ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Б3.01(Д) Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа бакалавра)

Направление подготовки 10.03.01 «Информационная безопасность»

Профиль подготовки «Безопасность автоматизированных систем»

Квалификация выпускника бакалавр

Форма обучения очная

СОДЕРЖАНИЕ

1. Цели государственной итоговой аттестации
1.1 Перечень планируемых результатов подготовки, сдачи государственного экзамена и защиты выпускной квалификационной работы, соотнесенных с планируемыми результатами освоения образовательной программы

Выпускник, освоивший программу бакалавриата, должен обладать следующими общекультурными компетенциями*:*

УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
УК-3 Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде
УК-4 Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)
УК-5 Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах
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
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 чрезвычайной ситуации и военных конфликтов
УК-9 Способен принимать обоснованные экономические решения в различных областях жизнедеятельности
УК-10 Способен формировать нетерпимое отношение к коррупционному поведению
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.
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;
ПК-1 Способен составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе
ПК-2 Способен администрировать средства защиты информации в компьютерных системах и сетях
ПК-3 Способен анализировать и противодействовать угрозам информации операционных систем, систем управления базами данных, вычислительных сетей
ПК-4 Способен оценивать последствия от реализации угроз безопасности информации в автоматизированной системе
ПК-5 Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
ПК-6 Способен проводить анализ рисков информационной безопасности автоматизированной системы
ПК-7 Способен разрабатывать комплекс мероприятий по защите информации в автоматизированных системах финансовых и экономических структур
ПК-8 Способен проводить анализ информационной безопасности объектов и систем на соответсвие требований стандартов и нормативно-правовых актов в области информационной безопасности
ПК-9 Способен применять технические средства защиты информации на основе знаний физических законов
ПК-10 Способен разрабатывать компьютерные модели исследуемых процессов и систем и применять их для определения оптимальных вариантов проектных, конструкторских и технологических решений
ПК-11 Способен участвовать в проектировании системы управления информационной безопасностью.

1.2 Условия допуска к государственной итоговой аттестации

К государственной итоговой аттестации допускается обучающийся, не имеющий академической задолженности и в полном объеме выполнивший учебный план или индивидуальный учебный план по соответствующей образовательной программе высшего образования.

1.1 Результаты обучения (компетентностная модель выпускника

Таблица 1 -Компетентностная модель выпускника

Компетенции		Код и наименование индикатора достижения компетенции	Знать	Уметь	Иметь навыки (владеть)
Индекс	Формулировка				
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1 Анализирует задачи, выделяяих базовые составляющие, осуществляет декомпозицию задач	теоретические, правовые и организационные основы обеспечении производственной безопасности	работать с разноплановыми источниками	анализа литературы, документации в области обеспечения техносферной безопасности
		УК-1.2 Находит и критически анализирует информацию, необходимую для решения поставленных задач	основные методы построения прогнозов, статистические методы принятия решений	анализировать, оценивать уровень опасности в условиях производства	аналитически мыслить
		УК-1.3 Рассматривает возможные варианты решения задач, оценивая их достоинства и недостатки	основные приемы и методы анализа, оценки производственнойбезопасности	самостоятельно обрабатывать, анализировать полученную информацию	навыки: самостоятельнойработы, самоорганизации и организации выполнения заданий
		УК-1.4 Грамотно, логично, аргументированно формирует собственные суждения и оценки. Отличает факты от мнений, интерпретаций, оценок и т.д. в рассуждениях других участников	основные приемы и методы анализа, оценки производственной безопасности	самостоятельно обрабатывать, анализировать полученную информацию	формированием собственных суждений и оценки

		деятельности			
		УК-1.5 Определяет и оценивает последствия возможных решений задач	правовые и организационные основы обеспечения производственной безопасности	работать с разноплановыми источниками	анализа литературы, документации в области обеспечения техносферной безопасности
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 в рамках поставленной цели проекта совокупность взаимосвязанных задач, обеспечивающих ее достижение. Определяет ожидаемые результаты решения выделенных задач	принципы и методы системного подхода	отличать факты от мнений, интерпретаций, оценок и т.д. в рассуждениях других участников деятельности; применять принципы и методы системного подхода для решения поставленных задач	практическими навыками выбора оптимальных способов решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
		УК-2.2 Проектирует решение конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений	принципы и методы анализа имеющихся ресурсов и ограничений	выбирать оптимальные способы решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	практическими навыками выбора оптимальных способов решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
		УК-2.3 Решает конкретные задач проекта заявленного качества и за установленное время	имеющиеся ресурсы и ограничения, оценивать и выбирать оптимальные способы решения поставленных задач	использовать имеющиеся ресурсы и знания о важнейших нормах, ограничений институтах и отраслях действующего российского права для	навыками работы в различных условиях с использованием аналитического оборудования

				определения круга задач и оптимальных способов их решения	
		УК-2.4 Публично представляет результаты решения конкретной задачи проекта	принципы и методы поиска, анализа и синтеза информации	применять принципы и методы поиска, анализа и синтеза информации	практическими навыками поиска, анализа и синтеза информациипрактике
УК-3	Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	УК-3.1 Понимает эффективность использования стратегии сотрудничества для достижения поставленной цели, определяет свою роль в команде	основные принципы командной работы	работать в команде на основе стратегии сотрудничества	способностью определять свою роль в командной работе для достижения поставленной цели
		УК-3.2 Понимает особенности поведения выделенных групп людей, с которыми работает/взаимодействует, учитывает их в своей деятельности (выбор категорий групп людей осуществляется образовательной организацией в зависимости от целей подготовки – по возрастным особенностям, поэтническому или религиозному признаку, социально незащищенные слои населения и т.п.).	сущность командных и личных интересов и особенности их согласования	выявлять особенности поведения и интересы участников командной работы	способностью реализовывать свою роль в командной работе с учетом особенностей поведения и интересов участников командной работы
		УК-3.3	особенности и	анализировать	способностью

		Эффективно взаимодействует с другими членами команды, в т.ч. участвует в обмене информацией, знаниями и опытом, и презентации результатов работы команды	стратегии межличностного взаимодействия в командной работе	возможные последствия личных действий в командной работе	строить продуктивное взаимодействие в команде на основе ответственного отношения к личным действиям
		УК-3.4 Предвидит результаты (последствия) личных действий и планирует последовательность шагов для достижения заданного результата	критерии оценки идей, информации, знаний и опыта	соблюдать правила и нормы командной работы	способностью нести личную ответственность в командной работ
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 на государственном и иностранном (-ых) языках коммуникативно приемлемые стиль делового общения, вербальные и невербальные средства взаимодействия с партнерами	принципы построения на русском и иностранном языках деловой устной и письменной коммуникации	применять на практике деловую коммуникацию в письменной форме	навыками чтения и перевода текстов на иностранном языке в профессиональном общении
		УК-4.2 Использует информационно-коммуникационные технологии при поиске необходимой информации в процессе решения стандартных коммуникативных задач на государственном и иностранном (-ых) языках	принципы построения и письменного высказывания на русском и иностранном языках	Применять на практике деловую коммуникацию в устной и письменной формах, навыки делового общения на русском и иностранном языках	навыками чтения и перевода текстов на иностранном языке в профессиональном общении, навыками деловых коммуникаций в устной и письменной формах на русском и иностранном

					языках
		УК-4.3 Ведет деловую переписку, учитывая особенности стилистики официальных и неофициальных писем, социокультурные различия в формате корреспонденции на государственном и иностранном (-ых) языках	принципы построения и письменного высказывания на русском и иностранном языках;	применять на практике деловую коммуникацию в устной и письменной формах	навыками чтения и перевода текстов на иностранном языке в профессиональном общении, навыками деловых коммуникаций в устной и письменной формах на русском и иностранном языках
		УК-4.4 Демонстрирует интегративные умения использовать диалогическое общение для сотрудничества в академической коммуникации общения: внимательно слушая и пытаясь понять суть идей других, даже если они противоречат собственным воззрениям; уважая высказывания других,как в плане содержания, так и в плане формы; критикуя аргументировано и конструктивно, не задевая чувств других; адаптируя речь и язык жестов к ситуациям взаимодействия.	правила и закономерности деловой устной и письменной коммуникации	методы и навыки делового общения на русском и иностранном языках	методикой составления суждений в межличностном деловом общении на русском и иностранном языках

		УК-4.5 Демонстрирует умение выполнять перевод профессиональных текстов с иностранного(-ых) на государственный язык и обратно.	основные правовые основы в области обеспечения информационной безопасности	применять на практике правовые акты	знаниями правовых основ в области обеспечения информационной безопасности
УК-5	Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах	УК-5.1 Находит и использует необходимую для саморазвития и взаимодействия с другими информацию о культурных особенностях и традициях различных социальных групп.	закономерности социально-исторического развития различных культур в этическом контексте	понимать и воспринимать разнообразие общества в социальноисторическом контексте	методами восприятия межкультурного разнообразия общества в социальноисторическом контексте.
		УК-5.2 Демонстрирует уважительное отношение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и	закономерности социально-исторического развития различных культур в этическом и философском контексте.	понимать и воспринимать разнообразие общества в социальноисторическом, этическом контекстах	методами восприятия межкультурного разнообразия общества в социальноисторическом, этическом и философском контекстах.

