту выпускной квалификационной работы.

2 СОДЕРЖАНИЕ ПРОГРАММЫ ВЫПОЛНЕНИЯ И ЗАЩИТЫ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

2.1 Вид выпускной квалификационной работы

В соответствии с порядком проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам бакалавриата, утвержденным приказом Министерства образования и науки РФ от 29.06.2015г. № 636, положением о порядке проведения государственной итоговой аттестации по не имеющим государственной аккредитации образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам бакалавриата. Дата утверждения: 28 августа 2019 года, протокол Ученого Совета № 1 (с изменениями и дополнениями от 01.07.2022, протокол Ученого Совета № 10), обучающиеся Академии ИМСИТ, получающие по окончании обучения квалификацию (степень) «Бакалавр» выполняют выпускную квалификационную работу.

Целью подготовки и защиты выпускной квалификационной работы является систематизация, закрепление и расширение теоретических и практических знаний в области информационной безопасности и выявление умения применять полученные знания при решении конкретных технических, научных и производственных задач, развитие навыков ведения самостоятельной аналитической работы и применения полученных знаний в исследовательской работе, выявление степени подготовленности выпускника к практической деятельности в различных областях российской экономики.

Защита выпускной квалификационной работы проводится на заседании Экзаменационной комиссии (ГЭК). Результаты защиты выпускной квалификационной работы являются основанием для принятия

Экзаменационной комиссией решения о присвоении соответствующей квалификации (степени) и выдаче диплома.

2.2 Структура выпускной квалификационной работы и требования к ее содержанию

Выпускная квалификационная работа должна представлять собой законченную разработку актуальной проблемы и обязательно включать в себя как аналитическую часть, в которой показаны знания основ теории по разрабатываемой проблеме, так и практическую часть, в которой необходимо показать уровень сформированности компетенций, предусмотренных соответствующим ФГОС ВО, профессиональных знаний выпускника, его умений и навыков по осуществлению практической и / или научной деятельности.

ВКР разрабатывается на конкретном материале предприятий, организаций, органов управления и должна содержать решение актуальных технических задач.

Выпускная квалификационная работа обязательно должна содержать как теоретический, так и практический материал. ВКР, содержащая только теоретический материал (или изложение действующих инструкций, методик и т.п.) без практических рекомендаций к защите не допускается.

Особое внимание следует уделить **логике изложения материала.**

Основные **требования:**

- движение от общего (основ теории) к частному (анализу и рекомендациям по конкретной организации);

- соответствие выводов и предложений результатам анализа; отсутствие повторений и дублирования по разделам;

- точное соответствие текста выпускной квалификационной работы поставленным в плане вопросам;

- корректность и ясность формулировок.

Не допускается дословное переписывание литературных источников.

Язык и стиль выпускной квалификационной работы должны соответствовать нормам письменной научной речи. Прежде всего, необходимо соблюдать формально-логическую последовательность, целостность и связность изложения материала. Также должен использоваться терминологический аппарат данной предметной области, без применения профессиональной лексики (жаргона) и лексики средств массовой информации. В этой связи необходимо обратить внимание на юридически правильные названия учреждений и организаций, упоминаемых в работе. Сокращения этих названий должны соответствовать требованиям ГОСТ или нормативных актов.

Выпускная квалификационная работа содержи следующие **структурные элементы:** титульный лист; реферат; содержание; введение; основная часть; заключение;

список использованных источников; приложения.

Структурные элементы перечислены в порядке размещения их в документе.

В состав выпускной квалификационной работы может также входить перечень определений, обозначений и сокращений.

Титульный лист является первой страницей выпускной квалификационной работы, заполняется по строго определенным правилам.

Реферат должен кратко отражать основное содержание выпускной квалификационной работы и содержать следующие структурные элементы:

- сведения об объеме выпускной квалификационной работы, количестве иллюстраций, таблиц, приложений, количестве частей выпускной квалификационной работы, количестве использованных источников;

- перечень ключевых слов и словосочетаний, включающий от 5 до 15 слов или словосочетаний из текста выпускной квалификационной работы, которые в наибольшей степени характеризуют её содержание и обеспечивают возможность информационного поиска. Ключевые слова приводятся в именительном падеже и печатаются прописными буквами в строку через запятые;

- текст реферата, который должен отражать объект исследования, цель работы, метод или методологию проведения работы, основные результаты работы, рекомендации по внедрению или итоги внедрения результатов выпускной квалификационной работы, область применения, эффективность (экономическую) или значимость работы, может содержать описание предмета дальнейших исследований.

Оптимальный объем реферата – 0,75 страницы текста**.**

В **Содержании** последовательно перечисляют все заголовки выпускной квалификационной работы с указанием страниц, с которых они начинаются. Заголовки должны точно повторять заголовки в тексте выпускной квалификационной работы. Сокращать заголовки в содержании, давать их в иной редакции по сравнению с заголовками в тексте не допускается.

Введение является важной частью работы, поэтому оно должно быть тщательно проработано, выверено логически, стилистически, орфографически и пунктуационно.

Несмотря на то, что Введение открывает выпускную квалификационную работу, его окончательный текст пишется уже после написания основной части.

Структурно введение состоит из нескольких логических элементов, большинство из которых были сформулированы ранее, а на заключительном этапе их необходимо лишь отредактировать.

Во Введении обосновываются:

1. ***Актуальность работы*** (необходимо аргументировать, в силу чего именно эта проблема значима для исследования). Освещение актуальности должно быть немногословным. В пределах одной машинописной страницы следует показать главное – суть проблемной ситуации, из чего и будет видна актуальность темы.

2. ***Цель выпускной квалификационной работы*** представляет собой формулировку результата исследовательской деятельности и путей его достижения с помощью определенных средств. Необходимо учитывать, что у работы может быть только одна цель. Целью выпускной квалификационной

работы может быть разработка студентом предложений по совершенствованию информационной инфраструктуры объекта исследования.

Не следует формулировать цель как *«Исследование ... », «Изучение ... »,* так как эти слова указывают на процесс достижения цели, а не на саму цель.

3. ***Задачи исследования*** – совокупность элементов цели исследования; составные части результата; этапы, которые нужно пройти для достижения цели. Это обычно делается в форме перечисления *(выявить..., описать..., установить..., определить.., разработать....* и т. п.). Так, если *целью* исследования является, например, сравнительная характеристика методов решения проблемы, то *задачами* будут - выработка критериев сравнения, описание методов, формулирование выводов по результатам анализа. Постановку задач следует делать как можно более тщательно, т.к. их решение составляет содержание разделов выпускной квалификационной работы.

4. ***Объект исследования*** – Объект исследования – это определённая часть знаний, подвергающаяся исследованию. Каждый объект содержит в себе множество предметов исследования.

5. Предмет исследования это конкретный аспект занимаясь рассмотрением которого познается целостный объект, обозначаются и выделяются его характерные свойства.

Как категории науки объект и предмет проблемы соотносятся как общее и, занимаясь частное. Предмет ВКР изучает отдельную, выбранную часть объекта. предмет, т.е. в предмете выделяется конкретное свойство, черта, признак, принадлежащий объекту.

Пример: объектом исследования является предприятие ООО «Прорыв», основным направлением деятельности которого является производство сельскохозяйственных удобрений. Предметом исследования является проблема совершенствование защиты информации, циркулирующей в автоматизированной информационной системе предприятия.

6. ***Методы исследования (****не обязательный элемент****).*** Метод можно определить как способ достижения цели, совокупность приемов и операций

теоретического или практического освоения действительности. Методы исследования, используемые в работе, зависят от поставленных целей и задач, а также от специфики объекта изучения.

Могут быть использованы как теоретические, так и практические методы исследования.

При обосновании методов исследования можно употребить такие обороты:

«При написании работы в методологическом плане применялась следующая совокупность методов ... », «В методологическом отношении для понимания ... использовались разработки ... ».

Структура работы (название разделов работы и их краткая характеристика).

По объему Введение обычно занимает 1-3 страницы текста.

При написании **основной части** исследования необходимо учитывать следующее.

1. Изложение материала должно быть ***последовательным и логичным.*** Общая логика написания параграфа сводится к стандартной логической схеме (количество таких цепочек в параграфе может быть любым):

«Тезис – Доказательство – Вывод».

Все разделы выпускной квалификационной работы должны быть связаны между собой. Особое внимание следует обращать на логические переходы от одного раздела к другому, от подраздела к подразделу, а внутри подраздела - от пункта к пункту.

Для связи разделов работы и подразделов между собой возможно использовать прием заключительного перехода, который состоит в кратком подведении итогов того, что излагалось в данном разделе и аннотации следующей части работы:

«Таким образом, / Итак, в данном разделе / в данном пункте мы рассмотрели/ мы пришли к выводу, что ... »

«*В следующем разделе / В следующем подразделе / В следующей части*

работы / *Далее мы рассмотрим/ проанализируем/ считаем необходимым представить ...* »

2. ***Использование цитат*** в тексте необходимо того, чтобы без искажений передать мысль автора первоисточника, для идентификации взглядов при сопоставлении различных точек зрения и т.д. Отталкиваясь от содержания цитат, необходимо создать систему убедительных доказательств, важных для объективной характеристики изучаемого вопроса. Цитаты также могут использоваться и для подтверждения отдельных положений работы.

Число используемых цитат должно быть оптимальным, то есть определяться потребностями разработки темы. Цитатами не следует злоупотреблять, их обилие может восприниматься как выражение слабости собственной позиции автора. Цитаты должны употребляться к месту и быть органически взаимосвязаны с содержанием работы.

Оптимальный объем цитаты – одно-два, максимум три предложения. При цитировании в тексте цитаты сохраняются все особенности документа, из которого она взята: орфография, пунктуация, расстановка абзацев, шрифтовые выделения. Цитата внутри текста заключается в кавычки. Если цитируемый текст имеет больший объем, его следует заменять аналитическим пересказом.

Во всех случаях употребления цитат или пересказа мысли автора необходимо делать точную ссылку на источник. Недопустимо дословное (без соответствующих ссылок) заимствование текста из учебников, специальной литературы, нормативных и инструктивных материалов.

3. Авторский текст (собственные мысли) должен быть передан в ***научном стиле.***

Научный стиль предполагает изложение информации от первого лица множественного числа. Его стоит обозначить: безличными предложениями:

«необходимо подчеркнуть, что ... », «важно обратить внимание на тот факт, что ... », «следует отметить ... » и т. д.

4. Отдельные положения выпускной квалификационной работы должны быть иллюстрированы ***цифровыми данными*** из справочников, монографий и

других литературных источников, при необходимости оформленными в справочные или аналитические таблицы, диаграммы, графики.

При составлении аналитических таблиц, диаграмм, графиков используемые исходные данные могут выносится в приложения. В тексте, анализирующем или комментирующем таблицу, не следует пересказывать ее содержание, а уместно формулировать основной вывод, к которому подводят табличные данные, или вводить дополнительные показатели, более отчетливо характеризующие то или иное явление или его отдельные стороны. Все материалы, не являющиеся необходимыми для решения поставленной в работе задачи, также выносятся в приложения.

Основная часть выпускной квалификационной работы, в зависимости от темы работы, может включать в себя аналитический, проектный разделы и раздел реализации проектных решений.

Аналитический раздел включает исследование предметной области, теоретический обзор состояния проблемы, концептуальную модель, анализ проблемы и постановку задачи, выбор метода решения проблемы и анализ требований.

Проектный раздел должен содержать определение архитектурных представлений решения проблемы, моделирование компонентов разрабатываемого решения. Второй раздел может включать описание экспериментов и методику обработки результатов исследований.

Реализация разработки содержать описание разработки. Это может быть реализация программных модулей, интерфейса пользователя. Описание реализации проектной документации. Содержание раздела зависит от темы исследования и направления подготовки. Третий раздел может включать постановку экспериментов и обработку результатов исследований.

Третий раздел выпускной квалификационной работы, таким образом, может содержать конкретные разработки по решению проблемы или задачи, вытекающие из предыдущих анализов и решений.

Если сформулированные в работе предложения уже внедрены, то

рекомендуется приложить соответствующий подтверждающий документ - акт о внедрении, решение руководителей объекта о целесообразности внедрения предложений и т.д. Это в значительной степени повышает практическую значимость выпускной квалификационной работы.

Результат работы зависит от особенностей формулировки темы, целей и задач, а также выбранных методов и рекомендаций научного руководителя и консультанта.

Также в работе может приводится технико-экономическое обоснование разработанных решений.

Следующая важная часть работы – **заключение.** Заключение представляет собой обобщение всего содержания работы с акцентом на решения, описанные в реализации разработки. Последовательность изложения Заключения соответствует последовательности рассмотренных в выпускной квалификационной работе проблем, отражает результаты проведенного анализа и выводы автора работы.

Заключению следует уделить особое внимание, поскольку оно должно дать полное представление о проделанной работе. Нельзя его составлять путем компилирования текста (фраз и абзацев) выпускной квалификационной работы. Заключение должно еще раз подчеркнуть те результаты, которых студенту удалось достичь при выполнении исследования.

Список использованных источников должен содержать перечень всех источников (законов, нормативных документов, монографий, учебников и учебных пособий, статей и т. п.), используемых при выполнении выпускной квалификационной работы и на которые по тексту работы сделаны ссылки. Список должен содержать не менее 25 источников, изданных или опубликованных за последние пять лет.

Приложения – это дополнительные материалы: вспомогательные, дополняющие и иллюстрирующие содержание ВКР (таблицы, рисунки, схемы и другие информационные данные) которые по тем или иным причинам (например, из-за большого объема) нецелесообразно приводить в тексте

работы.

Перечень определений, обозначений и сокращений не является обязательным, если в выпускной квалификационной работе специальные термины, сокращения, символы, обозначения и т. п. используются не часто. В этом случае их расшифровку приводят в тексте работы при первом упоминании, например, центр научно-технической информации (ЦНТИ). Если в работе используется специфическая терминология, а также употребляются малораспространенные сокращения, новые обозначения, символы и т. п., то составляется их перечень в виде отдельного списка. Его располагают столбцом, в котором слева (в алфавитном порядке) приводят термины, определения и сокращения, справа – детальную расшифровку. Лист со списком помещают после содержания.

Законченные разделы выпускной квалификационной работы сдаются руководителю на проверку в сроки, предусмотренные календарным планом-графиком. Проверенные разделы дорабатываются в соответствии с полученными от руководителя замечаниями, после чего студент приступает к техническому оформлению работы.

2.3 Примерная тематика выпускных квалификационных работ

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

1. Разработка нормативно-правовой документации по информационной безопасности компании (на конкретном примере).
2. Разработка организационно-технических рекомендаций по повышению эффективности защиты конфиденциальной информации предприятия (на конкретном примере).
3. Разработка организационно-технических мер по защите информации, составляющей служебную тайну, предприятия (на конкретном примере).