		этические учения			
		УК-5.3 Умеет не дискриминационно и конструктивно взаимодействовать с людьми с учетом их социокультурных особенностей в целях успешного выполнения профессиональных задач и усиления социальной интеграции	закономерности и особенности социально-исторического развития различных культур в этическом и философском контексте.	понимать и воспринимать разнообразие общества в социальноисторическом, этическом и философском контекстах.	методами восприятия межкультурного разнообразия общества в социальноисторическом, этическом и философском контекстах, навыками общения в мире культурного разнообразия с использованием этических форм поведения
УК-6	Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни	УК-6.1 Применяет знание о своих ресурсах и их пределах (личностных, ситуативных, временных и т.д.), для успешного выполнения порученной работы	инструменты и методы управления временем	использовать инструменты и методы управления временем	способностью управления временем при выполнении конкретных задач, проектов, при достижении поставленных целей
		УК-6.2 Понимает важность планирования перспективных целей собственной деятельности с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда	методы определения приоритетов личностного развития и профессионального роста	определять приоритеты и цели собственной деятельности	способностью реализовывать цели личностного развития и профессионального роста
		УК-6.3 Реализует намеченные цели	требования рынка труда и предложения	оценивать требования рынка труда и	способностью выстраивания траектории

		деятельности с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда	образовательных услуг в сфере профессиональной деятельности	предложения образовательных	собственного профессионального роста
		УК-6.4 Критически оценивает эффективность использования времени и других ресурсов при решения поставленных задач, а также относительно полученного результата.	принципы и методы управления временем	оптимально управлять своим временем для саморазвития на основе принципов образования в течение всей жизни	навыками приобретения новых знаний и навыков; оптимального управления своим временем для саморазвития на основе принципов образования в течение всей жизни
		УК-6.5 Демонстрирует интерес к учебе и использует предоставляемые возможности для приобретения новых знаний и навыков	методологию и методы проблематизации социальной реальности	использовать теоретические и эмпирические знания для выявления социально значимых проблем	способностью выявлять и обосновывать социально значимые проблемы
УК-7	Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	УК-7.1 Поддерживает должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности и соблюдает нормы здорового образа жизни	методы сохранения и укрепления физического здоровья в условиях полноценной социальной и профессиональной деятельности	организовывать режим времени, приводящий к здоровому образу жизни	опытом спортивной деятельности и физического самосовершенствования и самовоспитания
		УК-7.2 Использует	социально-гуманитарную	использовать средства и	способностью к организации

		основы физической культуры для осознанного выбора здоровьесберегающих технологий с учетом внутренних и внешних условий реализации конкретной профессиональной деятельности	роль физической культуры и спорта в развитии личности	методы физического воспитания для профессионально-личностного развития, физического самосовершенствования, формирования здорового образа	своей жизни в соответствии с социально-значимыми представлениями о здоровом образе жизни
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 чрезвычайной ситуации и военных конфликтов	УК-8.1 Обеспечивает безопасные и/или комфортные условия труда на рабочем месте, в т.ч. с помощью средств защиты	механизм распространения пламени по поверхности жидкостей и твердых горючих материалов, механизм их выгорания	рассчитывать объем и состав продуктов горения, теплоту сгорания и температуру горения; определять основные показатели пожарной опасности веществ и материалов (концентрационные пределы распространения пламени, температуру вспышки, температуру самовоспламенения и др.)	навыками проведения простых лабораторных исследований и построения по их результатам зависимостей влияния различных факторов на температуру вспышки и температуру самовоспламенения, на концентрационные пределы распространения пламени в паровоздушных смесях и скорость распространения пламени по горючим жидкостям и твердым материалам
		УК-8.2 Выявляет и устраняет проблемы, связанные с нарушениями техники безопасности на	физико-химические основы горения, теории горения, взрыва	проводить анализ изменения параметров горения в зависимости от различных	методами предсказания протекания возможных химических реакций и их кинетику

		рабочем месте		факторов	
		УК-8.3 Осуществляет действия по предотвращению возникновения чрезвычайных ситуаций (природного и техногенного происхождения) на рабочем месте, в т.ч. с помощью средств защиты.	организационные основы осуществления мероприятий по предупреждению и ликвидации последствий аварий и катастроф природного и антропогенного характера	анализировать и оценивать степень опасности	методикой идентификации негативных факторов источников чрезвычайных ситуаций
		УК-8.4 Принимает участие в спасательных и неотложных аварийно-восстановительных мероприятиях в случае возникновения чрезвычайных ситуаций.	особенности ЧС природного характера	осуществлять в общем виде оценку антропогенного воздействия на окружающую среду с учетом специфики природно-климатического условия	навыками оказание помощи пострадавшим в ЧС
УК-9	Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-9.1 Ознакомлен с основными документами, регламентирующими финансовую грамотность в профессиональной деятельности; источники финансирования профессиональной деятельности, критерии оценки затрат и обоснованности экономических решений	понятийный аппарат экономической науки	использовать методы экономического и планирования для достижения поставленной цели.	применения экономических инструментов для управления финансами.
		УК-9.2 Обосновывает экономический выбор в различных областях	понятийный аппарат экономической науки, базовые принципы	использовать методы экономического и финансового	применения экономических инструментов для управления финансами, с

		жизнедеятельности на основе учета факторов эффективности	функционирования экономики.	планирования для достижения поставленной цели.	учетом экономических и финансовых рисков в различных областях жизнедеятельности.
		УК-9.3 Планирует деятельность с учетом экономически оправданные затрат, направленных на достижение результата	принципы функционирования экономики, цели и механизмы основных видов социальной экономической политики	использовать методы экономического и финансового планирования для достижения поставленной цели	применения экономических инструментов для управления финансами, с учетом экономических и финансовых рисков в различных областях жизнедеятельности
УК-10	Способен формировать нетерпимое отношение к коррупционному поведению	УК-10.1 Знает действующие правовые нормы, обеспечивающие борьбу с коррупцией в различных областях жизнедеятельности; способы профилактики коррупции и формирования нетерпимого отношения к ней	основные термины и понятия гражданского права, используемые в антикоррупционном законодательстве	правильно толковать гражданско-правовые термины, используемые в антикоррупционном законодательстве	правильного толкования гражданскоправовых терминов, используемых в антикоррупционном законодательств
		УК-10.2 Осведомлен об ответственности за дачу либо за получение взятки, имеет сформированную гражданскую позицию нетерпимости к коррупции	основные термины и понятия гражданского права, используемые в антикоррупционном законодательстве, действующее антикоррупционное	правильно толковать гражданско-правовые термины, используемые в антикоррупционном законодательстве; давать оценку	правильного толкования гражданскоправовых терминов, используемых в антикоррупционном законодательстве, а также навыками применения на практике

			законодательство	коррупционному поведению и применять на практике антикоррупционное законодательство	антикоррупционного законодательства
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 Разрабатывает и реализовывает политики управления доступом в компьютерныйх системах	источники угроз безопасности информации	применять действующую законодательную базу в области обеспечения информационной безопасности и защиты информации	навыками сопровождения и управления системами защиты информации
		ОПК-1.2 Обеспечивает защиту информации при работе с базами данных, при передаче по компьютерным сетям)	структуру политики безопасности и основные законодательно-правовые положения защиты информации, виды и состав угроз информационной безопасности и меры из предотвращения	классифицировать угрозы информационной безопасности применительно к объектам защиты	навыками анализировать состояние информационной безопасности на конкретном объекте защиты, практическими навыками в использовании основных методов и средств обеспечения информационной безопасности
		ОПК-1.3 Оценивает уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	технологии хранения, поиска и сортировки информации	использовать информационные, компьютерные и сетевые технологии в профессиональной деятельности	приемами поиска, систематизации, хранения и обработки информации
ОПК-2	Способен применять информационно-	ОПК-2.1 Проводит анализ функционального процесса объекта	принципы организации информационных систем в	анализировать и оценивать угрозы информационн	методами и средствами выявления угроз

	коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;	защиты и его информационных составляющих с целью выявления возможных инсточников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	соответствии с требованиями по защите информации	ой безопасности обьекта	безопасности
		ОПК-2.2 Формирует предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям	структуру организации и управления деятельностью подразделений по защите объектов информатизации	проводить информационную характеристику и организационную структуру объектов информатизации предприятия	навыками выработки предложений о возможности внедрения дополнительных мер, в том числе, для обеспечения информационной безопасности функционирования информационных систем предприятия при взаимодействии с внешними информационными сетями
		ОПК-2.3 Разрабатывает , внедряет и сопровождает комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	цели, задачи, принципы и основные направления обеспечения информационной безопасности	анализировать качество средств и методов защиты информационных систем	навыками формальной постановки и решения задачи обеспечения информационной безопасности
		ОПК-2.4 Проводит аудит защищенности объекта информатизации в	методику проведения аудита информационной безопасности	оценивать эффективность и надежность защиты систем и	методами анализа и оценки механизмов защиты систем

		соответствии с нормативными документами	информационных систем и объектов информатизации	объектов информатизации	и объектов информатизации
ОПК-3	Способен использовать необходимые математические методы для решения задач профессиональной деятельности;	ОПК-3.1 Проводит работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от утечки по техническим каналам	Знает основы математики, основные понятия теории информации, основные методы оптимального кодирования источников информации	исследовать функциональные зависимости, возникающие при решении стандартных прикладных задач	навыками использования справочных материалов по математическому анализу, использования расчетных формул и таблиц при решении стандартных вероятностно-статистических задач, самостоятельного решения комбинированных задач
		ОПК-3.2 Проводит работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа	способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах	производить установку и настройку программно-технических средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами	навыками проведения работ по установке, настройке, испытаниям и техническому обслуживанию программно-технических средств защиты информации от несанкционированного доступа
		ОПК-3.3 Проводит контроль эффективности защиты информации от утечки по	технические каналы утечки информации	производить установку и монтаж технических средств защиты информации от	навыками проведения работ по установке, настройке, испытаниям и техническому

		техническим каналам		утечки в соответствии с техническим проектом, инструкциями по эксплуатации и эксплуатационно-техническими документами	обслуживанию технических средств защиты акустической речевой информации от утечки по техническим каналам
		ОПК-3.4 Проводит контроль эффективности защиты информации от несанкционированного доступа	методы защиты и контроля защищенности информации от несанкционированного доступа и специальных программных воздействий на нее	проводить техническое обслуживание программно-технических средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами	навыками проведения работ по установке, настройке, испытаниям и техническому обслуживанию программно-технических средств защиты информации от несанкционированного доступа
ОПК-4	Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности;	ОПК-4.1 Проводит организационные мероприятия по обеспечению безопасности информации в автоматизированных системах;	основополагающие принципы механики, термодинамики, молекулярной физики, квантовой физики; положения электричества и магнетизма, колебаний и оптики	делать выводы и формулировать их в виде отчета о проделанной исследовательской работе	методами расчета
		ОПК-4.2 Способен администрировать операционные системы, системы управления базами	основные направления администрирования компьютерных сетей	администрировать локальные вычислительные сети	навыками установки, настройки и сопровождения, контроле использования

		данных, вычислительные сети;			сервера и рабочих станций для безопасной передачи информации
		ОПК-4.3 Выполняет работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем;	технологию безопасности, протоколов авторизации, конфиденциальности и безопасности при работе с сетевыми ресурсами	принимать меры по устранению возможных сбоев	навыками обеспечения сетевой безопасности (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных), безопасность межсетевого взаимодействия
		ОПК-4.4 Осуществляет диагностику и мониторинг систем защиты автоматизированных систем;	об установке, настройке, обслуживании, диагностике, эксплуатации подсистем управления информационной безопасностью объекта защиты; перспективные современные методы и способы эксплуатации	принимать участие в установке, настройке, обслуживании, диагностике, эксплуатации подсистем управления информационной безопасностью объекта защиты	способностью принимать участие в установке, настройке, обслуживании, диагностике, эксплуатации подсистем управления информационной безопасностью объекта защиты
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в	ОПК-5.1 Применяет математические модели и решать задачи помехоустойчивого кодирования при проективании защищенных автоматизированных систем	основы математики, основные понятия теории информации, основные методы оптимального кодирования источников информации	исследовать функциональные зависимости, возникающие при решении стандартных прикладных задач	навыками использования справочных материалов по математическому анализу, использования расчетных формул и таблиц при решении стандартных

	сфере профессиональной деятельности;				вероятностно-статистических задач, самостоятельного решения комбинированных задач
		ОПК-5.2 Применяет технологии защиты информации при создании защищенных автоматизированных систем	классификацию современных компьютерных систем, типовые структуры и принципы организации компьютерных сетей; назначение, функции и обобщенную структуру операционных систем; назначение и основные компоненты систем баз данных	применять типовые программные средства сервисного назначения и пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет	навыками поиска информации в глобальной информационной сети Интернет; применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности
		ОПК-5.3 Осуществляет эксплуатацию и проводить техническое обслуживание защищенных автоматизированных систем	принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации	обеспечивать работоспособность, обнаруживать и устранять неисправности	навыками диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления
		ОПК-5.4 Проводит мониторинг функционирования защищенных автоматизированных систем	состав и принципы работы автоматизированных систем, операционных систем и сред	осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизиров	навыками эксплуатации компонентов систем защиты информации автоматизированных систем

				анных систем	
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.1 Использует нормативные правовые акты в профессиональной деятельности	основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры ответственности за утрату, разглашение, модификацию и уничтожение защищаемой информации	обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав	навыками разрабатывать локальные правовые документы, регламентирующие работу по обеспечению информационной безопасности в организации
		ОПК-6.2 Применяет нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности	нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	разрабатывать проекты локальных нормативных документов, регламентирующих защиту информации ограниченного доступа в организации	навыками по разработке политики безопасности объекта информатизации
		ОПК-6.3 Организовывает технологический	методы пресечения разглашения конфиденциаль	применять действующую законодательную	навыками сопровождения и управления

		процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами	ной информации	базу в области обеспечения информационной безопасности и защиты информации	системами защиты информации
ОПК-7	Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности;	ОПК-7.1 Применяет современные методы проектирования программного обеспечения, позволяющие вести разработку программных систем средней и высокой сложности	принципы информатики и широкой эрудиции в моделях и методах с ней связанных проектировать программно-аппаратные средства для решения практических задач на основе как неформального технического задания, так и формальных спецификаций	применять современные методы проектирования программного обеспечения, позволяющие вести разработку программных систем средней и высокой сложности	основными приемами функционального и логического программирования
		ОПК-7.2 Применяет современные технологии программирования для разработки компонентов аппаратно-программных комплексов и баз данных	методы настройки, наладки программно-аппаратных комплексов	анализировать техническую документацию, производить настройку, наладку и тестирование программно-аппаратных комплексов	навыками проверки работоспособности программно-аппаратных комплексов
		ОПК-7.3 Применять языки программирования и работы с базами данных, современные программные среды разработки информационных систем и технологий для автоматизации	основные языки программирования и работы с базами данных, операционные системы и оболочки, современные программные среды разработки информационных систем и	применять языки программирования и работы с базами данных, современные программные среды разработки информационных систем и технологий	основными методами решения типичных задач теории алгоритмов

		процессов, решения прикладных задач различных классов	технологий	для автоматизации бизнес-процессов, решения прикладных задач различных классов, ведения баз данных и информационных хранилищ	
ОПК-8	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	ОПК-8.1 Применяет стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы	принципы и порядок работы информационно-справочных систем; способы поиска и обработки информации, методы работы с научной информацией	обобщать, анализировать и систематизировать научную информацию в области информационной безопасности; пользоваться информационно-справочными системами	навыком составления и оформления отчетных документов по результатам обзора научно-технической литературы, нормативных и методических документов
		ОПК-8.2 Применяет принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	сущность и значение информации в развитии современного общества	на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности решать стандартные задачи	методами решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
		ОПК-8.3 Проводит решение стандартных задач профессиональной	принципы, методы и средства решения	решать стандартные задачи профессиональ	навыками подготовки обзоров, аннотаций,

		деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ОПК-9.1 Применяет математические модели и решать задачи криптографического преобразования при решении задач защиты информации	Математические модели, методы и алгоритмы решения типовых задач	строить алгоритмы решения типовых задач анализа информации	навыками оценки рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем
		ОПК-9.2 Определяет и анализирует технические каналы утечки информации	принципы работы с системами предотвращения утечек	изучать и анализировать характеристики и особенности применения основных приборов и оборудования, используемых для выявления каналов утечки информации	навыками расчета контролируемой зоны, в пределах которой могут происходить утечки информации
		ОПК-9.3 Проводит работы по установке и настройке средств технической защиты информации	технические описания и инструкции по эксплуатации технических средств обработки информации в защищенном исполнении	проводить техническое обслуживание защищенных технических средств обработки информации в соответствии с инструкциями по	навыками работы по установке и настройке средств технической защиты информации

				эксплуатации и эксплуатационно-технической документацией	
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 Способен организовывать и поддерживать выполнение комплекса мер по информационной безопасности	программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности	принципами формирования политики информационной безопасности объекта информатизации
		ОПК-10.2 Способен проводить построения как отдельных процессов управления информационной безопасностью, так и системы процессов в целом	стандартные вероятностно-статистические методы анализа экспериментальных данных	строить стандартные процедуры принятия решений, на основе имеющихся экспериментальных данных	навыками по проведению эксперимента по заданной методике с составлением итогового документа
		ОПК-10.3 Испотльзуя современные методы и средства разрабатывает процессы управления информационной безопасности, учитывающие особенности функционирования и решаемых задач, и оценивает их эффективность	способы поиска и обработки информации, методы работы с научной информацией	обобщать, анализировать и систематизировать научную информацию в области информационной безопасности	навыком составления и оформления отчетных документов по результатам обзора научно-технической литературы
ОПК-11	Способен проводить эксперименты по заданной методике и обработку их результатов;	ОПК-11.1 Проводит испытания по оценки защищенности объектов информатизацуии	стандартные вероятностно-статистические методы анализа экспериментальных данных	строить стандартные процедуры принятия решений, на основе имеющихся экспериментал	навыками по проведению эксперимента по заданной методике с составлением итогового документа

		на основе существующих методик ФСТЭК		ьных данных	
		ОПК-11.2 Способен проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	основные понятия и методы математической статистики	логически мыслить, подбирать формулы, соответствующие типам задач	основными приемами и способами вычисления вероятностей наступления случайных событий, их числовых характеристик, оценок
		ОПК-11.3 Приниает участие в проведении экспериментальных исследований системы защиты информации	основные понятия	логически мыслить, подбирать формулы, соответствующие типам задач	навыками использования математических моделей теории вероятностей и математической статистики
ОПК-12	Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.1 Проводит сбор исходных данных на объекте информатизации	принципы формирования политики информационной безопасности в информационных системах; основные этапы процесса проектирования и общие требования к содержанию проекта	определять информационную инфраструктуру и информационные ресурсы организации, подлежащих защите; анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации	навыками по разработке основных показателей технико-экономического обоснования соответствующих проектных решений
		ОПК-12.2 Осуществляет обработку и оценку исходных данных	основные виды и процедуры обработки информации, модели и методы решения задач обработки информации	осуществлять выбор модели и средства построения информационной системы и программных средств	навыками обеспечения сбора данных для анализа использования и функционирования информационной системы
		ОПК-12.3 Разрабатывает технико-экономическое	основы проведения технико-экономического	прогнозировать технико-экономические показатели	практическими навыками и умениями проведения