4. Разработка предложений по созданию системы защиты информации предприятия централизованной структуры (на конкретном примере).
5. Разработка предложений по созданию защищенной информационной системы предприятия децентрализованной структуры (на конкретном примере).
6. Разработка организационно-технических мер защиты выделенного помещения предприятия (на конкретном примере).
7. Разработка рекомендаций руководителю предприятия по оборудованию помещения для проведения служебных совещаний (на конкретном примере).
8. Разработка модели комплексной системы защиты информации предприятия (на конкретном примере).
9. Оценка рисков и управление информационной безопасностью предприятия (на конкретном примере).
10. Разработка автоматизированной системы оценки информационных рисков предприятия (на конкретном примере).
11. Организация комплексной системы защиты конфиденциальной информации предприятия (на конкретном примере).
12. Разработка политики информационной безопасности на основе анализа информационных рисков предприятия (на конкретном примере).
13. Совершенствование нормативно-методической базы защиты конфиденциальной информации предприятия (на конкретном примере).
14. Разработка организационно-технических мер противодействия утечке информации по техническим каналам предприятия (на конкретном примере).
15. Разработка рекомендаций по совершенствованию защиты коммерческой тайны предприятия (на конкретном примере).
16. Разработка рекомендаций по совершенствованию защиты ресурсов автоматизированной системы предприятия (на конкретном примере).
17. Оценка эффективности системы защиты информации предприятия (на конкретном примере).

18. Разработка рекомендаций по проведению аудита информационной безопасности предприятия (на конкретном примере).
19. Разработка нормативно-методических документов по регламентации организационной защиты информации, обрабатываемой средствами вычислительной и организационной техники предприятия (на конкретном примере).
20. Разработка направлений, методов и нормативно-методических документов по организационной защите персональных данных предприятия (на конкретном примере).
21. Разработка предложений по реализации на предприятии комплекса мер противодействия утечки информации по скрытым информационным каналам.
22. Организация системы защиты электронного документооборота предприятия (на конкретном примере).
23. Разработка защищенного web-приложения.
24. Создание системы защиты АСУ ТП предприятия (на конкретном примере).
25. Информационная безопасность предприятия при реализации технологий индустриального интернета вещей (на конкретном примере).
26. Обеспечение безопасности веб-приложений.
27. Разработка защищенной автоматизированной подсистемы оформления заказов предприятия (на конкретном примере).
28. Разработка защищенной автоматизированной подсистемы оформления счетов на оплату клиентам предприятия (на конкретном примере).
29. Разработка защищенной автоматизированной системы оперативного контроля (на конкретном примере).
30. Разработка защищенной автоматизированной системы кадрового учета (на конкретном примере).
31. Разработка системы передачи идентификационных данных на сервер авторизации с применением технологии NFC.

32. Разработка защищенной системы для учета и оценки сотрудников в масштабе профессиональной отрасли.
33. Разработка защищенной системы верификации и импорта внешних данных в корпоративную систему учета.
34. Разработка крипто-плагина для браузера Яндекс.
35. Организация комплексно-технической системы защиты объекта коммерческой деятельности (на конкретном примере).
36. Модификация инфраструктуры высшего учебного заведения с целью выполнения требований законодательства в области защиты биометрических данных пользователей.
37. Разработка мер защиты информации ограниченного доступа в структурном подразделении вуза.
38. Модель подсистемы анализа ситуаций угроз безопасности и поддержки принятия решений.
39. Реализация гибридной криптосистемы на основе алгоритма AES
40. Разработка защищенного Android-приложения для обмена конфиденциальными данными.
41. Разработка политики безопасности высшего учебного заведения.
42. Разработка подсистемы охраны объекта на основе технологии «Умный дом» с автоматическим оповещением об инцидентах.

2.4 Порядок выполнения и предоставления выпускной квалификационной работы

После утверждения темы вместе с руководителем обучающийся составляет задание на выполнение выпускной квалификационной работы. Оно подписывается обучающимся, преподавателем-руководителем выпускной квалификационной работы и утверждается заведующим кафедрой.

Обучающийся:

– уточняет с руководителем круг вопросов, подлежащих изучению;

– составляет план исследования и календарный план работы на весь период с указанием очередности выполнения отдельных этапов;

– систематически работает над литературой по теме выпускной квалификационной работы;

– занимается сбором и анализом первичного материала;

– докладывает о ходе проекта руководителю и получает необходимую консультацию;

– по мере написания отдельных глав обучающийся представляет их руководителю, исправляет и дополняет проект в соответствии с полученными от руководителя замечаниями;

– в установленные сроки согласно заданию отчитывается перед руководителем о готовности проекта.

За достоверность информации и обоснованность принятых решений в выпускной квалификационной работе ответственность несет обучающийся.

Непосредственное и систематическое руководство за работой обучающийся, а возлагается на руководителя, который:

– выдает задание на выполнение выпускной квалификационной работы;

– оказывает обучающемуся помощь в разработке календарного графика на весь период выполнения выпускной квалификационной работы;

– рекомендует обучающемуся необходимую литературу по теме;

– проводит консультации в соответствии с утвержденным графиком;

– систематически контролирует ход работы и информирует кафедру о состоянии дел;

– дает подробный отзыв на законченную выпускную квалификационную работу.

В случае необходимости, из профессорско-преподавательского состава академии, специалистов предприятий и организаций соответствующей квалификации кафедра приглашает консультантов по отдельным разделам проекта в счет времени, выделенного на научное руководство проектом.

Завершенная выпускная квалификационная работа подписывается обучающемуся на титульном листе и представляется руководителю, который подписывает пояснительную записку и презентацию и дает письменный отзыв-заключение о выпускной квалификационной работе на стандартном бланке, в котором отражается:

– правильность понимания дипломником цели и задач, поставленных темой ВКР и степень их проработки;

– существенную новизну и наиболее интересные решения, практическую полезность ВКР (внедрение, использование в отчете по НИР, публикации и пр.);

– качество разработки и оформления ВКР;

– умение анализировать и делать обоснованные выводы и предложения;

– знания, навыки и отношение к ВКР, показанные во время выполнения ВКР;

– степень самостоятельности в решении поставленных в ВКР задач.

Руководитель в конце отзыва оценивает ВКР и делает заключение о подготовленности обучающегося к самостоятельной работе в качестве менеджера.

Рецензентами для ВКР могут быть высококвалифицированные специалисты, как по проблеме ВКР, так и в соответствующей отрасли, работающие на предприятиях, в организациях, высших учебных заведениях, научно-исследовательских и проектных институтах. Предпочтение отдается специалистам тех предприятий, где обучающийся проходит преддипломную практику. В рецензии на ВКР отмечается:

– актуальность темы;

– соответствие выполненной ВКР заданной теме;

– использование современных достижений науки и техники;

– оригинальность, новизна, глубина и обоснованность проектных решений;

– возможность практического применения полученных результатов;

– качество ВКР, слабые стороны и недостатки;

– общий вывод о ВКР, его оценка, мнение о возможности присвоения автору квалификации по направлению.

Рецензия заверяется на предприятии, где работает рецензент. Допускается рецензирование ВКР специалистом сторонней организации (предприятие, ВУЗ, научная организация). После рецензирования всякие исправления в работе не допускаются, свое несогласие с рецензией обучающийся может высказать в заключительном слове на защите ВКР. Выпускная квалификационная работа подлежит обязательной поверке в системе «Антиплагиат ВУЗ» на установление уровня заимствования текста.

Проверка выпускных квалификационных работ на объем и характер заимствования курсовых и выпускных квалификационных работ по направлениям подготовки / специальностям высшего образования является составной частью реализуемого в академии процесса контроля соблюдения академических норм при выполнении и защите выпускных квалификационных работ.

Проверка работ на наличие неправомерных заимствований осуществляется с помощью программных продуктов электронных систем проверки заимствований. При наличии в выпускной квалификационной работе менее 55 % оригинального текста, она отправляется на доработку при сохранении ранее установленной темы и после этого подвергается повторной проверке.

При повторной проверке выпускной квалификационной работы, имеющая менее 55% оригинального текста, в течение 3-х дней должна быть доработана при сохранении ранее установленной темы и после этого подвергается окончательной проверке. Если после проведения научным руководителем окончательной проверки уровень оригинальности не достигает установленного минимального рубежа в 55%, выпускная квалификационная работа не допускается к защите.

2.5 Порядок защиты выпускной квалификационной работы

Готовясь к защите выпускной квалификационной работы, дипломник совместно с руководителем подготавливает доклад на 10 мин. выступления, в котором отражает:

– актуальность темы;

– концепцию ВКР: теоретические и методические положения, на которых он базируется;

– результаты проведенного анализа изучаемой проблемы;

– конкретные предложения по решению проблемы или совершенствованию соответствующих процессов с обоснованием возможности их реализации в условиях конкретного предприятия: экономический, социальный и экологический эффекты от разработок.

Выступление не должно включать теоретические положения, заимствованные из литературных или нормативных документов, ибо они не являются предметом защиты. Особое внимание следует сосредоточить на собственных разработках.

Презентация к работе должна иллюстрировать доклад, поэтому слайды располагают в последовательности упоминания в докладе, чем больше увязаны между собой доклад и слайды, тем он содержательнее и нагляднее.

После выступления обучающегося, ответов им на заданные вопросы и оглашения отзыва руководителя и внешней рецензии дипломник отвечает на замечания рецензента.

3 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ИТОГОВОЙ АТТЕСТАЦИИ

3.1 Перечень результатов обучения при прохождении ИА, соотнесенных с планируемыми результатами освоения образовательной программы по направлению подготовки 10.03.01 Информационная безопасность направленность (профиль) образовательной программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)»

Итоговая аттестация призвана определить степень сформированности компетенций – теоретические знания и практические навыки выпускника в соответствии с компетентностной моделью выпускника. В частности, ИА проверяется уровень владения выпускниками компетенциями в области видов профессиональной деятельности, предусмотренных образовательным стандартом.

Результаты освоения ОПОП определяются приобретаемыми выпускником компетенциями, т. е. его способностью применять знания, умения, опыт и личностные качества в соответствии с задачами и видами профессиональной деятельности.

3.2 Планируемые результаты обучения в результате освоения основной профессиональной образовательной программы направлению подготовки 10.03.01 Информационная безопасность направленность (профиль) образовательной программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)»

Планируемые результаты обучения в результате освоения основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность направленность (профиль) образовательной программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)» представлены в таблице 3.1.

Критерии оценивания уровня сформированности компетенций проверяемых ИА приведены в таблице 3.2.

Таблица 3.1 – 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)»

Код компетенции	**Название компетенции**	**Индикаторы достижения компетенций**	***Перечень планируемых результатов обучения по результатам освоения ОПОП***
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.	Знать: принципы сбора, отбора и обобщения информации Уметь: соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности Владеть: навыками работы с информационными объектами и сетью Интернет, опыт библиографического разыскания, создания научных текстов
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	Знать: различные модели жизненного цикла и стандарты на представление этапов работы над проектом Уметь: использовать современные бизнес- и информационные технологии для реализации проектов на различных этапах жизненного цикла Владеть: навыками реализации проектов на разных этапах жизненного цикла

		задач в зоне своей ответственности в соответствии с запланированными результатами контроля, при необходимости корректирует способы решения задач.	
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.	Знать: различные приемы и способы социализации личности и социального взаимодействия Уметь: строить отношения с окружающими людьми, с коллегами Владеть: навыками командной работы, в социальных проектах, в шефской или волонтерской деятельности, навыками распределения ролей в условиях командного взаимодействия
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	Знать: литературную форму государственного языка, основы устной и письменной коммуникации на иностранном языке, функциональные стили родного языка, требования к деловой коммуникации Уметь: выражать свои мысли на государственном, родном и иностранном языке в ситуации деловой коммуникации Владеть: навыками самостоятельного изучения программных систем с помощью соответствующей документации

		официальных и неофициальных писем и социокультурных различий в формате корреспонденции. УК-4.4. Представляет свою точку зрения при деловом общении и в публичных выступлениях.	
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.	Знать: основные категории философии, законы исторического развития, основы межкультурной коммуникации Уметь: вести коммуникацию с представителями иных национальностей и конфессий с соблюдением этических и межкультурных норм Владеть: навыками анализа философских и исторических фактов, навыками эстетической оценки явлений культуры
УК-6	Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни	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 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	Знать: основные принципы самовоспитания и самообразования, профессионального и личностного развития, исходя из этапов карьерного роста и требований рынка труда Уметь: планировать свое рабочее время и время для саморазвития, формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, индивидуально-личностных особенностей Владеть: навыками составления плана последовательных шагов для достижения поставленной цели

		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.	Знать: основы здорового образа жизни, здоровьесберегающих технологий, физической культуры Уметь: выполнять комплекс физкультурных упражнений Владеть: средствами и методами укрепления индивидуального здоровья, физического самосовершенствования
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	Знать: классификацию и источники чрезвычайных ситуаций природного и техногенного происхождения, методы защиты в условиях чрезвычайных ситуаций, военных конфликтов; методы сохранения природной среды, факторы обеспечения устойчивого развития общества Уметь: обеспечивать условия труда на рабочем месте, безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций и военных конфликтов Владеть: методами прогнозирования возникновения опасных или чрезвычайных ситуаций и военных конфликтов; навыками по применению основных методов защиты в условиях чрезвычайных ситуаций и военных конфликтов в повседневной жизни и профессиональной деятельности

		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.	
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.	Знать: экономическую теорию, основные документы, регламентирующие экономическую деятельность, источники финансирования профессиональной деятельности, принципы планирования экономической деятельности Уметь: обосновывать принятие экономических решений, использовать методы экономического планирования для достижения поставленных целей Владеть: навыками применения экономических методов и инструментов для обоснования экономических решений, технико-экономического обоснования проектных решений
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.	Знать: действующие правовые нормы, обеспечивающие борьбу с проявлениями экстремизма, терроризма, коррупции в различных областях жизнедеятельности, способы противодействия им в профессиональной деятельности Уметь: формировать гражданскую позицию, обеспечивающую нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной

			деятельности Владеть: навыками взаимодействия в обществе на основе нетерпимого отношения к проявлениям экстремизма, терроризма, коррупционному поведению и противодействия им в профессиональной деятельности
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.	Знать: классификацию угроз информационной безопасности в соответствии с нормативными документами Уметь: оценивать угрозы информационной безопасности с точки зрения основных концепций национальной безопасности Российской Федерации Владеть: навыками определения угроз 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.	Знать: методы доступа к информационным ресурсам Уметь: пользоваться современными справочными и библиотечными системами и системами дистанционного образования, определять тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств Владеть: навыками работы с поисковыми машинами, справочными и библиотечными системами и системами дистанционного образования, навыками применения технических и программных средств тестирования с целью определения