		обоснование проектных решений	обоснования		технико-экономического анализа
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 спользует базовые знания по всеобщей и отечественной истории для выражения своих мировозренческих установок и гражданской позиции	основные этапы и закономерности исторического развития российского общества, место и роль России в мировой истории и на современном этапе развития	использовать базовые знания по всеобщей и отечественной истории для выражения своих мировозренческих установок и гражданской позиции	навыками анализа основных этапов и закономерностей исторического развития России, её места и роли в современном мире в целях формирования гражданской позиции и развития патриотизма
		ОПК-13.2 Обладает навыками анализа основных этапов и закономерностей исторического развития России, её места и роли в современном мире в целях формирования гражданской позиции и развития патриотизма	основные закономерности развития общества, закономерности и этапы исторического процесса, сущность гражданства	ориентироваться в мировом историческом процессе, анализировать процессы и явления, происходящие в обществе	навыками целостного подхода к анализу проблем общества, навыками сбора, систематизации и самостоятельного анализа информации о социально-политических и экономических процессах
		ОПК-13.3 Ориентируется в хронологии исторического развития России, использовать базовые знания по отечественной истории в решении профессиональных задач в качестве иллюстраций и аргументов	хронологию основных событий истории России, базовые термины и понятия отечественной истории	ориентироваться в хронологии исторического развития России, использовать базовые знания по отечественной истории в решении профессиональных задач в качестве иллюстраций и аргументов	начальными навыками анализа отдельных событий отечественной истории в контексте мирового исторического процесса, обобщения исторических данных
ОПК-	Способен	ОПК-4.1.1	основные мероприятия по	использовать нормативно-	навыками работы с

4.1	проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах;	Организует и поддерживает выполнение комплекса мер по обеспечению информационной безопасности, управляет процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации	созданию и обеспечению функционирования комплексной системы защиты	правовую базу в решении задач обеспечения информационной безопасности и комплексной защиты информации на предприятии и в организации; строить концептуальные модели информационной безопасности объекта, формулировать основные задачи по созданию и обеспечению функционирования комплексной системы защиты на предприятии, в организации	нормативно-правовыми и организационно-распорядительными документами в сфере информационной безопасности
		ОПК-4.1.2 Обеспечивает блокирование возможных каналов утечки информации через технические средства с помощью специальных устройств	структуру государственной системы защиты информации от утечки по техническим каналам	изучать и анализировать характеристики и особенности применения основных приборов и оборудования, используемых для выявления каналов утечки информации	расчетом контролируемой зоны, в пределах которой могут происходить утечки информации
		ОПК-4.1.3 Осуществляет подбор, изучение и обобщение научно-технической литературы, нормативных и методических	принципы и порядок работы информационно-справочных систем; способы поиска и обработки информации, методы работы	обобщать, анализировать и систематизировать научную информацию в области информационной	навыком составления и оформления отчетных документов по результатам обзора научно-технической литературы,

		материалов по вопросам обеспечения информационной безопасности в автоматизированных системах	с научной информацией	безопасности; пользоваться информационно-справочными системами	нормативных и методических документов
ОПК-4.2	Способен администрировать операционные системы, системы управления базами данных, вычислительные сети;	ОПК-4.2.1 Применяет особенности и способы программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных	средства, методы и протоколы идентификации, аутентификации и авторизации	устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации	навыками управления полномочиями пользователей
		ОПК-4.2.2 Владеет технологиями проектирования информационных систем, выбора архитектуры и комплексирования аппаратных и программных средств администрирования и управления в информационных системах	основные методы и приемы реализации функций администрирования информационных систем	выполнять анализ возможных нарушений информационной безопасности	выбора архитектуры и комплексирования аппаратных и программных средств администрирования и управления в информационных системах
		ОПК-4.2.3 Определяет задачи администрирования для конкретного случая; выполняет анализ возможных нарушений информационной безопасности	основные методы и приемы реализации функций администрирования информационных систем	определить задачи администрирования для конкретного случая	технологиями проектирования информационных систем
ОПК-4.3	Способен выполнять работы по установке, настройке,	ОПК-4.3.1 Способен применять основные угрозы компьютерной	основные угрозы компьютерной информации, реализуемые на	определять рациональные меры для выбора необходимых	методами защиты информации в операционных системах и в

	администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем;	информации, реализуемые на различных уровнях программной иерархии и типы атак	различных уровнях программной иерархии и типы атак	средств защиты информации и уметь их оценивать	пользовательских приложениях
		ОПК-4.3.2 Выявляет принципы построения подсистем защиты компьютерной информации в операционных системах и в пользовательских программных приложениях	основные принципы построения подсистем защиты компьютерной информации в операционных системах и в пользовательских программных приложениях	выявлять слабости защиты ОС, ВС и СУБД и использовать их для вскрытия защиты	навыками анализа и администрирования подсистем защиты современных ОС, ВС и СУБД
		ОПК-4.3.3 Способен использовать сертифицированные и перспективные программно-аппаратные средства и методы защиты компьютерной информации (в том числе криптографических)	сертифицированные и перспективные программно-аппаратные средства и методы защиты компьютерной информации	применять и администрировать средства программно-аппаратной защиты информации	навыками использования межсетевых экранов и систем обнаружения вторжений
		ОПК-4.3.4 Выявляет средства и методы защиты от НСД хранимой информации с использованием возможностей устройств	средства и методы защиты от НСД хранимой информации с использованием возможностей устройств записи и чтения	планировать программно-аппаратную подсистему политики безопасности организации	методами защиты компьютерной информации от НСД
ОПК-4.4	Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем;	ОПК-4.4.1 Способен диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции систем защиты	методы тестирования функций отдельных программных и программно-аппаратных средств защиты	диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции	навыками тестирования функций, диагностики, устранения отказов и восстановления работоспособности

		автоматизированных систем	информации	программно-аппаратных средств защиты информации	программных и программно-аппаратных средств защиты информации
		ОПК-4.4.2 Способен осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации	особенности и способы применения программных и программно-аппаратных средств защиты информации	устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации	навыками использования программных и программно-аппаратных средств для защиты информации в сети
		ОПК-4.4.3 Применяет типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа	номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации	применять инженерно-технические средства физической защиты объектов информатизации	навыки выявлении технических каналов утечки информации
ПК-1	Способен составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	ПК-1.1 Разрабатывает предложения по совершенствованию системы управления защиты информации автоматизированных систем	основные меры по выполнения обеспечения информационной безопасности	разрабатывать меры по обеспечению информационной безопасности	навыками разработки мер поддержки обеспечения информационной безопасности
		ПК-1.2 Применяет технические средства контроля эффективности мер защиты информации	основные этапы контрольных проверок технических средств защиты информации	разрабатывать методику контрольных проверок технических средств защиты информации	навыками применения контрольных проверок
ПК-2	Способен администрировать средства защиты информации в компьютерных системах и	ПК-2.1 Осуществляет выбор и настройку средств защиты информации в компьютерных системах и сетях	об установке, настройке, обслуживании, диагностике, эксплуатации подсистем управления	принимать участие в установке, настройке, обслуживании, диагностике, эксплуатации	способностью принимать участие в установке, настройке, обслуживании, диагностике,

	сетях		информационной безопасностью объекта защиты	подсистем управления информационной безопасностью объекта защиты	эксплуатации подсистем управления информационной безопасностью объекта защиты
ПК-3	Способен анализировать и противодействовать угрозам информации операционных систем, систем управления базами данных, вычислительных сетей	ПК-3.1 Выявляет потенциальные угрозы	источники угроз безопасности информации и меры по их предотвращению	классифицировать потенциальные угрозы безопасности информации	комплексом мер по информационной безопасности
		ПК-3 .2 Разрабатывает меры противодействия потенциальным угрозам	источники угроз безопасности информации и меры по их предотвращению	классифицировать защищаемую информацию по видам тайны и степеням секретности	методами разработки компонентов по обеспечению информационной безопасности объекта защиты
ПК-4	Способен оценивать последствия от реализации угроз безопасности информации в автоматизированной системе	ПК-4.1 Оценивает информационные риски в автоматизированных системах	основные методики анализа угроз и рисков информационной безопасности	анализировать угрозы и проводить риск-анализ и реализовывать методики управления рисками с целью обеспечения безопасности объектов информатизации	технологиями обеспечения информационной безопасности в части проведения риск-анализа и управления риска
		ПК-4.2 Способен классифицировать и оценивать угрозы безопасности информации	источники и классификацию угроз информационной безопасности	классифицировать и оценивать угрозы информационной безопасности	способностью классифицировать и оценивать угрозы безопасности информации
		ПК-4.3 Определяет подлежащие защите информационные ресурсы автоматизированных систем	состав и принципы работы автоматизированных систем	осуществлять настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизиров	навыками определения и настройка компонентов систем защиты информации автоматизированных (информационных) систем

				анных систем	
		ПК-4.4 Применяет нормативные документы по противодействию технической разведки	основные руководящие и нормативные документы в сфере инженерно-технической защите информации	использовать основные руководящие и нормативные документы в сфере инженерно-технической защите информации	навыками работы с профессиональными аппаратными средствами инженерно-технической защиты информации
ПК-5	Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	ПК-5.1 Применяет существующие методики для аттестации объектов информатизации	основные понятия информационной безопасности	разрабатывать политику информационной безопасности на аттестуемых объектах	методами разработки политики информационной безопасности на аттестуемых объектах
ПК-6	Способен проводить анализ рисков информационной безопасности автоматизированной системы	ПК-6.1 Проводит оценку рисков информационной безопасности на основе существующих методик	методики оценки риска и управления рисками, а также тестирования средств обеспечения информационной безопасности	анализировать угрозы и оценивать риски информационной безопасности с целью обеспечения безопасности объектов информатизации	средствами обеспечения информационной безопасности, анализа угроз, риск-анализа и управления рисками
ПК-7	Способен разрабатывать комплекс мероприятий по защите информации в автоматизированных системах финансовых и экономических структур	ПК-7.1 Учитывает и использует правовые нормы реализации профессиональной детельности в облсти обеспечения инфрмационной безопсности и защиты интересов личности , обества и государства	технологии и нормы обеспечения информационной безопасности	обеспечивать информационную безопасность при интеграции в государственную и международную информационную среду	способами практического обеспечения норм информационной безопасности при интеграции в государственную и международную информационную среду
		ПК-7.2 Реализует	принципы организации	осуществлять меры	навыками безопасного

		комплекс мероприятий по защите информации в автоматизированных системах финансовых и экономических структур	информационных систем в соответствии с требованиями по защите информации	противодействия нарушениям информационной безопасности	использования технических сред
ПК-8	Способен проводить анализ информационной безопасности объектов и систем на соответсвие требований стандартов и нормативно-правовых актов в области информационной безопасности	ПК-8.1 Применяет стандарты и нормативно-правовые акты в области информационной безопасности	правила и нормативные требования к оформлению технической документации с учетом действующих методических документов	применять действующие нормативные и методические документы в области информационной безопасности	навыками оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов
ПК-9	Способен применять технические средства защиты информации на основе знаний физических законов	ПК-9.1 Выявляет технические каналы утечки на основе знаний физических законов	основные способы физической защиты объектов информатизации	применять инженерно-технические средства физической защиты объектов информатизации	навыками применения основных типов технических средств защиты информации
		ПК-9.2 Осуществляет сбор и анализ исходных данных для расчета и проектирования радиоэлектронных устройств и систем	принцип работы	самостоятельно проектировать	навыками осуществлять сбор и анализ исходных данных для расчета и проектирования
ПК-10	Способен разрабатывать компьютерные модели исследуемых процессов и систем и применять их	ПК-10.1 Использует современное программное обеспечение в области разработки компьютерной	понятийный аппарат (используемые термины и определения) современной сферы компьютерной	создавать и редактировать изображения в специализированных программах обработки графической	методами использования информационных технологий для решения задач компьютерной графики

	для определения оптимальных вариантов проектных, конструкторских и технологических решений	графики	графики	информации	
ПК-11	Способен участвовать в проектировании системы управления информационной безопасностью	ПК-10.1 Осуществляет проектирование средств защиты информации автоматизированных систем	методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации	применять программные и программно-аппаратные средства для защиты информации в базах данных	навыками обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами

2. Программа государственного экзамена (не предусмотрена УП)

3.Требования к выпускным квалификационным работам

3.1. Тематика выпускных квалификационных работ

по направлению подготовки 10.03.01 Информационная безопасность профиль «Безопасность автоматизированных систем»

1. Анализ организации защиты информации на предприятии и ее совершенствование на основе снижения демаскирующих признаков объектов защиты.
2. Анализ системы обеспечения информационной безопасности предприятия и разработка предложений по ее совершенствованию.
3. Анализ эффективности защиты информации в локальной вычислительной сети хозяйствующего субъекта (на конкретном примере) и разработка мероприятий по ее повышению.
4. Анализ эффективности защиты конфиденциальной информации в организации и разработка рекомендаций по ее повышению.
5. Анализ эффективности мероприятий по защите информации, циркулирующей в защищаемых помещениях хозяйствующего субъекта (на конкретном примере), и разработка рекомендаций по ее повышению.
6. Анализ эффективности организации технической защиты конфиденциальной информации хозяйствующего субъекта (на конкретном примере) и разработка рекомендаций по ее повышению.
7. Анализ эффективности противодействия утечке информации по техническим каналам в системах связи предприятия (организации) и разработка мероприятий по ее повышению.
8. Защита информации в системе поддержки принятия решения по отбору персонала.
9. Комплексный анализ угроз и уязвимостей информационной системы хозяйствующего субъекта (на конкретном примере) на основе метода многофакторного анализа.
10. Модернизация комплексной системы защиты информации предприятия.

11. Модернизация подсистемы защиты конфиденциального документооборота на основе криптографических средств.
12. Модернизация программно-аппаратной защиты конфиденциальной информации при передаче ее в открытых каналах связи.
13. Модернизация системы защиты информационных ресурсов предприятия.
14. Модернизация системы защиты конфиденциальной информации на основе программно-аппаратных средств.
15. Модернизация системы защиты персональных данных предприятия.
16. Модернизация системы защиты электронного документооборота предприятия.
17. Модернизация системы информационной безопасности АСУТП и П предприятия.
18. Модернизация системы информационной безопасности предприятия.
19. Обеспечение информационной безопасности в организации (на предприятии) на основе технических средств охраны.
20. Организация защиты корпоративной информационной системы хозяйствующего субъекта (на конкретном примере) на основе типовых решений (на конкретных примерах).
21. Организация межсетевого взаимодействия между предприятием и его филиалом.
22. Организация системы антивирусной защиты информационной инфраструктуры хозяйствующего субъекта (на конкретном примере) на основе оценки отечественного и зарубежного рынка.
23. Оценка защищенности веб-приложения предприятия.
24. Оценка защищенности конфиденциальной информации от утечки за счет наводок на технические средства, системы и их коммуникации линиям связи.
25. Оценка защищенности конфиденциальной от утечки за счет побочных электромагнитных излучений и наводок при использовании электронно-вычислительной техники.
26. Оценка защищенности помещения от утечки речевой информации по каналам электроакустических преобразований.
27. Оценка защищенности помещения от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам.
28. Оценка состояния акустической защищенности помещений при добывании конфиденциальной информации с использованием инфразвука.
29. Оценка эффективности системы противодействия утечке информации по ПЭМИН в режимном помещении и разработка рекомендаций по ее повышению (С).
30. Повышение эффективности программно-аппаратной защиты конфиденциальной информации.
31. Прогнозирование эффективности средств защиты информации предприятия.
32. Проектирование комплексной системы защиты информации на предприятии.
33. Проектирование системы защиты информации на предприятии.
34. Проектирование системы защиты информации от утечки по каналам связи.
35. Проектирование системы защиты информации от утечки по техническим каналам.
36. Проектирование системы защиты информационных ресурсов предприятия (организации) при проведении электронных торгов.
37. Проектирование системы защиты компьютерной информации на объектах информационной инфраструктуры предприятия.
38. Проектирование системы защиты конфиденциальной информации предприятия.
39. Проектирование системы защиты персональных данных в организации (на предприятии).
40. Проектирование системы инженерно-технической защиты выделенного помещения.
41. Проектирование системы обнаружения возможных каналов утечки сведений, относящихся к конфиденциальной информации.
42. Проектирование системы охраны режимных помещений в организации (на предприятии).

43. Проектирование системы программно-аппаратной защиты информации предприятия на основе методов криптозащиты.
44. Проектирование системы технической защиты средств обработки, хранения и передачи информации в организации.
45. Разработка и внедрение шпионского программного обеспечения с использованием Rootkit - технологии на АРМ администратора безопасности предприятия.
46. Разработка комплекса мер по криптографической защите информации на предприятии.
47. Разработка методики анализа и оценки угроз информационной безопасности для предприятия.
48. Разработка методики оценки рисков информационной безопасности хозяйствующего субъекта (на конкретном примере) на основе моделирования угроз и уязвимостей его информационной системы.
49. Разработка методики проведения мероприятий по обнаружению и поиску устройств несанкционированного съема информации в защищаемом помещении хозяйствующего субъекта (на конкретном примере).
50. Разработка организационно - технических мероприятий по защите информации для диспетчерской службы ГБУЗ «Клиническая станция скорой медицинской помощи» г. Оренбурга
51. Разработка подсистемы обеспечения информационной безопасности.
52. Разработка предложений по проведению мероприятий по лицензированию объекта информационной системы хозяйствующего субъекта (на конкретном примере) в области защиты информации.
53. Разработка предложений по проведению мероприятий по сертификации объекта информационной системы хозяйствующего субъекта в области защиты информации (на конкретном примере).
54. Разработка проекта охраны режимных помещений в организации (на предприятии).
55. Разработка рекомендаций по организации подготовки и проведения совещаний по конфиденциальным вопросам.
56. Разработка системы внутриобъектового и пропускного режимов на предприятии с помощью инженерно-технических средств защиты на объекте информатизации.
57. Разработка системы защиты информации от утечки на основе показателей аттестации защищаемого помещения.
58. Разработка системы защиты информации по противодействию утечки информации по каналам связи.
59. Разработка системы защиты информационных ресурсов в автоматизированной системе предприятия.
60. Разработка системы комплексной защиты конфиденциальной информации организации.
61. Разработка системы материально-технического обеспечения функционирования КСЗИ предприятия.
62. Разработка системы нормативно-методического обеспечения функционирования КСЗИ предприятия.
63. Разработка системы охраны предприятия.
64. Разработка системы программно-аппаратной защиты конфиденциальной информации в локально-вычислительной сети.
65. Разработка системы программно-аппаратной защиты объекта информатизации от несанкционированных воздействий.
66. Системный анализ информационной инфраструктуры и разработка защищенной корпоративной информационной системы предприятия (на конкретном примере).
67. Совершенствование криптографической защиты информации в информационной системе хозяйствующего субъекта (на конкретном примере) на основе анализа современных предложений.
68. Совершенствование системы защиты информации на предприятии.