			исправности компьютера и оценки его производительности
ОПК-3	Способен использовать необходимые математические методы для решения задач профессиональной деятельности	ОПК-3.1. Использует методы аналитической геометрии и векторной алгебры при решении прикладных задач. 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).	Знать: основные приемы решения математических задач; утверждения для обоснования выбираемых методов математического анализа и их следствия; основные понятия о погрешности вычислений; основные требования, предъявляемые к вычислительным схемам (корректность, устойчивость, сходимость); основные методы и алгоритмы численного интегрирования и дифференцирования; методы и алгоритмы теории обработки результатов эксперимента; содержание основных понятий дискретной математики; основные приемы работы с комбинаторными объектами, булевыми функциями, графами; возможности использования дискретной математики в будущей профессиональной деятельности; виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач, действующее законодательство и правовые нормы, регулирующие профессиональную деятельность; методы сжатия данных, методы контроля и коррекции ошибок; математические модели сигналов и процессов обработки информации. Уметь: применять инструментарий математического анализа при решении задач; анализировать способы решения поставленных задач; разработать алгоритм

			решения поставленной задачи; применять полученные знания к численному решению задач практики; использовать дискретную математику при проектировании сетей, разработке программного обеспечения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности; оценивать технические возможности и вырабатывать рекомендации по построению систем и сетей передачи информации общего и специального назначения. Владеть: навыками применения моделей вычислительной математики для решения прикладных задач; навыками работы с математическими методами и моделями компьютерной математики в рамках своей профессиональной деятельности; навыками работы с нормативно-правовой документацией; методами оценки эффективности систем связи с учетом факторов среды, класса защищенности передаваемой информации и других параметров систем связи.
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	Знать: базовые физические законы; принципы действия основных электрических устройств и электронных приборов, их эквивалентные схемы; современные средства автоматизированного проектирования ЭС; Уметь: формулировать задачу с

		электрических цепях.	использованием соответствующих физических законов; рассчитывать электрическую схему; использовать функциональные возможности САПР при исследовании и анализе параметров и характеристик ЭС. Владеть: методами экспериментального исследования параметров и характеристик электронных приборов; методами расчета электрических цепей; методами моделирования электронных средств в САПР;
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.	Знать: порядок разработки и содержания организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности; основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации. Уметь: разрабатывает проекты локальных правовых регламентирующих работу по обеспечению информационной безопасности; Владеть: навыками разработки организационно-распорядительных документов по защите конфиденциальной информации и персональных данных.
ОПК-6	Способен при решении	ОПК-6.1. Разрабатывает модели угроз и	Знать: модели угроз и модели нарушителя

	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	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.	объекта информатизации. Уметь: определять политику контроля доступа работников к информации ограниченного доступа; формулировать требования, предъявляемые к физической защите объекта и пропускному. Владеть: навыками разработки проектов инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа.
ОПК-7	Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности	ОПК-7.1. Разрабатывает с помощью языков высокого уровня алгоритмы решения типовых профессиональных задач. ОПК-7.2. Разрабатывает программы для работы с файлами как с источником данных. ОПК-7.3. Отлаживает разработанные программные средства.	Знать: основные спецификации программного обеспечения при структурном и объектном подходах; основы работы с файловой системой с использованием относительных путей; основы работы в режиме пошаговой отладки приложения. Уметь: проектировать структуры для учета данных; контролировать целостность источника данных; выполнять отладку приложения в пошаговом режиме и с контрольными точками. Владеть: навыками программирования на языке высокого уровня; навыками инициализации базы данных; методами отладки программных модулей.
ОПК-8	Способен осуществлять подбор, изучение и обобщение научно-	ОПК-8.1. Составляет рефераты по результатам обзора научно-технической литературы, нормативных и методических документов.	Знать: стандарты и локальные нормативы представления результатов исследования в отчетах, рефератах, публикациях и

	технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-8.2. Систематизирует научную информацию в области информационной безопасности. ОПК-8.3. Использует информационно-справочные системы при поиске информации в области профессиональной деятельности.	презентациях; Уметь: систематизировать научную информацию в области информационной безопасности. Владеть: опытом использования информационно-справочных 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.	Знать: классификацию криптографических методов защиты информации; модель криптосистемы с открытым ключом; способы защиты информации от утечки по техническим каналам на объектах информатизации; угрозы информационной безопасности объекта информатизации; средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации. Уметь: выполнять шифрование криптографическими методами; решать задачи с использованием криптографических систем с открытым ключом; защищать информацию от утечки по техническим каналам на объектах информатизации; оценивать угрозы информационной безопасности объекта информатизации; использовать средства защиты информации от утечки по техническим каналам. Владеть: навыками автоматизации этапов криптографического преобразования; способами защиты информации от утечки по техническим каналам на объектах

			информатизации; навыками использования средств защиты информации от утечки по техническим каналам.
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.	Знать: требования политик безопасности на объектах информатизации; Уметь: применять средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях. Владеть: навыками конфигурирования программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности.
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.	Знать: стандартные процедуры принятия решений на основе имеющихся экспериментальных данных; стандартные вероятностно-статистические методы экспериментальных данных; порядок сбора, анализа и систематизации информации по заданной методике; методы обработки результатов физического эксперимента. Уметь: использовать программный инструментарий статистической обработки данных; формулировать выводы по результатам исследования. Владеть: навыкам проведения экспериментов; навыками формулирования выводов по результатам исследования.
ОПК-12	Способен проводить	ОПК-12.1. Определяет информационную	Знать: порядок подготовки исходных

	подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	инфраструктуру и информационные ресурсы организации, подлежащие защите. 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.	данных для проектирования подсистем, средств обеспечения защиты информации. Уметь: оценивать информационные риски в автоматизированных системах. Владеть: навыками анализа показатели качества и критерии оценки систем и отдельных методов и средств защиты информации.
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.	Знать: этапы и закономерности исторического развития России. Уметь: соотносить общие исторические процессы и отдельные факты. Владеть: навыки выявления существенных черт исторических процессов, явлений и событий.
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	Знать: организационные мероприятия по обеспечению безопасности информации в автоматизированных системах. Уметь: определять подлежащие защите информационные ресурсы автоматизированных систем; разрабатывать документы, определяющие правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации. Владеть: навыками организации работы персонала автоматизированной системы с

		защиты информации в информационной системе в ходе ее эксплуатации.	учетом требований по защите информации.
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.	Знать: полномочия пользователей автоматизированной системы. Уметь: настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации. Владеть: навыками управления программными средствами обеспечения безопасности данных.
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.	Знать: порядок настройки администрирования и проверки работоспособности программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации. Уметь: устранять известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации. Владеть: программными средствами резервирования и восстановления информации в автоматизированных системах.
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.	Знать: порядок применения инструментальных средств контроля защищенности информации в автоматизированных системах. Уметь: документировать действия по устранению неисправностей в работе системы защиты информации

		ОПК-4.4.3. Регистрирует события, связанные с защитой информации в автоматизированных системах.	автоматизированной системы. Владеть: навыками регистрации событий, связанных с защитой информации в автоматизированных системах.
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 реализуемыми процедурами обеспечения информационной безопасности.	Знать: процедуры обеспечения информационной безопасности. Уметь: внедрять в состав автоматизированных систем средств обеспечения информационной безопасности. Владеть: навыками эксплуатации средств обеспечения информационной безопасности автоматизированных систем.
ПК-2	Способен реализовывать политики безопасности с использованием инструментальных средств обеспечения информационной безопасности.	ПК-2.1 Формулирует критерии безопасности обработки 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. ПК-2.5 Устанавливает программное обеспечение в соответствии с требованиями по защите информации.	Знать: политики информационной безопасности; критерии безопасности обработки информации в автоматизированных системах. Уметь: определять состав средств, необходимый для управления автоматизированными системами и средствами их защиты от НСД. Владеть: навыками установки и настройки технических средств для управления автоматизированными системами и средствами их защиты от НСД.
ПК-3	Способен обеспечивать безопасную обработку данных в	ПК-3.1 Фиксирует возникновение инцидентов информационной безопасности. ПК-3.2 Использует методы и средства	Знать: порядок действий при возникновении инцидентов информационной безопасности. Уметь: устранять уязвимости в

	автоматизированных системах.	резервного копирования информации. ПК-3.3 Устраняет уязвимости в автоматизированной системе. ПК-3.4 Соотносит изменения в конфигурации автоматизированной системы с её защищенностью.	автоматизированной системе. Владеть: средства резервного копирования информации.
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.	Знать: состав технической и проектной документации по вопросам создания и эксплуатации автоматизированных систем. Уметь: разрабатывать проектные документы на средства защиты информации создаваемых автоматизированных систем. Владеть: навыками проектирования автоматизированных систем в защищенном исполнении.
ПК-5	Способен выполнять работы по обеспечению информационной безопасности автоматизированных систем на всех этапах их жизненного цикла.	ПК-5.1 Проверяет соответствие внедряемых решений и средств для обеспечения информационной безопасности требованиям реализуемой политики безопасности. ПК-5.2 Восстанавливает работоспособность автоматизированных систем после инцидентов информационной безопасности. ПК-5.3 Проводит операции вывода защищённых автоматизированных систем из эксплуатации.	Знать: требования политик безопасности; порядок вывода защищённых автоматизированных систем из эксплуатации. Уметь: восстанавливать работоспособность автоматизированных систем после инцидентов информационной безопасности. Владеть: навыками работы по обеспечению информационной безопасности автоматизированных систем на всех этапах их жизненного цикла.
ПК-6	Способен документально оформлять работы по	ПК-6.1 Анализирует полноту и нормативным требованиям руководящих документов,	Знать: требования руководящих документов, по обеспечению информационной

	обеспечению информационной безопасности.	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 требованиями 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.	безопасности. Уметь: формировать отчётные и руководящие документы для обеспечения защиты информации в информационной системе в ходе ее эксплуатации. Владеть: навыками подготовки документов для проведения работ по аттестации объектов информатизации и автоматизированных систем.
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.	Знать: целевые показатели функционирования защищенных автоматизированных систем. Уметь: определять уровень защищённости автоматизированных систем. Владеть: навыками анализа уязвимостей автоматизированных систем в соответствии с нормативными документами.
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	Знать: методическую, техническую, рекомендательную и отчётную документацию по анализу защищённости автоматизированной системы. Уметь: проводить контроль защищённости и функционирования программно-аппаратных и технических средств автоматизированной системы. Владеть: навыками подбора программных средств тестирования защищённости

		программных и аппаратных платформ узлов автоматизированной системы. ПК-8.4 Проводит контроль защищённости и функционирования программно-аппаратных и технических средств автоматизированной системы.	автоматизированной системы в зависимости от предъявляемым к ней требованиям.
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.	Знать: правила работы персонала со средствами защиты информации. Уметь: сопоставлять результат работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации. Владеть: навыками распределения обязанностей и полномочий персонала, обслуживающего защищённую автоматизированную систему.
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 автоматизированных систем.	Знать: характеристики систем и средств защиты информации; меры защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности. Уметь: обосновывать необходимость модернизации системы защиты информации автоматизированной системы. Владеть: навыками формулирования правил протоколирования результатов мониторинга безопасности автоматизированных систем.

Таблица 3.2 - Критерии оценивания уровня сформированности компетенций проверяемых ИА

Код компетенции	**Показатели оценивания компетенций**	**Критерии и шкала оценивания компетенций**			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
УК-1	Системное и критическое мышление	Не способен без помощи преподавателя анализировать задачи, определять информацию, требуемую для решения поставленной задачи, формировать собственное мнение, анализировать пути решения проблем мировоззренческого, нравственного и личностного характера.	Осуществляет элементарный анализ поставленных задач. Определяет минимум информации, требуемой для решения поставленной задачи. Формирует собственные мнения и простейшие суждения, недостаточно полно аргументирует свои выводы. Предлагает наиболее очевидные пути решения проблем мировоззренческого, нравственного и личностного характера.	Грамотно анализирует поставленные задачи. Определяет необходимую и достаточную информацию, требуемую для решения поставленной задачи. Развернуто формирует собственные мнения и суждения, в том числе сложные, аргументирует свои выводы. Мотивированно выбирает пути решения проблем мировоззренческого, нравственного и личностного характера.	Всесторонне анализирует задачу, выделяя ее базовые составляющие. Исчерпывающе определяет и правильно ранжирует информацию, требуемую для решения поставленной задачи. Оперативно и технично осуществляет поиск информации в различных источниках для решения поставленной задачи по различным типам запросов. При обработке информации безошибочно отличает факты от мнений, интерпретаций, оценок, конструктивно формирует собственные мнения и суждения, убедительно аргументирует свои выводы, в том числе с применением

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
					философского понятийного аппарата. Тщательно анализирует пути решения проблем собственные мнения и суждения, убедительно аргументирует свои вы воды, в том числе с применением философского понятийного аппарата. Тщательно анализирует пути решения проблем мировоззренческого, нравственного и личностного характера на основе использования основных философских идей и категорий в их историческом развитии и социально-культурном контексте.
УК-2	Разработка и реализация проектов	Не может самостоятельно сформулировать проблему, решение которой напрямую связано с достижением цели проекта. Затрудняется в	Приблизительно формулирует проблему, решение которой напрямую связано с достижением цели проекта. Понимает логическую связь между	Формулирует проблему, решение которой связано с достижением цели проекта. Правильно определяет большинство связей между поставленными	Точно формулирует проблему, решение которой напрямую связано с достижением цели проекта. Четко и полно определяет все имеющиеся связи между поставленными задачами

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
		определении связи между поставленными задачами и ожидаемыми результатами их решения. Нарушает план-график реализации проекта. Не может самостоятельно определить имеющиеся ресурсы и ограничения, действующие правовые нормы. Не понимает зону своей ответственности в решении поставленных задач.	поставленными задачами и ожидаемыми результатами их решения, но определяет их неполно и (или) неточно. Соблюдает план-график реализации проекта. Определяет необходимые ресурсы и основные действующие правовые нормы. Применяет наиболее простые способы решения задач в зоне своей ответственности.	задачами и ожидаемыми результатами их решения. Верно анализирует план-график реализации проекта в целом и выбирает приемлемый способ решения поставленных задач. Правильно определяет имеющиеся ресурсы и ограничения, действующие правовые нормы. Выбирает наиболее эффективные способы решения задач в зоне своей ответственности.	и ожидаемыми результатами их решения. Досконально анализирует план-график реализации проекта в целом и выбирает оптимальный способ решения поставленных задач. В рамках поставленных задач в полном объеме определяет имеющиеся ресурсы и ограничения, действующие правовые нормы. Правомерно оценивает решение поставленных задач в зоне своей ответственности в соответствии с запланированными результатами контроля, при необходимости быстро корректирует способы решения задач.
УК-3	Командная работа и лидерство	Не выполняет свою роль в команде. Не замечает особенности поведения	Выполняет свою роль в команде, но часто нуждается в помощи. Понимает особенности	Ответственно выполняет свою роль в команде. Учитывает наиболее	Тактично определяет свою роль в команде, исходя из стратегии сотрудничества для

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
		других членов команды. Не задумывается о возможных последствиях личных действий. Не заинтересован в обмене информацией, знаниями и опытом с членами команды. Нарушает установленные нормы и правила командной работы, перекладывает ответственность за общий результат на других членов команды.	поведения других членов команды, предпринимает попытки учитывать их. Предвидит не все возможные последствия личных действий. Пассивно участвует в обмене информацией, знаниями и опытом с членами команды. Соблюдает установленные нормы и правила командной работы, не всегда готов нести личную ответственность за общий результат.	явные особенности поведения других членов команды. Анализирует возможные последствия личных действий и корректирует их по необходимости. Результативно делится информацией, знаниями и опытом с членами команды, в целом справедливо оценивает идеи других членов команды для достижения поставленной цели. Соблюдает установленные нормы и правила командной работы, несет личную ответственность за общий результат.	достижения поставленной цели. При реализации своей роли в команде психологически точно учитывает особенности поведения других членов команды. Обстоятельно анализирует возможные последствия личных действий и планирует свои действия для достижения заданного результата. Активно и продуктивно осуществляет обмен информацией, знаниями и опытом с членами команды, доброжелательно и корректно оценивает идеи других членов команды для достижения поставленной цели. Безукоризненно соблюдает установленные нормы и правила командной работы, несет полную личную ответственность

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
					за общий результат.
УК-4	Коммуникация	На государственном языке РФ изъясняется, допуская грубые речевые ошибки; не владеет официально-деловым стилем речи. Не способен осуществлять деловое общение на иностранном языке и переводы профессиональных деловых текстов с иностранного языка на государственный язык РФ. Не владеет навыками ведения деловой переписки на государственном языке РФ и иностранном языке. Не способен в монологической речи сформулировать простейшие суждения, выводы, оценки, изложить свою точку зрения.	Осуществляет деловое общение на государственном языке РФ и иностранном языке, но допускает негрубые логические и (или) речевые ошибки. Выполняет перевод со словарем несложных профессиональных деловых текстов с иностранного языка на государственный язык РФ и с государственного языка РФ на иностранный. Ведет элементарную деловую переписку на государственном языке РФ и иностранном языке. Излагает в устной и письменной форме свои суждения, выводы, оценки, свою точку зрения, но ограничен в речевых средствах.	Свободно осуществляет деловое общение на государственном языке РФ и иностранном языке исходя из особенностей конкретных ситуаций взаимодействия. Выполняет переводы со словарем профессиональных деловых текстов с иностранного языка на государственный язык РФ и с государственного языка РФ на иностранный. Самостоятельно ведет обычную деловую переписку на государственном языке РФ и иностранном языке. Аргументированно представляет свою точку зрения при	Корректно выбирает стиль делового общения на государственном языке РФ и иностранном языке в зависимости от цели и условий партнерства; уместно адаптирует речь, стиль общения и язык жестов к ситуациям взаимодействия. Самостоятельно переводит профессиональные деловые тексты (в том числе сложные) с иностранного языка на государственный язык РФ и с государственного языка РФ на иностранный. Уверенно ведет деловую переписку на государственном языке РФ и иностранном языке с учетом особенностей стилистики официальных и неофициальных писем и

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
				деловом общении и в публичных выступлениях.	социокультурных различий в формате корреспонденции. Ясно, точно, убедительно и ярко представляет свою точку зрения при деловом общении и в публичных выступлениях.
УК-5	Межкультурное взаимодействие	Слабо ориентируется в истории России, не соотносит ее с мировым историческим развитием. Не разбирается в межэтнических, межконфессиональных и социальных различиях. Допускает неэтичное поведение (неэтичные высказывания) при общении с представителями других народов, социальных групп, конфессий.	Обладает общим представлением об истории России в контексте мирового исторического развития. Ориентируется в основных социокультурных традициях различных социальных групп, этносов и конфессий, мировых религиях, наиболее известных философских и этических учениях. Проявляет толерантность при личном и массовом профессиональном общении с	Осуществляет попытки самостоятельной интерпретации истории России в контексте мирового исторического развития. Достаточно свободно ориентируется в социокультурных традициях различных социальных групп, этносов и конфессий, мировых религиях, философских и этических учениях. Демонстрирует недискриминационное поведение при личном и массовом общении с	Интересно и доказательно интерпретирует историю России в контексте мирового исторического развития. Максимально учитывает при социальном и профессиональном общении историческое наследие и социокультурные традиции различных социальных групп, этносов и конфессий, включая мировые религии, философские и этические учения. Безукоризненно придерживается принципов

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
			представителями различных социальных групп, этносов и конфессий в целях выполнения профессиональных задач.	представителями других народов, социальных групп, конфессий в целях выполнения профессиональных задач и усиления социальной интеграции.	недискриминационного взаимодействия при личном и массовом общении в целях выполнения профессиональных задач и усиления социальной интеграции.
УК-6	Самоорганизация и саморазвитие (в том числе здоровьесбережение)	Не способен организовать свою учебную и профессиональную деятельность без помощи руководителя. Не занимается саморазвитием и самообразованием.	Правильно распределяет свое время при выполнении конкретных задач, проектов, при достижении поставленных целей. Ставит перед собой наиболее общие задачи саморазвития и профессионального роста на краткосрочный период. Нерегулярно занимается саморазвитием в профессиональной области.	Использует основные инструменты и методы управления временем при выполнении конкретных задач, проектов, при достижении поставленных целей. Ставит перед собой задачи саморазвития и профессионального роста на средне- и краткосрочный период. Понимает значимость непрерывного образования (образования в течение всей жизни), постоянно занимается	Эффективно использует инструменты и методы управления временем при выполнении конкретных задач, проектов, при достижении поставленных целей. Рационально определяет конкретные задачи саморазвития и профессионального роста, распределяет их на долго-, средне- и краткосрочные с обоснованием актуальности и определением необходимых ресурсов для их выполнения. Успешно использует

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
				самообразованием и саморазвитием.	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	Самоорганизация и саморазвитие (в том числе здоровьесбережение)	Пренебрегает условиями здоровьесберегающими технологиями и здоровым образом жизни. Не заботится о чередовании физической и умственной нагрузки для обеспечения собственной работоспособности.	Демонстрирует приверженность здоровому образу жизни. Чередует физическую и умственную нагрузку для обеспечения собственной работоспособности. Соблюдает нормы здорового образа жизни в различных жизненных ситуациях и в профессиональной деятельности.	Подробно разбирается в здоровьесберегающих технологиях, сознательно выбирает здоровый образ жизни. Разумно чередует физическую и умственную нагрузку для обеспечения собственной работоспособности. Строго соблюдает нормы здорового образа жизни в различных жизненных	Сознательно и добровольно выбирает здоровьесберегающие технологии для поддержания здорового образа жизни с учетом физиологических особенностей организма. Идеально планирует свое рабочее и свободное время для оптимального сочетания физической и умственной нагрузки и обеспечения работоспособности. Образцово соблюдает и убежденно

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
				ситуациях и в профессиональной деятельности.	пропагандирует нормы здорового образа жизни в различных жизненных ситуациях и в профессиональной деятельности
УК-8	Безопасность жизнедеятельности	Затрудняется в анализе простейших факторов вредного влияния на жизнедеятельность элементов среды обитания и идентифицировать опасные и вредные факторы в рамках осуществляемой деятельности. Не может определить проблемы, связанные с нарушениями техники безопасности на рабочем месте. Не может составить перечень необходимых мероприятий по предотвращению ЧС, разъяснить правила поведения при возникновении ЧС природного и	Определяет очевидные факторы вредного влияния на жизнедеятельность элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений). Идентифицирует некоторые опасные и вредные факторы в рамках осуществляемой деятельности. Выявляет основные проблемы, связанные с нарушениями техники безопасности на рабочем месте; предлагает основные	Развернуто анализирует основные факторы вредного влияния на жизнедеятельность элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений). В целом правильно идентифицирует опасные и вредные факторы в рамках осуществляемой деятельности. Выявляет большинство проблем, связанных с нарушениями техники	Досконально анализирует факторы вредного влияния на жизнедеятельность элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений). Точно идентифицирует опасные и вредные факторы в рамках осуществляемой деятельности. В полном объеме выявляет проблемы, связанные с нарушениями техники безопасности на рабочем месте; предлагает наиболее эффективные

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
		техногенного происхождения, оказать первую помощь, описать способы участия в восстановительных мероприятиях.	мероприятия по предотвращению ЧС. Разъясняет элементарные правила поведения при возникновении ЧС природного и техногенного происхождения; оказывает первую помощь в простейших случаях, описывает некоторые способы участия в восстановительных мероприятиях.	безопасности на рабочем месте; предлагает достаточные мероприятия по предотвращению ЧС. Разъясняет основные правила поведения при возникновении ЧС природного и техногенного происхождения; правильно оказывает первую помощь в большинстве случаев, описывает основные способы участия в восстановительных мероприятиях.	мероприятия по предотвращению ЧС. Доходчиво и полно разъясняет правила поведения при возникновении ЧС природного и техногенного происхождения; уверенно оказывает первую помощь, подробно описывает всевозможные способы участия в восстановительных мероприятиях.
УК-9	Экономическая культура, в том числе финансовая грамотность	Не может принимать обоснованных экономических решений в различных областях жизнедеятельности по причине отсутствия (недостаточности) знаний принципов функционирования экономики и	Понимает основные принципы функционирования экономики и экономического развития, цели и некоторые формы участия государства в экономике. Применяет наиболее распространенные	Правильно понимает базовые принципы функционирования экономики и экономического развития, цели и различные формы участия государства в экономике. Обоснованно применяет методы	Глубоко понимает базовые принципы функционирования экономики и экономического развития, цели и различные формы участия государства в экономике. Эффективно применяет методы личного

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
		экономического развития, форм участия государства в экономике, методов личного экономического и финансового планирования, финансовых инструментов для управления личными финансами.	методы личного экономического и финансового планирования для достижения текущих и долгосрочных финансовых целей, использует широко известные финансовые инструменты для управления личными финансами (личным бюджетом), спонтанно контролирует собственные экономические и финансовые рынки.	личного экономического и финансового планирования для достижения текущих и долгосрочных финансовых целей, использует широкодоступные финансовые инструменты для управления личными финансами (личным бюджетом), системно осуществляет контроль собственных экономических и финансовых рынков.	экономического и финансового планирования для достижения текущих и долгосрочных финансовых целей, использует всевозможные финансовые инструменты для управления личными финансами (личным бюджетом), результативно контролирует собственные экономические и финансовые рынки.
УК-10	Гражданская позиция	Не понимает правовых последствий коррупционной деятельности, в том числе собственных действий или бездействий.	Предвидит основные правовые последствия коррупционной деятельности, в том числе собственных действий или бездействий. Выбирает правомерные формы взаимодействия с гражданами, структурами гражданского общества	Грамотно анализирует правовые последствия коррупционной деятельности, в том числе собственных действий или бездействий. Выбирает правомерные формы взаимодействия с гражданами, структурами	Безошибочно и обстоятельно анализирует правовые последствия коррупционной деятельности, в том числе собственных действий или бездействий. Добровольно и сознательно выбирает правомерные формы

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
			и органами государственной власти в типовых ситуациях.	гражданского общества и органами государственной власти в типовых ситуациях.	взаимодействия с гражданами, структурами гражданского общества и органами государственной власти в типовых ситуациях.
ОПК-1	Теоретические и практические основы профессиональной деятельности	Не классифицирует угрозы информационной безопасности в соответствии с нормативными документами, не даёт некоторые качественные и количественные оценки угроз информационной безопасности, не определяет угрозы информационной безопасности для различных систем	Классифицирует наиболее распространённые угрозы информационной безопасности в соответствии с нормативными документами, даёт некоторые качественные и количественные оценки угроз информационной безопасности, определяет некоторые угрозы информационной безопасности для различных систем	Грамотно классифицирует угрозы информационной безопасности в соответствии с нормативными документами, оценивает угрозы информационной безопасности, определяет угрозы информационной безопасности для различных систем	Информативно и понятно классифицирует угрозы информационной безопасности в соответствии с нормативными документами, оценивает угрозы информационной безопасности с точки зрения основных концепций национальной безопасности Российской Федерации, точно и обоснованно определяет угрозы информационной безопасности для различных систем
ОПК-2	Информационно коммуникационные технологии для	Не способен применять современные информационные технологии, в том числе	Способен применять современные информационные технологии, в том	Способен самостоятельно применять современные	Способен самостоятельно применять современные информационные

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	Пороговый уровень	Продвинутый уровень	Высокий уровень
	профессиональной деятельности	и отечественные, при проведении работ по обеспечению информационной безопасности при условии консультаций и под руководством специалиста.	числе и отечественные, при проведении работ по обеспечению информационной безопасности, но требует руководства.	информационные технологии, в том числе и отечественные, при проведении работ по обеспечению информационной безопасности	технологии, в том числе и отечественные, при проведении работ по обеспечению информационной безопасности, находить наиболее эффективные пути их применения
ОПК-3	Теоретические и практические основы профессиональной деятельности	Не способен применять современный математический аппарат, связанный с проведением работ по обеспечению информационной безопасности даже при условии консультаций и под руководством специалиста.	Способен применять современный математический аппарат, связанный с проведением работ по обеспечению информационной безопасности, но требует руководства.	Способен самостоятельно применять современный математический аппарат, связанный с проведением работ по обеспечению информационной безопасности.	Способен самостоятельно применять современный математический аппарат при проведении работ по обеспечению информационной безопасности находить наиболее эффективные пути их использования.
ОПК-4	Теоретические и практические основы профессиональной деятельности	Не способен решать базовые прикладные физические задачи, анализировать электрические цепи в переходных и установившихся режимах в частотной и временной областях, анализировать процессы,	Под руководством решает базовые прикладные физические задачи, анализирует электрические цепи в переходных и установившихся режимах в частотной и временной областях, анализирует процессы,	Самостоятельно решает базовые прикладные физические задачи, анализирует электрические цепи в переходных и установившихся режимах в частотной и временной областях, анализирует	Самостоятельно и на высоком научном уровне решает базовые прикладные физические задачи, анализирует электрические цепи в переходных и установившихся режимах в частотной и временной областях, анализирует процессы,

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
		протекающие в линейных и нелинейных электрических цепях	протекающие в линейных и нелинейных электрических цепях	процессы, протекающие в линейных и нелинейных электрических цепях	протекающие в линейных и нелинейных электрических цепях
ОПК-5	Правовые основы обеспечения информационной безопасности	Не способен разработать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации, сформулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации, сформулировать основные требования	Под руководством разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации, формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации, формулирует основные требования при лицензировании	Самостоятельно разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации, формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации,	Самостоятельно и на высоком уровне разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации, формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации, формулирует основные требования при