69. Совершенствование системы защиты информационной сети предприятия.
70. Совершенствование состояния акустической защищенности выделенного помещения.
71. Сравнительный анализ безопасности электронных платежных систем (на конкретных примерах).

3.2 Порядок выполнения выпускных квалификационных работ

Выполнение выпускных квалификационных работ является заключительным этапом обучения студентов и имеет своей целью:

- систематизацию, закрепление и расширение теоретических знаний по направлению подготовки 10.03.01 «Информационная безопасность» и применение этих знаний при решении конкретных практических задач;

- развитие навыков ведения самостоятельной работы, овладение методикой исследования и эксперимента при решении разрабатываемых в ВКР проблем и вопросов.

Студенту может предоставляться право выбора темы ВКР вплоть до предложения своей темы с необходимым обоснованием целесообразности её разработки.

Тематика ВКР должна соответствовать требованиям ФГОС ВО, рекомендациям учебно-методических объединений, быть актуальной, соответствовать современному состоянию и перспективам развития науки и техники.

Выпускная квалификационная работа должна содержать:

- обоснование актуальности выбранной темы и новизны работы;
- постановку задач, решаемых в ходе исследования;
- обзор использованных источников и предыдущих исследований по данной тематике;
- обоснование избранной тематики исследования;
- сведения об апробации результатов исследования в виде публикаций, докладов на студенческих научных конференциях, семинарах и т.п.;
- изложение результатов исследования и их анализ;
- выводы и (или) рекомендации;
- список использованных источников и литературы.

В структуру ВКР входит:

- титульный лист;
- задание;
- реферат;
- оглавление;
-введение;
- содержание;
-заключение;
- библиографический список;
- приложения.

При подготовке ВКР каждому обучающемуся университета назначается руководитель, рецензент и, при необходимости, консультанты. Закрепление студента за руководителем и утверждение темы работы оформляется распоряжением директора института, по представлению заведующего кафедрой с учетом личного письменного заявления студента.

В обязанности руководителя входит:

- составление задания и графика выполнения ВКР;

- оказание необходимой помощи студенту при составлении плана ВКР, при подборе литературы и фактического материала в ходе преддипломной практики;

- консультирование студента по вопросам согласно установленному на семестр графику консультаций;

- постоянный контроль за сроками выполнения ВКР, своевременностью и качеством написания отдельных глав и разделов работы с отметкой в графике;

- составление задания на преддипломную практику по изучению объекта практики и сбору материала для выполнения выпускной работы;

- оформление отзыва на ВКР;

- практическая помощь студенту в подготовке текста доклада и иллюстративного материала к защите;

- присутствие на заседании ГЭК при защите выпускником ВКР.

В отзыве руководителя следует отразить:

- подготовленность выпускника к профессиональной деятельности в соответствии с ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность»;

- умение работать с литературой (насколько выпускник ознакомлен с современными литературными источниками по рассматриваемой проблеме);

- умение отстаивать собственную точку зрения, делать обоснованные выводы и предложения.

В соответствии с вышеуказанными требованиями научный руководитель в отзыве выставляет соответствующую оценку – «отлично», «хорошо», «удовлетворительно».

На завершающем этапе выполнения ВКР на выпускающей кафедре проводится предварительная защита (предзащита). Предзащита организуется в форме обсуждения выпускной квалификационной работы. Студент, не аттестованный по результатам предзащиты ВКР, может быть отчислен из университета за невыполнение учебного плана. В случае наличия уважительных причин, подтвержденных документально, студенту устанавливаются индивидуальный порядок и сроки выполнения и защиты ВКР.

При планировании учебного процесса на подготовку ВКР должно предусматриваться определённое время, продолжительность которого регламентируется ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность».

К защите допускается лицо, успешно сдавшее государственный экзамен.

Выпускная квалификационная работа должна быть напечатана в соответствии с требованиями Единой системы конструкторской документации (ЕСКД) — комплекса государственных стандартов, устанавливающих взаимосвязанные правила, требования и нормы по разработке, оформлению и обращению конструкторской документации на стандартном листе писчей бумаги в формате А4 с соблюдением следующих требований:

- поля: левое – 30 мм, правое – 20 мм, верхнее – 20 мм, нижнее – 20 мм;

- шрифт размером 14 пт, гарнитурой Times New Roman;

- межстрочный интервал – полуторный;

- отступ красной строки – 1,5 см;

- выравнивание текста – по ширине.

Объем выпускной квалификационной работы, как правило, выполняется на 50-60 страницах. Для восприятия результатов работы, необходимо представить 6-7 листов иллюстрированного материала в виде карт, схем, рисунков, графиков и фотографий.

Выпускные квалификационные работы подлежат обязательному рецензированию.

В рецензии дается характеристика ВКР в целом и ее отдельных разделов, оценивается актуальность темы, теоретическая и практическая значимость работы, использование новейших достижений в данном направлении науки, соответствие содержания поставленным целям и задачам. Рецензент оценивает теоретическую подготовку выпускника, его умение самостоятельно использовать полученные профессиональные знания и исследовательские умения для решения конкретных задач, отмечает обоснованность выводов и рекомендаций, грамотность оформления, достаточность иллюстративного материала и т.д. В рецензии указываются разделы, где имеются недостатки. Рецензент дает общую оценку работы («отлично», «хорошо», «удовлетворительно», «неудовлетворительно») и может выразить мнение о присвоении студенту квалификации «инженер».

Оформленная в установленном порядке ВКР с отзывом научного руководителя и рецензией представляется в экзаменационную комиссию не позднее, чем за три дня до назначенного срока защиты.

Защита ВКР проводится в соответствии с утвержденным графиком проведения государственных аттестационных испытаний на заседании ГЭК по направлению подготовки 10.03.01 «Информационная безопасность». Защита начинается с доклада студента по теме ВКР.

Выпускник должен излагать основное содержание своей ВКР свободно, не читая письменного текста. В процессе доклада используется компьютерная презентация работы, подготовленный наглядный графический (таблицы, схемы) или иной материал, иллюстрирующий основные положения работы. После завершения доклада члены ГЭК задают выпускнику вопросы как непосредственно связанные с темой ВКР, так и близко к ней относящиеся. При ответах на вопросы студент имеет право пользоваться своей работой. После окончания обсуждения выпускнику предоставляется заключительное слово. В своём заключительном слове выпускник должен ответить на замечания рецензента. После заключительного слова выпускника процедура защиты ВКР считается оконченной.

3.3 Порядок защиты выпускной квалификационной работы

Защита выпускной квалификационной работы является завершающим этапом государственной итоговой аттестации выпускника.

Сроки выполнения выпускной квалификационной работы определяются учебным планом и графиком учебного процесса.

Выпускная квалификационная работа выполняется студентов в соответствии с календарным планом, подписанным студентом, руководителем и утвержденным заведующим кафедрой не позднее, чем за год до защиты. Студент может быть не допущен к защите выпускной квалификационной работы в ГЭК в следующих случаях:

1. Невыполнение учебного плана в положенные сроки.
2. Срыв сроков подготовки выпускной квалификационной работы, получение

отрицательного отзыва руководителя; подготовка ВКР, не отвечающей предъявленным к ней требованиям.

3. По решению заведующего кафедрой при несовпадении мнений с научным руководителем при представлении работы неудовлетворительного качества после прохождения предварительной защиты.

Выпускная квалификационная работа оценивается на степень самостоятельности выполнения. Данную работу проводит ответственный работник кафедры, на которой закреплен выпускник. На плагиат проверяется только конечная версия ВКР; проходной процент своего, то есть оригинального текста будет доведен до руководителей.

Электронная версия выпускной квалификационной работы сдается ответственному по антиплагиату на CD-R, CD-RW носителях за две недели до предполагаемой защиты.

Отчет об антиплагиате подписывается ответственным за данный вид работы на кафедре. Только после этого на выпускную квалификационную работу может быть выдан отзыв руководителя.

Выполненная выпускная квалификационная работа подлежит рецензированию.

Список рецензентов утверждается приказом ректора вместе с утверждением тематики ВКР.

Законченная выпускная квалификационная работа, подписанная студентом, консультантом, имеющая отзыв научного руководителя и подписанная заведующим

кафедрой, направляется на рецензирование. Оформленная выпускная квалификационная работа должна быть представлена на рецензию студентом лично не позднее, чем за 10 дней до защиты.

Заведующий кафедрой после ознакомления с отзывом руководителя и рецензией решает вопрос о допуске студента к защите и передает выпускную квалификационную работу в ГЭК.