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
		при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации	деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации	формулирует основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации	лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации
ОПК-6	Правовые основы обеспечения информационной безопасности	Не способен даже под руководством использовать нормативные и правовые акты для обеспечения безопасности профессиональной деятельности, разрабатывать модели угроз и модели нарушителя объекта информатизации	Допускает ошибки при использовании нормативных правовых актов для обеспечения безопасности профессиональной деятельности, при разработке модели угроз и модели нарушителя объекта информатизации.	Использует нормативные правовые акты для обеспечения безопасности профессиональной деятельности, разрабатывает модели угроз и модели нарушителя объекта информатизации.	Грамотно и самостоятельно использует нормативные правовые акты для обеспечения безопасности профессиональной деятельности в нестандартных ситуациях, разрабатывает модели угроз и модели нарушителя объекта информатизации
ОПК-7	Информационно-коммуникационные технологии для	Не способен применять современные информационные технологии, в том числе и отечественные, при	Способен применять современные информационные технологии, в том числе и отечественные,	Способен самостоятельно применять современные информационные	Способен самостоятельно применять современные информационные технологии, в том числе

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
	профессиональной деятельности	создании программных продуктов и программных комплексов различного назначения даже при условии консультаций и под руководством специалиста.	при создании программных продуктов и программных комплексов различного назначения, но требует руководства.	технологии, в том числе и отечественные, при создании программных продуктов и программных комплексов различного назначения	и отечественные, при создании программных продуктов и программных комплексов различного назначения и находить наиболее эффективные пути их применения
ОПК-8	Профессиональное мышление	Не составляет рефераты по результатам обзора научно-технической литературы, нормативных и методических документов, не может даже при руководстве систематизировать научную информацию в области информационной безопасности, не использует доступные информационно-справочные системы при поиске информации в области профессиональной деятельности	С недочётами и не в полном объёме составляет рефераты по результатам обзора научно-технической литературы, нормативных и методических документов, допускает ошибки при систематизации научной информации в области информационной безопасности, использует не все доступные информационно-справочные системы при поиске	Самостоятельно составляет рефераты по результатам обзора научно-технической литературы, нормативных и методических документов, систематизирует научную информацию в области информационной безопасности, использует информационно-справочные системы при поиске информации в области профессиональной	Самостоятельно и в полном объёме составляет рефераты по результатам обзора научно-технической литературы, нормативных и методических документов, точно систематизирует научную информацию в области информационной безопасности, грамотно использует информационно-справочные системы при поиске информации в области профессиональной

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
			информации в области профессиональной деятельности	деятельности	деятельности
ОПК-9	Профессиональное мышление	Не способен даже под руководством использовать средства криптографической защиты информации в автоматизированных системах, решает задачи криптографической защиты информации, организовывать защиту информации от утечки по техническим каналам на объектах информатизации, использовать средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	Неэффективно использует средства крипто- графической защиты информации в автоматизированных системах, решает задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов, организует защиту информации от утечки по техническим каналам на объектах информатизации, использует средства защиты информации от утечки по техническим каналам и контроля	Самостоятельно использует средства криптографической защиты информации в автоматизированных системах, решает задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов, организует защиту информации от утечки по техническим каналам на объектах информатизации, использует средства защиты информации	Самостоятельно и эффективно использует средства криптографической защиты информации в автоматизированных системах, решает задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов, организует защиту информации от утечки по техническим каналам на объектах информатизации, использует средства защиты информации от утечки по техническим каналам и контроля

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
			эффективности защиты информации	от утечки по техническим каналам и контроля эффективности защиты информации	эффективности защиты информации
ОПК-10	Готовность применять знания, умения, навыки, личностные качества и опыт в самостоятельной эксплуатационной деятельности	Не реализует требования политик безопасности на объектах информатизации, не конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности, не может применить средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	Неэффективно реализует требования политик безопасности на объектах информатизации, конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности, применяет средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	Самостоятельно реализует требования политик безопасности на объектах информатизации, конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности, применяет средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	Самостоятельно и эффективно реализует требования политик безопасности на объектах информатизации, конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности, применяет средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях
ОПК-11	Готовность применять знания, умения, навыки,	Не реализует требования политик безопасности на объектах	Реализует требования политик безопасности на объектах информатизации лишь	Самостоятельно реализует требования политик безопасности на объектах	Самостоятельно и с применением всего стека технологий реализует требования политик

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
	личностные качества и опыт в самостоятельной эксплуатационной деятельности	информатизации лишь даже под руководством, не конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности, не способен применять средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	под руководством, с ошибками конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности, неэффективно применяет средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	информатизации, конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности, применяет средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	безопасности на объектах информатизации, корректно конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности, эффективно применяет средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях
ОПК-12	Готовность применять знания, умения, навыки, личностные качества и опыт в самостоятельной экспериментально-исследовательской деятельности	Не способен под непосредственным руководством строить стандартные процедуры принятия решений на основе имеющихся экспериментальных данных, использовать стандартные вероятностно-статистические методы анализа	Под непосредственным руководством строит стандартные процедуры принятия решений на основе имеющихся экспериментальных данных, допускает ошибки даже при использовании стандартных вероятностно-	Самостоятельно строит стандартные процедуры принятия решений на основе имеющихся экспериментальных данных, использует стандартные вероятностно-статистические методы анализа экспериментальных	Самостоятельно и на высоком уровне строит процедуры принятия решений на основе имеющихся экспериментальных данных, использует вероятностно-статистические методы анализа экспериментальных данных, проводить

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
		экспериментальных данных, проводить физический эксперимент и обрабатывать результаты физического эксперимента лишь в составе коллектива исполнителей	статистических методов анализа экспериментальных данных, проводит физический эксперимент и обрабатывает результаты физического эксперимента лишь в составе коллектива исполнителей	данных, проводить физический эксперимент, обрабатывает результаты физического эксперимента	физический эксперимент на высоком научном уровне, грамотно обрабатывает результаты физического эксперимента
ОПК-13	Готовность применять знания, умения, навыки, личностные качества и опыт в самостоятельной проектно-технологической деятельности	Допускает грубые ошибки при определении информационной инфраструктуры и информационных ресурсов организации, подлежащих защите, не анализирует даже наиболее часто используемые показатели качества и критерии оценки систем и отдельных методов и средств защиты информации, не оценивает информационные риски	Определяет информационную инфраструктуру и информационные ресурсы организации, подлежащие защите, анализирует наиболее часто используемые показатели качества и критерии оценки систем и отдельных методов и средств защиты информации, приблизительно оценивает информационные риски в автоматизированных системах и отдельные	Самостоятельно определяет информационную инфраструктуру и информационные ресурсы организации, подлежащие защите, анализирует основные показатели качества и критерии оценки систем и отдельных методов и средств защиты информации, оценивает информационные риски в автоматизированных системах и	Самостоятельно и точно определяет информационную инфраструктуру и информационные ресурсы организации, подлежащие защите, грамотно анализирует показатели качества и критерии оценки систем и методов и средств защиты информации, корректно оценивает информационные риски в автоматизированных системах и разрабатывает адекватные показатели

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
		в автоматизированных системах и отдельные показатели технико-экономического обоснования соответствующих типовых решений	показатели технико-экономического обоснования соответствующих проектных решений	разрабатывает основные показатели технико-экономического обоснования соответствующих проектных решений	технико-экономического обоснования соответствующих проектных решений
ОПК-4.1	Готовность применять знания, умения, навыки, личностные качества и опыт в самостоятельной организационно-управленческой деятельности	Не способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами.	Самостоятельно организует технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами, но требует руководства.	Самостоятельно организует технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами.	Самостоятельно организует технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами на сложных и нетиповых объектах информатизации.
ОПК-4.2	Готовность применять знания, умения, навыки, личностные качества и опыт в самостоятельной	Не способен выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления	Выполняет задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных,	Самостоятельно выполняет выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем,	Самостоятельно выполняет комплекс задач администрирования подсистем информационной безопасности операционных систем,

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
	эксплуатационной деятельности	базами данных, компьютерных сетей.	компьютерных сетей, но требует руководства.	систем управления базами данных, компьютерных сетей.	систем управления базами данных, компьютерных сетей с использованием полного спектра средств администрирования и защиты информации.
ОПК-4.3	Готовность применять знания, умения, навыки, личностные качества и опыт в самостоятельной эксплуатационной деятельности	Не способен организовывать комплекс мероприятий, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации.	Организовывает комплекс мероприятий, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации, но требует руководства.	Самостоятельно организовывает комплекс мероприятий, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации.	Самостоятельно организовывает комплекс мероприятий, связанных с обеспечением надежности функционирования и отказоустойчивости широкого спектра аппаратных и программных средств обработки информации.
ОПК-4.4	Готовность применять знания, умения, навыки, личностные качества и опыт в самостоятельной экспериментальн о-	Не способен применять инструментальные средства контроля защищенности информации в автоматизированных системах, документировать основные действия по устранению	Под руководством применяет инструментальные средства контроля защищенности информации в автоматизированных системах, документирует основные действия по	Самостоятельно применяет инструментальные средства контроля защищенности информации в автоматизированных системах, документирует действия по	Самостоятельно и эффективно применяет инструментальные средства контроля защищенности информации в автоматизированных системах, в полном объёме документирует действия по устранению

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
	исследовательской деятельности	неисправностей в работе системы защиты информации автоматизированной системы, регистрировать события, связанные с защитой информации в автоматизированных системах	устранению неисправностей в работе системы защиты информации автоматизированной системы, регистрирует базовые события, связанные с защитой информации в автоматизированных системах	устранению неисправностей в работе системы защиты информации автоматизированной системы, регистрирует события, связанные с защитой информации в автоматизированных системах	неисправностей в работе системы защиты информации автоматизированной системы, точно и наиболее эффективным образом регистрирует события, связанные с защитой информации в автоматизированных системах
ПК-1	Готовность применять знания, умения, навыки, личностные качества и опыт в самостоятельной эксплуатационной деятельности	Под руководством производит внедрение в состав автоматизированных систем средств обеспечения информационной безопасности, выполняет основные этапы работ по эксплуатации средств защиты информации, устраняет типовые неисправности при эксплуатации средств защиты информации	Под руководством производит внедрение в состав автоматизированных систем средств обеспечения информационной безопасности, выполняет основные этапы работ по эксплуатации средств защиты информации, устраняет типовые неисправности при эксплуатации средств защиты информации	Самостоятельно производит внедрение в состав автоматизированных систем средств обеспечения информационной безопасности, выполняет регламентные работы по эксплуатации средств защиты информации, устраняет неисправности при эксплуатации средств защиты информации	Самостоятельно и эффективно производит внедрение в состав автоматизированных систем средств обеспечения информационной безопасности, выполняет разноплановые работы по эксплуатации средств защиты информации, устраняет различные неисправности при эксплуатации средств защиты информации
ПК-2	Готовность применять	Даже под руководством не выполняет	Под руководством выполняет	Самостоятельно выполняет	Самостоятельно и эффективно выполняет

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
	знания, умения, навыки, личностные качества и опыт в самостоятельной организационно-управленческой деятельности	мероприятия для реализации политики информационной безопасности, не способен устанавливать программное обеспечение в соответствии с требованиями по защите информации	мероприятия для реализации политики информационной безопасности, определяет в соответствии с установленными руководителем критериями состав средств, необходимый для управления автоматизированными системами и средствами их защиты от НСД, предлагает порядок настройки технических средств для управления автоматизированными системами и средствами их защиты от НСД, устанавливает программное обеспечение в соответствии с требованиями по защите информации	мероприятия для реализации политики информационной безопасности, определяет в соответствии с выбранными критериями состав средств, необходимый для управления автоматизированными системами и средствами их защиты от НСД, самостоятельно определяет порядок настройки технических средств для управления автоматизированными системами и средствами их защиты от НСД, устанавливает программное обеспечение в соответствии с требованиями по защите информации	мероприятия для реализации политики информационной безопасности, определяет в соответствии с выбранными критериями состав средств, необходимый для управления автоматизированными системами и средствами их защиты от НСД, определяет целесообразный порядок настройки технических средств для управления автоматизированными системами и средствами их защиты от НСД, корректно устанавливает программное обеспечение в соответствии с требованиями по защите информации
ПК-3	Готовность	Не может использовать	Нуждается в	Использует	Самостоятельно

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
	применять знания, умения, навыки, личностные качества и опыт в самостоятельной экспериментально-исследовательской деятельности	методы и средства резервного копирования информации, выполнять мероприятия по устранению уязвимостей в автоматизированной системе, фиксировать изменения в конфигурации автоматизированной системы и изменении её защищенности	руководстве при использовании методов и средств резервного копирования информации, выполняет мероприятия по устранению уязвимостей в автоматизированной системе, фиксирует изменения в конфигурации автоматизированной системы и изменение её защищенности	предлагаемые методы и средства резервного копирования информации, устраняет уязвимости в автоматизированной системе, соотносит изменения в конфигурации автоматизированной системы с её защищенностью	формулирует критерии и в соответствии с ними использует методы и средства резервного копирования информации, оперативно устраняет уязвимости в автоматизированной системе, корректно и грамотно соотносит изменения в конфигурации автоматизированной системы с её защищенностью
ПК-4	Готовность применять знания, умения, навыки, личностные качества и опыт в самостоятельной проектно-технологической деятельности	Не способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов.	Оформляет техническую и проектную документацию с учетом действующих нормативных и методических документов, но требует руководства.	Самостоятельно оформляет техническую и проектную документацию с учетом действующих нормативных и методических документов.	Самостоятельно оформляет техническую и проектную документацию с учетом действующих нормативных и методических документов при разработке нестандартных и типовых проектов.
ПК-5	Готовность применять знания, умения,	Не способен под руководством проверять соответствие	Под руководством проверяет соответствие внедряемых решений и	Самостоятельно проверяет соответствие	Самостоятельно проверяет соответствие внедряемых решений и

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
	навыки, личностные качества и опыт в самостоятельной эксплуатационной деятельности	внедряемых решений и средств для обеспечения информационной безопасности требованиям политики безопасности, восстанавливать работоспособность автоматизированных систем после инцидентов информационной безопасности, проводить типовые операции вывода защищённых автоматизированных систем из эксплуатации	средств для обеспечения информационной безопасности требованиям реализуемой политики безопасности, своевременно, в неполном объёме восстанавливает работоспособность автоматизированных систем после инцидентов информационной безопасности, проводит типовые операции вывода защищённых автоматизированных систем из эксплуатации	внедряемых решений и средств для обеспечения информационной безопасности требованиям реализуемой политики безопасности в достаточном объёме восстанавливает работоспособность автоматизированных систем после инцидентов информационной безопасности, проводит операции вывода защищённых автоматизированных систем из эксплуатации	средств для обеспечения информационной безопасности требованиям реализуемой политики безопасности, своевременно, эффективно и в полном объёме восстанавливает работоспособность автоматизированных систем после инцидентов информационной безопасности, проводит операции вывода защищённых автоматизированных систем из эксплуатации с соблюдением норм и правил
ПК-6	Готовность применять знания, умения, навыки, личностные качества и опыт в самостоятельной	Не способен даже под руководством анализировать структуру и состав руководящих документов, описывающих работы по обеспечению	Под руководством и с незначительными ошибками проверяет структуру и состав руководящих документов, описывающих работы по обеспечению ин-	Самостоятельно проверяет соответствие нормативным требованиям руководящих документов, описывающих работы	Самостоятельно анализирует полноту и соответствие нормативным требованиям руководящих документов, описывающих работы по

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
	организационно-управленческой деятельности	информационной безопасности, не формирует типовые отчётные и руководящие документы для обеспечения защиты информации в информационной системе в ходе ее эксплуатации, не формулирует состав и содержание процедур контроля обеспеченности уровня защищенности информации, не готовит даже типовые документы для проведения работ по аттестации объектов информатизации и автоматизированных систем	формационной безопасности, формирует типовые отчётные и руководящие документы для обеспечения защиты информации в информационной системе в ходе ее эксплуатации, формулирует в соответствии с требованиям руководящих документов состав и содержание процедур контроля обеспеченности уровня защищенности информации, готовит типовые документы для проведения работ по аттестации объектов информатизации и автоматизированных систем	по обеспечению информационной безопасности, формирует типовые отчётные и руководящие документы для обеспечения защиты информации в информационной системе в ходе ее эксплуатации, формулирует в соответствии с требованиям руководящих документов состав и содержание процедур контроля обеспеченности уровня защищенности информации, готовит типовые документы для проведения работ по аттестации объектов информатизации и автоматизированных систем	обеспечению информационной безопасности, формирует отчётные и руководящие документы для обеспечения защиты информации в информационной системе в ходе ее эксплуатации, корректно формулирует в соответствии с требованиям руководящих документов состав и содержание процедур контроля обеспеченности уровня защищенности информации, готовит разнообразные документы для проведения работ по аттестации объектов информатизации и автоматизированных систем
ПК-7	Готовность	Не способен даже под	Под руководством	Самостоятельно	Самостоятельно и в

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
	применять знания, умения, навыки, личностные качества и опыт в самостоятельной экспериментальн о-исследовательск ой деятельности	руководством, формулировать основные угрозы информационной безопасности исходя из выявленных характеристик автоматизированной системы	формулирует целевые показатели функционирования защищенных автоматизированных систем, анализирует уязвимости автоматизированных систем в соответствии с нормативными документами, формулирует основные угрозы информационной безопасности исходя из выявленных характеристик автоматизированной системы.	формулирует целевые показатели функционирования защищенных автоматизированных систем, анализирует уязвимости автоматизированных систем в соответствии с нормативными документами, формулирует угрозы информационной безопасности исходя из выявленных характеристик автоматизированной системы.	полном объёме формулирует целевые показатели функционирования защищенных автоматизированных систем, анализирует разнообразные уязвимости автоматизированных систем в соответствии с нормативными документами, формулирует полный спектр угроз информационной безопасности исходя из выявленных характеристик автоматизированной системы.
ПК-8	Готовность применять знания, умения, навыки, личностные качества и опыт в самостоятельной экспериментальн	Не способен разрабатывать отдельные положения методической, технической, рекомендательной и отчётной документации по анализу защищённости	Разрабатывает отдельные положения методической, технической, рекомендательной и отчётной документации по анализу защищённости автоматизированной	Самостоятельно разрабатывает методическую, техническую, рекомендательную и отчётную документацию по анализу защищённости	Самостоятельно и на высоком уровне разрабатывает методическую, техническую, рекомендательную и отчётную документацию по анализу защищённости

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
	о-исследовательской деятельности	автоматизированной системы, осуществлять подбор программных средств тестирования защищённости автоматизированной системы, использовать отдельные средства инструментального анализа защищённости программных и аппаратных платформ узлов автоматизированной системы, выполняет контроль защищённости и функционирования программно-аппаратных и технических средств автоматизированной системы	системы, с ошибками осуществляет подбор программных средств тестирования защищённости автоматизированной системы, использует отдельные средства инструментального анализа защищённости программных и аппаратных платформ узлов автоматизированной системы, выполняет контроль защищённости и функционирования программно-аппаратных и технических средств автоматизированной системы	автоматизированной системы, осуществляет подбор программных средств тестирования защищённости автоматизированной системы в зависимости от предъявляемых к ней требований, использует набор инструментального анализа защищённости программных и аппаратных платформ узлов автоматизированной системы, выполняет контроль защищённости и функционирования программно-аппаратных и технических средств автоматизированной системы	автоматизированной системы, осуществляет грамотный подбор программных средств тестирования защищённости автоматизированной системы в зависимости от предъявляемых к ней требований, использует весь арсенал средств инструментального анализа защищённости программных и аппаратных платформ узлов автоматизированной системы, выполняет всеобъемлющий контроль защищённости и функционирования программно-аппаратных и технических средств автоматизированной системы
ПК-9	Готовность применять	Не формулирует даже отдельные положения	Формулирует лишь отдельные положения	Формулирует правила работы персонала со	Формулирует корректные правила

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
	знания, умения, навыки, личностные качества и опыт в самостоятельной организационно-управленческой деятельности	правил работы персонала со средствами защиты информации, не распределяет обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему, ошибается при сопоставлении результат работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации	правил работы персонала со средствами защиты информации, частично распределяет обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему, с незначительными неточностями сопоставляет результат работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации	средствами защиты информации, распределяет обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему, с незначительными неточностями сопоставляет результат работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации	работы персонала со средствами защиты информации, грамотно распределяет обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему, правильно сопоставляет результат работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации
ПК-10	Готовность применять знания, умения, навыки, личностные качества и опыт в	Под руководством не соотносит инциденты информационной безопасности с характеристиками систем и средств защиты информации, не	Только под руководством соотносит инциденты информационной безопасности с характеристиками систем и средств	Самостоятельно соотносит инциденты информационной безопасности с характеристиками систем и средств защиты информации,	Самостоятельно и корректно соотносит инциденты информационной безопасности с характеристиками систем и средств защиты

Код компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций			
		Недостаточный уровень	**Пороговый уровень**	**Продвинутый уровень**	**Высокий уровень**
	самостоятельной организационно-управленческой деятельности	формулирует даже отдельные положения для обоснования необходимости модернизации системы защиты информации автоматизированной системы, не формулирует правила применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности и правила протоколирования результатов мониторинга безопасности автоматизированных систем	защиты информации, формулирует отдельные положения для обоснования необходимости модернизации системы защиты информации автоматизированной системы, с ошибками формулирует правила применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности и правила протоколирования результатов мониторинга безопасности автоматизированных систем	обосновывает необходимость модернизации системы защиты информации автоматизированной системы, грамотно формулирует правила применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности и правила протоколирования результатов мониторинга безопасности автоматизированных систем	информации, обосновывает необходимость модернизации системы защиты информации автоматизированной системы, грамотно формулирует правила применения мер защиты информации, направленные на оперативное устранение причин возникновения инцидентов информационной безопасности и правила всеобъемлющего протоколирования результатов мониторинга безопасности автоматизированных систем

3.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения компетенций, проверяемых ИА

Задание для выпускной квалификационной работы обучающегося Иванова Александра Петровича группы

Тема выпускной квалификационной работы: «Разработка защищенной системы поддержки принятия решений» (по материалам ООО «ИТМ», г. Краснодар)

Закреплена приказом ректора от «_____» 20___г.

Целевая установка: Разработать защищенную систему поддержки принятия решений.

Основные вопросы, подлежащие разработке (исследованию):

1) Выполнить анализ предметной области.
2) Разработать техническое задание на систему.
3) Выполнить проектирование и реализацию разработки.
4) Обосновать экономическую эффективность от внедрения системы.

Основная литература:

1. Вендров, А. М. Проектирование программного обеспечения экономических информационных систем [Текст] / А. М. Вендров. — М.: Финансы и статистика, 2022. — 544 с. – ISBN 5-279-02937-8.
2. Карпова, Т. С. Базы данных: модели, разработка, реализация [Текст] / Т. С. Карпова. — СПб.: Питер, 2022. —304 с. – ISBN 5-272-00278-4.
3. Разработка приложений на C# с использованием СУБД PostgreSQL / Васюткина И.А., Трошина Г.В., Бычков М.И. - Новосибирск :НГТУ, 2015. - 143 с.: ISBN 978-5-7782-2699-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/556925. – Режим доступа: по подписке.
4. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1912987. – Режим доступа: по подписке.
5. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2022. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1861657. – Режим доступа: по подписке.

Вопросы членов ГЭК:

1. Критерии выбора средств разработки программного обеспечения.

2 Результаты анализа предметной области.

3. Какие выявлены недостатки в автоматизированной информационной системе предприятия.

4. Чем обусловлен выбор алгоритмов принятия решений.

5. Опишите модель программного обеспечения системы.

6. Чем обусловлен выбор системы управления базами данных.

7. Чем обусловлен выбор средств защиты информации.

8. Опишите функциональные требования к проектируемой информационный системе.

9. Результаты обследования объекта работы.

10. Модель данных информационного обеспечения.

11. Экономическая эффективность внедрения разработки.

12. Основные этапы внедрения предложенной разработки

13. Чем обусловлен выбор элементной базы устройства.

14. Раскройте источники финансирования разработанного Вами проекта.

3.4 Методические материалы, определяющие процедуру оценивания результатов освоения компетенций, проверяемых ИА

ВКР позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и оценить уровень сформированности аналитических, исследовательских навыков, а также навыков практического и творческого мышления, что даст возможность выполнять профессиональные трудовые действия. Результаты защиты обсуждаются Экзаменационной комиссией на закрытом заседании и объявляются в тот же день после оформления протоколов работы комиссии. Решение об окончательной оценке по защите выпускной квалификационной работе основывается на рецензии, выступлении с презентацией и ответах студента-выпускника в процессе защиты работы, результатах портфолио. Результаты защиты работы определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и объявляются в тот же день

после оформления в установленном порядке протоколов заседания Экзаменационной комиссии.

Решения Экзаменационной комиссии принимаются на закрытых заседаниях простым большинством голосов членов комиссии, участвующих в заседании. При равном числе голосов председатель комиссии обладает правом решающего голоса. Все решения Экзаменационной комиссии оформляются протоколами.

Критерии оценивания ВКР состоят из следующих групп.

1) Профессиональная группа критериев: степень актуальности тематики работы; степень раскрытия темы ВКР; корректность постановки задачи исследования и разработки; оригинальность и новизна полученных результатов, научных, конструкторских и технологических решений.

2) Справочно-информационная группа критериев: степень комплексности работы, использование в ней знаний дисциплин всех циклов; использование информационных ресурсов Интернет; использование современных пакетов компьютерных программ и технологий.

3) Оформительская группа критериев: объем и качество оформления материалов ВКР, выполнения графического материала.

4) Показатели защиты: качество представления доклада и материалов ВКР, уровень полноты и корректности ответов.

5) Отзывы руководителя и рецензента: оценка руководителя; оценка рецензента.

Измерительная шкала для оценки уровня сформированности компетенций обучающихся освоивших основную профессиональную образовательную программу 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 3.3.

Члены Экзаменационной комиссии оценивают выпускные квалификационные работы исходя из степени раскрытия темы,

самостоятельности и глубины изучения проблемы, научной новизны и практической значимости исследований, обоснованности выводов и предложений:

Оценка «отлично» – выпускная квалификационная работа выполнена в соответствии с целевой установкой (заданием), содержит элементы научной новизны и практической значимости, выводы обоснованы и являются итогом проведенного исследования.

Оценка «хорошо» – допускаются одна-две неточности при раскрытии причин выбора и актуальности темы, целей работы и ее задач, предмета, объекта и хронологических рамок исследования, допускается неточность в логике выведения одного из наиболее значимого вывода; в заключительной части нечетко начертаны перспективы и задачи дальнейшего исследования данной темы, вопросы практического применения и внедрения результатов исследования в практику.

Оценка «удовлетворительно» – допускаются неточности при раскрытии причин выбора и актуальности темы, целей работы и ее задач, предмета, объекта и хронологических рамок исследования, допущена грубая погрешность в логике изложения элементов научной новизны, которая при указании на нее устраняется с трудом; в заключительной части слабо показаны перспективы и задачи дальнейшего исследования данной темы, вопросы практического применения и внедрения результатов исследования в практику.

Оценка «неудовлетворительно» – слабо раскрываются причины выбора и актуальность темы, цели работы и ее задачи, предмет, объект и хронологические рамки исследования, допускаются грубые погрешности в логике выведения нескольких из наиболее значимых выводов, которые при указании на них не устраняются; затруднения в формулировке элементов научной новизны исследований; в заключительной части не отражаются перспективы и задачи дальнейшего исследования данной темы, вопросы практического применения и внедрения результатов исследования в практику.

4 ПОРЯДОК ПРОВЕДЕНИЯ ИТОГОВОЙ АТТЕСТАЦИИ ДЛЯ ВЫПУСКНИКОВ ИЗ ЧИСЛА ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Порядок проведения итоговой аттестации для выпускников из числа лиц с ограниченными возможностями здоровья регламентирован положениями Академии ИМСИТ о организации инклюзивного обучения обучающихся с ограниченными возможностями здоровья и обучающихся инвалидов.

Специфика получаемой специализации предполагает возможность проведения аттестации следующих категорий инвалидов и лиц с ограниченными возможностями здоровья:

- с ограничением двигательных функций;
- с нарушениями слуха;
- с нарушениями зрения.

Организация итоговой аттестации обеспечивает возможность беспрепятственного доступа обучающихся с ограниченными возможностями здоровья и (или) инвалидов в помещения, для этого имеются пандусы, поручни, лифты и расширенные дверные проемы.

В помещениях имеется возможность оборудовать места для обучающихся-инвалидов с различными видами нарушения здоровья, в том числе опорно-двигательного аппарата и слуха. Освещенность учебных мест устанавливается в соответствии с положениями СНиП 23-05-95 «Естественное и искусственное освещения». Все предметы, необходимые для учебного процесса, располагаются в зоне максимальной досягаемости вытянутых рук.

Помещения предусматривают места для лиц с ограниченными возможностями здоровья и инвалидов, имеющих сердечно-сосудистые заболевания, они оборудованы солнцезащитными устройствами (жалюзи), в них имеется система климат-контроля.

5 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ИТОГОВОЙ АТТЕСТАЦИИ

Материально-техническое и программное обеспечение итоговой аттестации включает: помещение для проведения итоговой аттестации, укомплектованное учебной мебелью и техническими средствами обучения, дающими студенту возможность представления презентационных материалов при защите ВКР.

Освоение дисциплины предполагает использование академической аудитории для проведения лекционных и семинарских занятий с необходимыми техническими средствами (компьютер или ноутбук, оборудование мультимедиа (проектор), доска). Мультимедиа-проектор необходим для демонстрации электронных презентаций по разделам дисциплины.

Перечень электронных ресурсов представлен в таблице 5.1.