Не позднее, чем за 7 дней до защиты выпускник предоставляет секретарю ГЭК следующие организационные документы:

1. Выпускную квалификационную работу, полностью оформленную и содержащую титульный лист, подписанный выпускником, руководителем и заведующим кафедрой (первый лист сшиваемого текста); заполненный бланк задания по выполнению работы (второй лист сшиваемого текста); календарный план, подписанный выпускником, руководителем, утвержденный заведующим кафедрой (третий лист сшиваемого текста); текст ВКР с содержанием, списком использованных источников и приложениями (сшиваемый).

2. Отзыв руководителя (вкладывается).

3. Рецензия (вкладывается).

4. Отчет об антиплагиате (вкладывается).

5. Справка о результатах внедрения решений, разработанных в данной выпускной квалификационной работе (подшивается в конце ВКР после приложений).

Защита ВКР проводится на открытом заседании Государственной

экзаменационной комиссии (ГЭК), в состав которой входят директор Института управления рисками и комплексной безопасности, заведующие кафедр института, преподаватели кафедр института, представители производства,

Списки студентов, допущенных к защите, предоставляются в ГЭК деканатом института.

На заседании могут присутствовать руководители ВКР, а также студенты и все заинтересованные лица.

Защита ВКР происходит в следующей последовательности:

1) секретарь ГЭК объявляет фамилию студента, зачитывает тему ВКР;

2) заслушивается доклад студента (не более 10 минут);

3) члены ГЭК задают вопросы по существу работы, а также вопросы, отвечающие общим требованиям к профессиональному уровню выпускника, предусмотренные федеральным государственным образовательным стандартом высшего образования по данному направлению подготовки.

4) студент отвечает на вопросы;

5) секретарем ГЭК зачитывается отзыв руководителя ВКР и рецензия;

6) заслушиваются ответы студента на замечания рецензента;

7) затем студенту предоставляется заключительное слово.

Задача ГЭК - выявление подготовленности студента к профессиональной деятельности и принятие решения о том, можно ли выпускнику присвоить квалификацию «бакалавр» по направлению подготовки 10.03.01 «Информационная безопасность».

Студент, получив разрешение о допуске к защите, должен подготовить доклад (до 10 минут), в котором четко и кратко излагаются основные положения ВКР. Для удобства доклада

и наглядности специалист должен использовать демонстрационный материал (презентацию и графический материал), согласованный с научным руководителем.

Краткий доклад может быть подготовлен письменно. В докладе необходимо отразить:

- обоснование актуальности выбранной темы;
- цель и задачи ВКР;
- используемые методы при проведении анализа;
- характеристики объекта исследования;
- краткое содержание работы, обращая особое внимание на освещенный в работе передовой опыт и отличительные недостатки в практике учетно-аналитической работы;
- выводы и рекомендации, которые, по мнению студента-выпускника, будут способствовать обеспечению информационной безопасности.

Доклад не следует перегружать цифровыми показателями, а привести лишь те данные, на которые сделаны ссылки в раздаточных материалах.

По окончании доклада докладчику задают вопросы председатель, члены государственной экзаменационной комиссии, присутствующие. Количество вопросов, задаваемых студенту при защите выпускной квалификационной работы, не ограничивается. Вопросы могут быть заданы как непосредственно по теме защищаемой работы, так и по другим дисциплинам направления подготовки. Нужно давать самый короткий из всех возможных ответов и не повторять фрагменты доклада. Ответы на вопросы должны быть убедительны, теоретически обоснованы, а при необходимости подкреплены цифровым материалом.

По докладу и ответам на вопросы государственная экзаменационная комиссия судит о широте кругозора выпускника, его эрудиции, умении публично выступать и аргументированно отстаивать свою точку зрения при ответах на вопросы. Таким образом, ответы на вопросы, их полнота и глубина, влияют на оценку по защите ВКР, поэтому их необходимо тщательно продумывать.

Оценка результата защиты выпускной квалификационной работы производится на закрытом заседании ГЭК. При оценке принимаются во внимание оригинальность и научно-практическое значение темы, качество выполнения и оформления работы, а также содержательность доклада и ответов на вопросы.

Оценка объявляется после окончания защиты всех работ на открытом заседании ГЭК.

Студенту, проявившему себя в научной работе, сдавшему курсовые экзамены с оценкой ≪отлично≫ не менее чем по 75 % всех дисциплин учебного плана, а по остальным дисциплинам - с оценкой ≪хорошо≫, а также защитившему выпускную квалификационную работу с оценкой ≪отлично≫, выдается диплом с отличием.

При получении оценки ≪неудовлетворительно≫ на защите выпускной квалификационной работы обучаемый имеет право на повторную защиту. Повторное прохождение итоговых аттестационных испытаний назначается не ранее чем через три месяца.

После защиты ВКР остается на выпускающей кафедре.

3.4 Критерии оценки защиты выпускных квалификационных работ

Оценка	Показатели оценивания	Характеристика оценки
«Отлично»	Научный уровень доклада, степень освещенности в нем вопросов темы исследования, значение сделанных выводов и предложений для организации использование специальной научной литературы, нормативных актов, материалов производственной практики	выставляется, если: - при выполнении ВКР выпускник продемонстрировал полное соответствие уровня своей подготовки требованиям ФГОС ВО, показал глубокие знания и умения; - представленная к защите работа выполнена в полном соответствии с заданием, отличается глубиной профессиональной проработки всех разделов ее содержательной части,

	Стиль изложения, правильность и научная обоснованность выводов Оформление ВКР Качество ответов на вопросы членов государственной экзаменационной комиссии	выполнена и оформлена качественно и в соответствии с установленными правилами; - в докладе исчерпывающе, последовательно, четко, логически стройно и кратко изложена суть работы и ее основные результаты; - на все вопросы членов государственной экзаменационной комиссии даны обстоятельные и правильные ответы; - критические замечания научного руководителя выпускником проанализированы, и в процессе защиты приведены аргументированные доказательства правильности решений, принятых в работе.
«Хорошо»	Научный уровень доклада, степень освещенности в нем вопросов темы исследования, значение сделанных выводов и предложений для организации, использование специальной научной литературы, нормативных актов, материалов производственной практики Стиль изложения, правильность и научная обоснованность выводов Оформление ВКР Качество ответов на вопросы членов государственной экзаменационной комиссии	выставляется, если: - при выполнении ВКР выпускник продемонстрировал соответствие уровня своей подготовки требованиям ФГОС ВО, показал достаточно хорошие знания и умения; - представленная к защите работа выполнена в полном соответствии с заданием, отличается глубиной профессиональной проработки всех разделов ее содержательной части, выполнена и оформлена качественно и в соответствии с установленными правилами; - в докладе правильно изложена суть работы и ее основные результаты, однако при изложении допущены отдельные неточности; - на большинство вопросов членов государственной экзаменационной комиссии даны правильные ответы; - критические замечания научного руководителя выпускником проанализированы, и в процессе защиты приведены аргументированные доказательства правильности решений, принятых в работе.
«Удовлетворительно»	Научный уровень доклада, степень освещенности в нем вопросов темы исследования, значение сделанных выводов и предложений для организации, использование специальной научной литературы, нормативных	выставляется, если: - при выполнении ВКР выпускник продемонстрировал соответствие уровня своей подготовки требованиям ФГОС ВО, показал удовлетворительные знания и умения; - представленная к защите работа выполнена в соответствии с заданием,

	актов, материалов производственной практики Стиль изложения, правильность и научная обоснованность выводов Оформление ВКР Качество ответов на вопросы членов государственной экзаменационной комиссии	но без достаточно глубокой проработки некоторых разделов, имеют место несущественные ошибки и нарушения установленных правил оформления работы; - в докладе изложена суть работы и ее результаты; - на вопросы членов государственной экзаменационной комиссии выпускник отвечает, но неуверенно; - не все критические замечания научного руководителя проанализированы правильно.
«Неудовлетворительно»	Научный уровень доклада, степень освещенности в нем вопросов темы исследования, значение сделанных выводов и предложений для организации использование специальной научной литературы, нормативных актов, материалов производственной практики Стиль изложения, правильность и научная обоснованность выводов Оформление ВКР Качество ответов на вопросы членов государственной экзаменационной комиссии	выставляется тогда, когда: - в ВКР обнаружены значительные ошибки, свидетельствующие о том, что уровень подготовки выпускника не соответствует требованиям федерального государственного образовательного стандарта; - при решении задач, сформулированных в задании, выпускник не показывает необходимых знаний и умений; - доклад затянут по времени и (или) читался с листа; - на большинство вопросов членов государственной экзаменационной комиссии ответы даны неправильные или не даны вообще.

3.5 Литература для выполнения выпускной квалификационной работы

Основная литература:

1.Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург: Лань, 2019.—344с.—ISBN 978-5-8114-3940-9.Текст:электронный//Лань: электронно-библиотечная система.

2. Голиков, А. М. Основы информационной безопасности : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2007. — 201 с. — ISBN 978-5-868889-467-1. — Текст : электронный // Лань : электронно-библиотечная система.

Дополнительная литература:

1. 1. Информационные технологии. Базовый курс : учебник для вузов / А. В. Костюк, С. А. Бобонец, А. В. Флегонтов, А. К. Черных. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 604 с. — ISBN 978-5-8114-8776-9. — Текст : электронный // Лань : электронно-библиотечная система.

2. Мошак, Н. Н. Защищенные информационные системы : учебное пособие / Н. Н. Мошак,Л. К. Птицына. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 216 с. — Текст : электронный // Лань : электронно-библиотечная система.