Таблица 5.1 – Перечень электронно-библиотечных систем

№	Наименование ресурса	Наименование документа с указанием реквизитов	Срок действия документа
1	ЭБС Znanuim	ООО «ЗНАНИУМ». Договор № 1393 эбс от 28.09.2023 г.	с 28.09.2023 по 27.09.2024 г.
2	Научная электронная библиотека eLibrary (ринц)	ООО «Научная электронная библиотека» (г. Москва). Лицензионное соглашение № 7241 от 24.02.12 г.	бессрочно
3	ЭБС IBooks	ООО «Айбукс». Договор № 27-01/23К от 27.01.2023 г	с 26.01.2023 по 26.01.2024 г.
4	ЭБС Book.ru	ООО «КноРус медиа». Договор №18511468 от 08 сентября 2023 г.	с 08.09.2023 по 09.09.2024 г.

Перечень профессиональных баз данных и информационных справочных систем:

1. Кодекс – Профессиональные справочные системы – URL: https://kodeks.ru
2. РОССТАНДАРТ Федеральное агентство по техническому регулированию и метрологии – URL: https://www.gost.ru/portal/gost/
3. ИСО Международная организация по стандартизации – URL: https://www.iso.org/ru/home.html
4. ABOUT THE UNIFIED MODELING LANGUAGE SPECIFICATION – URL: https://www.omg.org/spec/UML
5. Проект IDEF.ru – URL: http://idef.ru
6. Портал выбора технологий и поставщиков – URL: http://www.tadviser.ru

7. ARIS BPM Community – URL: https://www.ariscommunity.com
8. Global CIO Официальный портал ИТ-директоров – URL: http://www.globalcio.ru
9. Библиотеки и 3D модели DipTrace – URL: https://diptrace.com/rus/download/libraries-and-3d-models/
10. Development - OpenFOAM-plus – Repository – URL: https://develop.openfoam.com/
11. MecSoft Corporation Resource Portal – URL: https://mecsoft.com/resources/
12. Галерея знания CSoft Development – URL: http://csdev.ru/pages/gallery/
13. Электронная энциклопедия PLM. [Электронный ресурс] – Режим доступа: http://plmpedia.ru/
14. Техническая документация Windows для разработчиков и ИТ-специалистов. – Режим доступа: https://docs.microsoft.com/ru-RU/windows
15. Справочный центр Astra Linux. – Режим доступа: https://wiki.astralinux.ru
16. База знаний Astra. – Режим доступа: https://wiki.astralinux.ru/kb
17. Совет Безопасности Российской Федерации. – Режим доступа: http://www.scrf.gov.ru
18. Информационно-правовой портал ГАРАНТ.РУ. – Режим доступа: https://www.garant.ru
19. Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс». – Режим доступа: https://docs.cntd.ru
20. Федеральная служба по техническому и экспортному контролю. – Режим доступа: https://fstec.ru
21. Код Безопасности. – Режим доступа: https://www.securitycode.ru/

Перечень программных средств информационно-коммуникационных технологий, представлен в таблице 5.2.

Таблица 5.2 – Перечень программных средств информационно-коммуникационных технологий

Перечень лицензионного программного обеспечения, реквизиты подтверждающего документа	
1.	Windows 10 Pro RUS Операцинная система – Windows 10 Pro RUS Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2021
2.	Яндекс Браузер Браузер Яндекс Браузер Лицензионное соглашение на использование программ Яндекс Браузер https://yandex.ru/legal/browser_agreement/
3.	Mozilla Firefox Браузер Mozilla Firefox Программное обеспечение по лицензии GNU GPL
4.	LibreOffice Офисный пакет LibreOffice Программное обеспечение по лицензии GNU GPL
5.	Notepad++. Тектовый редактор Notepad++. Программное обеспечение по лицензии GNU GPL
6.	Kaspersky Endpoint Security Антивирусное ПО Kaspersky Endpoint Security для бизнеса Стандартный (350шт). Договор № ПР-00035750 от 13 декабря 2022г. (ООО Прима АйТи)
7.	Oracle VM VirtualBox VM VirtualBox — программный продукт виртуализации для операционных систем Программное обеспечение по лицензии GNU GPL
8.	Adobe Reader DC Adobe Acrobat — пакет программ, предназначенный для создания и просмотра электронных публикаций в формате PDF Adobe Acrobat Reader DC and Runtime Software distribution license agreement for use on personal computers от 31.01.2017
9.	Консоль Kaspersky Security Center Консоль администрирования Kaspersky Security Center Договор № ПР-

	00035750 от 13 декабря 2022г. (ООО Прима АйТи)
10.	Kaspersky Endpoint Security 11 Kaspersky Endpoint Security 11 для Windows Договор № ПР-00035750 от 13 декабря 2022г. (ООО Прима АйТи)
11.	10-Страйк Сканирование Сети Сканирование Сети - программа-сканер TCP-портов и IP-адресов Лицензионный сертификат от 01.01.2011
12.	Traffic inspector Special Unlimited ОРГАНИЗАЦИЯ ДОСТУПА В ИНТЕРНЕТ. NAT, ПРОКСИ-СЕРВЕР, VPN, AD Лицензионный договор №649 от 23.09.2019
13.	Astra Linux Операционная система семейства Linux. Версия "Орел" Программное обеспечение по лицензии GNU GPL
14.	Secren Net LSP Средство защиты информации от несанкционированного доступа для операционных систем семейства Linux Договор №КБ/04085/1/11 от 14.02.2022
15.	Astra Linux Special Edition Операционная система Astra Linux Special Edition "Смоленск" Лицензионный договор №А-2023-3968-ВУЗ 08 августа 2023 г.
16.	Secren Net Studio Единая система управление продуктами для защиты Windows, Linux и платами доверенной загрузки Договор №КБ/04085/1/11 от 14.02.2022
17.	PostgreSQL Система управления базами данных Программное обеспечение по лицензии GNU GPL
18.	vGate Средство микросегментации и защиты жизненного цикла виртуальных машин Договор №КБ/04085/1/11 от 14.02.2022

Перечень средств материально-технического обеспечения для обучения представлен в таблице 5.3.

Таблица 5.3 – Перечень средств материально-техническое обеспечение

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
Специальные помещения для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации		
Аудитории, с возможностью использования мультимедийного проектора ауд. 301-303, 206	мультимедийный проектор доска парты, или столы со стульями	Программное обеспечение по лицензии GNU GPL: 7-Zip, Google Chrome, LibreOffice.
Лаборатория программно-аппаратных средств защиты Лаборатория технической защиты информации	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016	20 посадочных мест, рабочее место преподавателя 20 компьютеров P55-UD3/INTEL-i5-750/DDR3-1333- 8Гб/SSD Flexis 120Gb /WD3200AAKS/Radeon HD-4600/DWL-G520 Wireles 20 мониторов Acer V193W-19” 20 комплектов клавиатура+мышь 1 коммутатор неуправляемый DES-1024D 1 беспроводная точка доступа DWL-3200AP 3 Комплект оборудования Arduino 5 учебных комплектов SDK 1.1s 1 МФУ HP LJ M1212nf MFP 12 Инструмент для сборки ПК (отвертка ph-1, плоскогубцы 150 мм,

	MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC Traffic inspector Special Unlimited Ramus Educational Micro-Cap Evaluation vGate Secren Net Studio Secren Net LSP	термопаста 2гр., Антистатический браслет, стяжки 150 мм) антивирусные программные комплексы, аппаратные средства аутентификации пользователя, программно-аппаратные комплексы защиты информации, включающие в том числе средства криптографической защиты информации (средства анализа защищенности компьютерных сетей, аппаратно-программные средства управления доступом к данным, стенды средства защиты информации от утечки по акустическому каналу, каналу побочных электромагнитных излучений и наводок, акустовибрационному и акустоэлектрическому каналам, техническими средствами контроля эффективности защиты информации от утечки по указанным каналам
Лаборатория Интеллектуальные системы и технологии (Research Laboratory of Intelligent Systems and Technologies). Лаборатория Электротехники, электроники и схемотехники.ауд. 208	19 посадочных мест, рабочее место преподавателя, 10 компьютеров H97-PLU/INTEL i5-4460/DDR3-1333-16Гб/SD7SB6S-128G+ST500DM002/Radeon R7 200/Realtek PCIe GBE 9 компьютеров A320M-H-CF/AMD Ryzen 5 2600/DDR4-2666-16Гб/Apacer AS2280P4-256Gb, Toshiba HDWD110 1Tb/Nvidia GT-710/Realtek PCI-E GBE 1 компьютер P8Z77-V-LX2/INTEL I5-3570K/DDR3-1600-8Гб/ SSD SSDPR-CX400-128G2, WDC WS15EARS/AMD HD-5700 Realtek PCIe GBE 10 мониторов Philips 274E5QSB 27” 1 монитор Samsung SyncMaster E1720 11 комплектов клавиатура+мышь 1 принтер HP LaserJet 1018 1 коммутатор неуправляемый TL-	1С:Предприятие 8. Комплект для обучения в высших и средних учебных заведениях. Сублицензионный договор № 32/180913/005 от 18.09.2013. (Первый БИТ) Diptrace Лицензия для образовательной организации. Лицензионное соглашение с оконечным пользователем ООО «Новарм» Kaspersky Endpoint Security для бизнеса – Стандартный (350шт) Договор № ПР-00035750 от 13 декабря 2022г. (ООО Прима АйТи) сроком на 1 год. Embarcadero RAD Studio XE8 (10шт.). Сублицензионный договор №Tr000019973 от 23.04.2015 (ЗАО СофтЛайн Трейд Microsoft Access 2016. Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2022. Microsoft Office 2007 Russian. Лицензионный сертификат № 42373687 от 27.06.2007 Microsoft Project профессиональный 2016. Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2022.

	SG1024D Междисциплинарная лабораторная станция NI ELVIS II и ПО Circuit Design Suit Лаборатория схемотехники (необходимо наличие лаб. станции ELVIS) Практикум по цифровым элементам вычислительной и информационно-измерительной техники (необходимо наличие лабораторной станции ELVIS) Лаборатория проектирование цифровых устройств и программирования ПЛИС (необходимо наличие лабораторной станции ELVIS) Комплект аксессуаров NI myRIO Starter Accessory Kit (опционально) Комплект аксессуаров NI myRIO Mechatronics Accessory Kit Комплект аксессуаров NI myRIO Embedded Systems Accessory Kit Лаборатория программирования встраиваемых систем Локальные вычислительные сети (необходимо наличие лабораторной станции ELVIS) Промышленные интерфейсы и протоколы (программная версия) Академическая лицензия NI LabVIEW на неограниченное кол-во рабочих мест в пределах кафедры. Arduino Robot.	Microsoft Visio профессиональный 2016. Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2022. National Instruments Software – NI LabVIEW Full (10 р.м.). Договор № 222015 от 27.04.2015 (ООО «ЮГРОН») ОС – Windows 10 Pro RUS. Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2022. Программное обеспечение по лицензии GNU GPL: 7-Zip (22.01) Archi 5.0.2 Arduino Software (IDE), 2.0.4 Apache-NetBeans IDE 17 Blender 3D 3.4.1 GIMP 2.10.34 GvSig 1.11 Inkscape 1.3 KdenLive 22.12.3 LibreCAD 2.2 LibreOffice 7.5.1.2 Maxima computer algebra system 5.46 Node.js 19.6.0 Oracle VM VirtualBox 7.0.6 PostgreSQL 15 Yandex brouser Бесплатные и учебные версии: Adobe Reader DC. Adobe Acrobat Reader AnyDynamic8 ARIS EXPRESS 2.4 Cisco Packet Tracer 8.0 64Bit Deductor Academic 5.3 IntelliJ IDEA Community JetBrains PyCharm Community Microsoft SQL Server 2019 Express Microsoft SQL Server Management Studio 18.8. Microsoft Visual Studio Code 1.79.2 Microsoft Visual Studio Community 2022 17.7.3 Open Server 5.4.3 Python-3.11.5 StarUML V1, КОМПАС-3D LT V12
Компьютерный класс ауд.113	20 посадочных мест, рабочее место преподавателя 20 компьютеров P55-	1С:Предприятие 8. Комплект для обучения в высших и средних учебных заведениях. Сублицензионный договор № 32/180913/005 от 18.09.2013.

	UD3/INTEL-i5-750/DDR3-1333-8Гб/SSD Flexis 120Gb /WD3200AAKS/Radeon HD-4600/DWL-G520 Wireles 20 мониторов Acer V193W-19” 20 комплектов клавиатура+мышь 1 коммутатор неуправляемый DES-1024D 3 Комплект оборудования Arduino 5 учебных комплектов SDK 1.1s 1 МФУ HP LJ M1212nf MFP 12 Инструмент для сборки ПК (отвертка ph-1, плоскогубцы 150 мм, термопаста 2гр., Антистатический браслет, стяжки 150 мм)	(Первый БИТ) Diptrace Лицензия для образовательной организации. Лицензионное соглашение с оконечным пользователем ООО «Новарм» Kaspersky Endpoint Security для бизнеса – Стандартный (350шт) Договор № ПР-00035750 от 13 декабря 2022г. (ООО Прима АйТи) сроком на 1 год. Embarcadero RAD Studio XE8 (10шт.). Сублицензионный договор №Tr000019973 от 23.04.2015 (ЗАО СофтЛайн Трейд Microsoft Access 2016. Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2022. Microsoft Project профессиональный 2016. Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2022. Microsoft Visio профессиональный 2016. Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2022. ОС – Windows 10 Pro RUS. Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2022. Программное обеспечение по лицензии GNU GPL: 7-Zip (22.01) Archi 5.0.2 Arduino Software (IDE), 2.0.4 Apache-NetBeans IDE 17 Blender 3D 3.4.1 GIMP 2.10.34 GvSig 1.11 Inkscape 1.3 KdenLive 22.12.3 LibreCAD 2.2 LibreOffice 7.5.1.2 Maxima computer algebra system 5.46 Node.js 19.6.0 Oracle VM VirtualBox 7.0.6 PostgreSQL 15 Yandex brouser Бесплатные и учебные версии: Adobe Reader DC. Adobe Acrobat Reader AnyDynamic8 ARIS EXPRESS 2.4

		Cisco Packet Tracer 8.0 64Bit Deductor Academic 5.3 IntelliJ IDEA Community JetBrains PyCharm Community Microsoft SQL Server 2019 Express Microsoft SQL Server Management Studio 18.8. Microsoft Visual Studio Code 1.79.2 Microsoft Visual Studio Community 2022 17.7.3 Open Server 5.4.3 Python-3.11.5 StarUML V1, КОМПАС-3D LT V12
Помещения для самостоятельной работы		
Лаборатория Интеллектуальные системы и технологии (Research Laboratory of Intelligent Systems and Technologies). Лаборатория Электротехники, электроники и схемотехники.ауд. 208	19 посадочных мест, рабочее место преподавателя, 10 компьютеров H97-PLU/INTEL i5-4460/DDR3-1333-16Гб/SD7SB6S-128G+ST500DM002/Radeon R7 200/Realtek PCIe GBE 9 компьютеров A320M-H-CF/AMD Ryzen 5 2600/DDR4-2666-16Гб/Apacer AS2280P4-256Gb, Toshiba HDWD110 1Tb/Nvidia GT-710/Realtek PCI-E GBE 1 компьютер P8Z77-V-LX2/INTEL I5-3570K/DDR3-1600-8Гб/ SSD SSDPR-CX400-128G2, WDC WS15EARS/AMD HD-5700 Realtek PCIe GBE 10 мониторов Philips 274E5QSB 27” 1 монитор Samsung SyncMaster E1720 11 комплектов клавиатура+мышь 1 принтер HP LaserJet 1018 1 коммутатор неуправляемый TL-SG1024D Междисциплинарная лабораторная станция NI ELVIS II и ПО Circuit Design Suit Лаборатория схемотехники	1С:Предприятие 8. Комплект для обучения в высших и средних учебных заведениях. Сублицензионный договор № 32/180913/005 от 18.09.2013. (Первый БИТ) Diptrace Лицензия для образовательной организации. Лицензионное соглашение с оконечным пользователем ООО «Новарм» Kaspersky Endpoint Security для бизнеса – Стандартный (350шт) Договор № ПР-00035750 от 13 декабря 2022г. (ООО Прима АйТи) сроком на 1 год. Embarcadero RAD Studio XE8 (10шт.). Сублицензионный договор №Tr000019973 от 23.04.2015 (ЗАО СофтЛайн Трейд Microsoft Access 2016. Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2022. Microsoft Office 2007 Russian. Лицензионный сертификат № 42373687 от 27.06.2007 Microsoft Project профессиональный 2016. Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2022. Microsoft Visio профессиональный 2016. Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2022. National Instruments Software – NI LabVIEW Full (10 р.м.). Договор №

	(необходимо наличие лаб. станции ELVIS) Практикум по цифровым элементам вычислительной и информационно-измерительной техники (необходимо наличие лабораторной станции ELVIS) Лаборатория проектирование цифровых устройств и программирования ПЛИС (необходимо наличие лабораторной станции ELVIS) Комплект аксессуаров NI myRIO Starter Accessory Kit (опционально) Комплект аксессуаров NI myRIO Mechatronics Accessory Kit Комплект аксессуаров NI myRIO Embedded Systems Accessory Kit Лаборатория программирования встраиваемых систем Локальные вычислительные сети (необходимо наличие лабораторной станции ELVIS) Промышленные интерфейсы и протоколы (программная версия) Академическая лицензия NI LabVIEW на неограниченное кол-во рабочих мест в пределах кафедры. Arduino Robot.	222015 от 27.04.2015 (ООО «ЮГРОН») ОС – Windows 10 Pro RUS. Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2022. Программное обеспечение по лицензии GNU GPL: 7-Zip (22.01) Archi 5.0.2 Arduino Software (IDE), 2.0.4 Apache-NetBeans IDE 17 Blender 3D 3.4.1 GIMP 2.10.34 GvSig 1.11 Inkscape 1.3 KdenLive 22.12.3 LibreCAD 2.2 LibreOffice 7.5.1.2 Maxima computer algebra system 5.46 Node.js 19.6.0 Oracle VM VirtualBox 7.0.6 PostgreSQL 15 Yandex brouser Бесплатные и учебные версии: Adobe Reader DC. Adobe Acrobat Reader AnyDynamic8 ARIS EXPRESS 2.4 Cisco Packet Tracer 8.0 64Bit Deductor Academic 5.3 IntelliJ IDEA Community JetBrains PyCharm Community Microsoft SQL Server 2019 Express Microsoft SQL Server Management Studio 18.8. Microsoft Visual Studio Code 1.79.2 Microsoft Visual Studio Community 2022 17.7.3 Open Server 5.4.3 Python-3.11.5 StarUML V1, КОМПАС-3D LT V12
Компьютерный класс ауд. 120 Лаборатория «Программной инженерии и разработки ПО». Полигон Кибер-спорт	20 посадочных мест, рабочее место преподавателя 20 компьютеров A320M-H-CF/AMD Ryzen 5 2600X/DDR4-2933 16Гб/SSD XPG GAMMIX S11 Pro 512Гб/NVIDIA GeForce GTX 1050 Ti/Realtek PCIe GbE Family	ОС – Windows 10 Pro RUS. Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2022. 1С:Предприятие 8. Комплект для обучения в высших и средних учебных заведениях. Сублицензионный договор № 32/180913/005 от 18.09.2013. (Первый БИТ) Kaspersky Endpoint Security для бизнеса – Стандартный (350шт)

	Controller 40 мониторов Samsung S24R350FHI 23.8" 20 ИБП CyberPower UT650EG 20 комплектов клавиатура+мышь 20 гарнитур Defenfer G-320 1 неуправляемый коммутатор TP-LINK TL-SG1024D 1 Интерактивная панель EliteBoard LR-75UT40i7	Договор № ПР-00035750 от 13 декабря 2022г. (ООО Прима АйТи) сроком на 1 год. Microsoft Access 2016. Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2022. Microsoft Project профессиональный 2016. Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2022. Microsoft Visio профессиональный 2016. Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2022. Microsoft Visual Studio Professional 2019. Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2022. Программное обеспечение по лицензии GNU GPL: Anaconda3, 7-Zip, Blender, GIMP, Google Chrome, Inkscape, LibreCAD, LibreOffice, Klite Mega Codec Pack, Model Vision Free, Maxima, Mozilla Firefox, Notepad++, Oracle VM VirtualBox, StarUML V1, SMath Studio, Apache-NetBeans, IntelliJ IDEA Community, JetBrains PyCharm Community, Microsoft SQL Server 2019 Express, KDELive, Microsoft SQL Server Management Studio 18.8. Adobe Reader DC. Adobe Acrobat Reader DC and Runtime Software distribution license agreement for use on personal computers от 31.01.2017
Читальный зал	15 посадочных мест, 2 рабочих места библиотекаря 15 моноблоков HP AMD Athlon Silver 3050U 1 моноблок Lenovo E1 1 системный блок Intel G5400-3,7/DDR4-2400 4Gb/SSD CT240BX/UHD Graphics 610/ Realtek PCIe GbE Family Controller 1 монитор Samsung SyncMaster 920n 2 сканера HP ScanJet G2410 1 принтер HP LaserJet P1005	Kaspersky Endpoint Security для бизнеса – Стандартный (350шт) Договор № ПР-00035750 от 13 декабря 2022г. (ООО Прима АйТи) сроком на 1 год. Microsoft Access 2016. Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2022. Microsoft Project профессиональный 2016. Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2022. Microsoft Visio профессиональный 2016. Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2022. ОС – Windows 10 Pro RUS OEM – Договор №18/03 от 21.03.2023 ООО

		БКТ, Приложение №1 Программное обеспечение по лицензии GNU GPL: 7-Zip (22.01) Apache-NetBeans IDE 17 Blender 3D 3.4.1 GIMP 2.10.34 Inkscape 1.3 KdenLive 22.12.3 LibreCAD 2.2 LibreOffice 7.5.1.2 Maxima computer algebra system 5.46 Yandex brouser Бесплатные и учебные версии: Adobe Reader DC. Adobe Acrobat Reader IntelliJ IDEA Community JetBrains PyCharm Community Microsoft Visual Studio Code 1.79.2

Специальные помещения для хранения и профилактического обслуживания учебного оборудования		
Кабинет №123а Специальное помещение для хранения и профилактического обслуживания учебного оборудования	Системный блок AMD FX-8120 1шт Системный блок Intel Core 2 CPU 4400 1шт. Монитор “PHILIPS E2243FWS” 1 шт. Монитор “BENQ CL2240” 1шт. Монитор “SAMSUNG 740n” 1шт. Набор иснтрументов 1 шт. Паяльная станция Lukey 902 1 шт Принтер SAMSUNG ML-1665 1 шт. Принтер HP LJ 1018 1 шт. Коммутатор D-Link DES-1005D 1 шт. Роутер Keenetic Lite (KN-3110)1 шт. Паяльник 40 Вт дер/ручка 1 шт. Лампа настольная 1 шт. Пылесос “SUPRA 1800W” 1 шт.	Windows 10 Professional Microsoft Open License 48587685 от 02.06.2011 - 2 шт. Программное обеспечение по лицензии GNU GPL: 7-Zip, LibreOffice, Java 8, K-Lite Mega Codec Pack, PDF24 Creator, CCleaner, Google Chrome Canary, Notepad++, Oracle VM VirtualBox Adobe Reader DC. Adobe Acrobat Reader DC and Runtime Software distribution license agreement for use on personal computers от 31.01.2017 – 2шт. Kaspersky Endpoint Security для бизнеса – Стандартный (350шт) Договор № ПР-00035750 от 13 декабря 2022г. (ООО Прима АйТи) сроком на 1 год. ПАРУС-Бюджет 8.5.6.1 Договор № 001-1 от 09.01.2017, Товарная накладная №1 от 23.01.2017 – 1 шт. Microsoft Office 2007 Professional Plus Microsoft Open License 42060616 от 20.04.2007 2 шт. 10-Strike File search pro – Лицензионный сертификат от 01.01.2011 – 1 шт. 10-Страйк Сканирование Сети -– Лицензионный сертификат от 01.01.2011 – 1 шт. 10-Страйк Инвентаризация Компьютеров -– Лицензионный сертификат от 01.01.2011 – 1

	Шуруповерт “Hitachi ds12dvf3” 1 шт. Веб-камера Logitech HD WebCam C525 1280*720 MicUSB - 2 шт Перфоратор Град-М 1 шт. Микрофон Yanmai R933 – 2 шт	шт.
Кабинет №127 Специальное помещение для хранения и профилактического обслуживания учебного оборудования	Парта Стул ИЗО на металокаркасе Набор инструментов Пылесос «RSE 1400»	Нет
Кабинет №124 Кластерная лаборатория Серверный центр	Стойка серверная Серверный узел SuperMicro 1U6019PMT\Xeon silver 4108\8xDDR4 8Gd\ - 2 шт Сетевое хранилище данных Synology DS-418 1 шт. Монитор Acer V193 1 шт. Шкаф 2-х дверный архивный металл. - 2шт Сплит система AirWell 1 шт. Сплит-система Lessar 1 шт. Система контроля доступа СКАТ 1200 И7 1 шт. Комутатор TPLINK T1600G-28TS ИБП APC Smart-UPS C 3000VA 2U 230V SMC3000R2I-RS Управляющий узел кластера I500PX-S5380\ Xeon E5345\ DDR-2-667-8192Mb\WD5001ABYS 1 шт.	Windows Server 2016 Standard - Microsoft Open License № 68891953 от 2017.09.15 . 2 шт.+ 4 виртульных Сервер администрирования Kaspersky Security Center Договор № ПР-00035750 от 13 декабря 2022г. (ООО Прима АйТи) сроком на 1 год УМКК «Телекоммуникации и сети» Лицензия: С00001 Номер лицензии: 20030400000000000033 УМКК «Коммутаторы локальных сетей» Лицензия: С00001 Номер лицензии: 20030400000000000033 УМКК «Электротехника и электроника» Лицензия: С00001 Номер лицензии: 20030400000000000033 УМКК «Информационные системы в экономике» Лицензия: С00001 Номер лицензии: 20030400000000000033 УМКК «Корпоративные информационные системы» Лицензия: С00001 Номер лицензии: 20030400000000000033 УМКК "Моделирование данных" Лицензия: С00001 Номер лицензии: 20030400000000000033 УМКК «Управление базами данных» Лицензия: С00001 Номер лицензии: 20030400000000000033 УМКК «Сетевые информационные технологии» Лицензия: С00001 Номер лицензии: 20030400000000000033 УМКК «Теоретические основы информатики» Лицензия: С00001 Номер лицензии: 20030400000000000033

	Рабочий узел кластера I500PX-S5380\ Xeon E5345\ DDR-2-667-8192Mb\WD800JD\ - 16 шт Серверный узел Spectrus I500PX-S5380\ Xeon E5345\ DDR-2-667-8192Mb Серверный узел DEXUS II I500PX-S5380\ Xeon E5345\ DDR-2-667-8192Mb\ Коммутатор DLink ИБП ДРУГОЙ - 1 шт. БОЛЬШАЯ КУЧА хлама	УМКК "Основы алгоритмизации и программирования" Лицензия: C00001 Номер лицензии: 20030400000000000033 УМКК "Объектно-ориентированные технологии" Лицензия: C00001 Номер лицензии: 20030400000000000033 УМКК «Информационные технологии» Лицензия: C00001 Номер лицензии: 20030400000000000033 AppWave Enterprise License Center Сублицензионный договор №Tr000019973 от 23.04.2015 (ЗАО СофтЛайн Трейд). Microsoft SQL Server 2016 Подписка Microsoft Imagine Premium – – Order №143659 от 12.07.2022.. 1 шт. Kaspersky Endpoint Security для бизнеса – Стандартный (350шт) Договор № ПР-00035750 от 13 декабря 2022г. (ООО Прима АйТи) сроком на 1 год. - 6 шт Traffic inspector Special Unlimited. Лицензионный договор №649 от 23.09.2019 – 1шт. Система зашиты Эшэлон II “Кредо-диалог” Акт № 123 от 01.11.2018, . Сертификат от 24.08.2018. – 1 шт. Система утпавления хранилищем документов “Кредо-диалог” Акт № 123 от 01.11.2018, . Сертификат от 24.08.2018. – 1 шт Центр управления ПО Кредо Акт № 123 от 01.11.2018, . Сертификат от 24.08.2018. 1 шт. Ваш финансовый аналитик, сетевой – ООО «Прософт» Договор № 14521/48385от 16.05.2022г. Акт передави прав №14512/48385 от 17.05.2022г Windows Server 2003 R2 Standart - Microsoft Open License № 42060616 от 20.04.2007 1 шт. FreeWare, OpenSource, программное обеспечение по лицензиям GNU GPL7: 7zip 6 шт., Open SuSe Linux Open Source 17 шт., MySql Server Community 1 шт., Apache HTTP Server 1 шт., Oracle Database 11g Express Edition 1 шт., Java 8 – 6 шт, Mozilla Firefox 6 шт. Windows Server 2008 R2 Standart - Microsoft Open License № 46794243 от 19.04.2010 2 шт.
Преподавательская	Управляемый комутатор T2600G-52TS 2 шт	
Кафедра математики и вычислительной	Системный блок H310CM-DVS P 1.30\Intel(R)	

техники (118а)	Pentium(R) Gold G5400 CPU 3.70GHz\DDR4-4Gb\SSD 240Gb Монитор SAMSUNG SM 943n Принтер HP LaserJet 1018 МФУ Brother DCP-L2540DNR	

Автор: Капустин Сергей Алимович

ПРОГРАММА ИТОГОВОЙ АТТЕСТАЦИИ

для обучающихся очной и заочной форм обучения
направления подготовки 10.03.01 Информационная безопасность
направленность (профиль) образовательной программы
«Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)»

Редактор: Капустин С.А.
Верстка: Капустин С.А.

Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования «Академия маркетинга и социально-информационных технологий»
Редакционно-издательская группа ИМСИТ
350000, Краснодар, ул. Зиповская, 5

Краснодар, 2023