4. Порядок подачи и рассмотрения апелляций

4.1 По результатам государственных аттестационных испытаний обучающийся имеет право на апелляцию.

4.2 Обучающийся имеет право подать в апелляционную комиссию письменное заявление о нарушении, по его мнению, установленной процедуры проведения государственного аттестационного испытания и (или) несогласии с результатами государственного аттестационного испытания. см. Приложения А, Б.

4.3 Заявление подается лично обучающимся в апелляционную комиссию не позднее следующего рабочего дня после объявления результатов государственного аттестационного испытания.

4.4 Для рассмотрения апелляции секретарь государственной экзаменационной комиссии направляет в апелляционную комиссию протокол заседания государственной экзаменационной комиссии, заключение председателя государственной экзаменационной комиссии о соблюдении процедурных вопросов при проведении государственного аттестационного испытания, а также выпускную квалификационную работу, отзыв и рецензию (рецензии) (для рассмотрения апелляции по проведению защиты выпускной

квалификационной работы).

4.5 Апелляция рассматривается не позднее 2 рабочих дней со дня подачи заявления на заседании апелляционной комиссии, на которое приглашаются председатель государственной экзаменационной комиссии и обучающийся, подавший апелляционное заявление.

Решение апелляционной комиссии доводится до сведения обучающегося, подавшего заявление, в течение 3 рабочих дней со дня заседания апелляционной комиссии. Факт ознакомления обучающегося, подавшего апелляцию, с решением апелляционной комиссии удостоверяется подписью обучающегося.

Решения, принятые апелляционной комиссией, оформляются протоколами.

Протоколы заседаний комиссии подписываются членами комиссии, секретарем комиссии, а также обучающимся, подававшим апелляционное заявление см. Приложения В, Г.

4.6 При рассмотрении апелляции о нарушении порядка проведения государственного аттестационного испытания апелляционная комиссия принимает одно из следующих решений:

- об отклонении апелляции, если изложенные в ней сведения о нарушениях процедуры проведения государственной итоговой аттестации обучающегося не подтвердились и (или) не повлияли на результат государственного аттестационного испытания;
- об удовлетворении апелляции, если изложенные в ней сведения о допущенных нарушениях процедуры проведения государственной итоговой аттестации обучающегося подтвердились и повлияли на результат государственного аттестационного испытания.

В случае, указанном в абзаце третьем настоящего пункта, результат проведения государственного аттестационного испытания подлежит аннулированию, в связи с чем протокол о рассмотрении апелляции не позднее следующего рабочего дня передается в государственную экзаменационную комиссию для реализации решения апелляционной комиссии. Обучающемуся предоставляется возможность пройти государственное аттестационное испытание в сроки, установленные образовательной организацией.

4.7 При рассмотрении апелляции о несогласии с результатами государственного аттестационного испытания апелляционная комиссия выносит одно из следующих решений:

- об отклонении апелляции и сохранении результата государственного аттестационного испытания;
- об удовлетворении апелляции и выставлении иного результата государственного аттестационного испытания.

Решение апелляционной комиссии не позднее следующего рабочего дня передается в государственную экзаменационную комиссию. Решение апелляционной комиссии является основанием для аннулирования ранее выставленного результата государственного аттестационного испытания и выставления нового.

4.8 Решение апелляционной комиссии является окончательным и пересмотру не подлежит.

4.9 Повторное проведение государственного аттестационного испытания осуществляется в присутствии одного из членов апелляционной комиссии не позднее 15 июля.

4.10 Апелляция на повторное проведение государственного аттестационного испытания не принимается.

Программа разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 10.03.01 «Информационная безопасность»

Приложение А

Форма апелляционного заявления о нарушении установленной процедуры проведения государственного аттестационного испытания

Федеральное государственное бюджетное образовательное учреждение
высшего образования
≪Оренбургский государственный аграрный университет≫

Председателю апелляционной комиссии
_____
(Фамилия И.О.)
обучающегося _____ группы
по направлению подготовки _____
_____
(указать направление подготовки)
_____
(Фамилия)
_____
(Имя)
_____
(Отчество)
документ, удостоверяющий личность
_____
(серия, номер)

Заявление

Прошу комиссию рассмотреть мою апелляцию по процедуре проведения
_____
(наименование государственного аттестационного испытания)
Краткое содержание претензии: _____
_____
_____
_____
_____

Указанный выше факт существенно затруднил для меня выполнение экзаменационных заданий *(процесс ответа на заданные вопросы),* что привело к необъективной оценки моих знаний.

_____/_____/ _____20___г.
(подпись заявителя) (расшифровка подписи)

_____
_____

Заполняется *секретарем /удостоверяющим лицом* апелляционной комиссии

Дата объявления результатов ГИА: ≪___≫ _____ 20___г.
Дата *подачи (принятия)* заявления: ≪___≫ _____ 20___г.
Заявление принял: _____
(должность)
_____/_____
подпись удостоверяющего лица *расшифровка подписи*

Приложение Б

Форма апелляционного заявления о несогласии с результатами государственного аттестационного испытания

Федеральное государственное бюджетное образовательное учреждение
высшего образования
≪Оренбургский государственный аграрный университет≫

Председателю апелляционной комиссии
_____
(Фамилия И.О.)
обучающегося _____ группы
по направлению подготовки _____
_____
(указать направление подготовки)
_____
(Фамилия)
_____
(Имя)
_____
(Отчество)
документ, удостоверяющий личность
_____
(серия, номер)

Заявление

Прошу пересмотреть, в моем присутствии, выставленные мне результаты по
_____
(наименование государственного аттестационного испытания)
так как, по моему мнению, данные мною ответы на заданные вопросы были оценены не верно.

_____/_____/ _____20___г.
(подпись заявителя) (расшифровка подписи)

_____

_____

Заполняется *секретарем удостоверяющим лицом* апелляционной комиссии
Дата объявления результатов ГИА: ≪___≫ _____ 20___г.
Дата *подачи (принятия)* заявления: ≪___≫ _____ 20___г.
Заявление принял: _____
(должность)
_____/_____
подпись удостоверяющего лица расшифровка подписи

Приложение В

Форма протокола о рассмотрении апелляции о нарушении проведения процедуры государственной итоговой аттестации.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
≪Оренбургский государственный аграрный университет≫

Протокол рассмотрения апелляции о нарушении проведения процедуры государственной итоговой аттестации.

№ ____ ≪___≫_____20___г.
Сведения об *участнике ГИА*
ФИО полностью_____
форма обучения _____
направление подготовки_____

КРАТКОЕ СОДЕРЖАНИЕ АПЕЛЛЯЦИИ: _____
_____
_____
_____
_____

Комиссия:
Председатель
апелляционной комиссии_____
Члены комиссии:
_____
_____
_____

рассмотрев обстоятельства, изложенные в поданной апелляции, считает, что вышеизложенные факты:
_____
_____
имели, не имели место
влияние вышеуказанных фактов на результаты государственного аттестационного испытания *значимо, незначимо*
рекомендовано комиссии апелляцию *принять, отклонить*

Решение апелляционной комиссии:
признать вышеизложенные факты действительно имевшими место быть *да, нет*
признать вышеизложенные факты значимыми *да, нет*
принять апелляцию *да, нет*

Председатель апелляционной комиссии: _____/_____
подпись расшифровка подписи
Члены апелляционной комиссии: _____/_____
_____/_____
Секретарь комиссии: _____/_____
Дата принятия решения ≪___≫ _____20___г.
С решением апелляционной комиссии ознакомлен:
≪__≫ _____ 20__г. _____/_____
подпись расшифровка подпись

Приложение Г

Форма протокола о рассмотрении апелляции по результатам государственной итоговой аттестации.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
≪Оренбургский государственный аграрный университет≫

Протокол рассмотрения апелляции по результатам государственной итоговой аттестации.

№ ____ ≪___≫_____20___г.
Сведения об *участнике ГИА*
ФИО полностью_____
форма обучения _____
направление подготовки_____
КРАТКОЕ СОДЕРЖАНИЕ АПЕЛЛЯЦИИ: _____
_____
_____
_____
_____
Комиссия:
Председатель
апелляционной комиссии_____
Члены комиссии:
_____
_____
_____
рассмотрев апелляцию о несогласии с выставленной оценкой, считает, что
вышеизложенные факты _____
_____
имели, не имели место
Решение апелляционной комиссии:
признать вышеизложенные факты действительно имевшими место *да, нет*
признать вышеизложенные факты значимыми *да, нет*
принять апелляцию *да, нет*
Председатель апелляционной комиссии: _____/_____
подпись расшифровка подписи
Члены апелляционной комиссии: _____/_____
_____/_____
Дата принятия решения ≪___≫ _____20___г.
С решением апелляционной комиссии ознакомлен:
≪__≫ _____ 20__г. _____/_____
подпись расшифровка подписи

Программа разработана в соответствии с Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

Разработал(и):

Заведующий кафедрой,к.т.н. _____ Урбан Владимир Александрович

Рабочая программа рассмотрена и одобрена на заседании кафедры Техносферной и информационной безопасности, протокол № 6 от 17.01.2024 г.

Зав. кафедрой _____ Урбан Владимир Александрович

Программа рассмотрена и утверждена на заседании Ученого совета Института управления рисками и комплексной безопасности, протокол № 7 от 23.02.2024 г.

Директор Института управления рисками и комплексной безопасности
_____ Яковлева Евгения Васильевна