

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Амурский государственный университет"

УТВЕРЖДАЮ

Проректор по учебной и
научной работе

Лейфа А.В. Лейфа

26 апреля 2024 г.

ПРОГРАММА

государственной итоговой аттестации выпускников по направлению подготовки
10.03.01 Информационная безопасность

Направленность (профиль) образовательной программы – Безопасность
автоматизированных систем (по отраслям или в сфере профессиональной деятельности)

Квалификация выпускника – Бакалавр

Год набора – 2024

Форма обучения – Очная

2024

Программа разработана на основании квалификационных требований ФГОС ВО 10.03.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 17.11.20 № 1427

Ответственный разработчик

доцент С.Г. Самохвалова

Самохвалова

Программа обсуждена на заседании кафедры информационной безопасности, 01.02.2024 г., протокол № 8

Заведующий кафедрой Никифорова Л.В. Никифорова

СОГЛАСОВАНО

Научная библиотека

Петрович О.В. Петрович

26 апреля 2024 г.

СОГЛАСОВАНО

Центр цифровой трансформации и
технического обеспечения

Тодосейчук А.А. Тодосейчук

26 апреля 2024 г.

1 Общие положения

1.1. Федеральным государственным образовательным стандартом ВО по 10.03.01 Информационная безопасность, утвержденным приказом Министерством науки и высшего образования РФ 17.11.20 № 1427 предусмотрена государственная итоговая аттестация выпускников в виде:

а) защиты выпускной квалификационной работы

1.2 Виды деятельности выпускников и соответствующие им типы задач профессиональной деятельности:

1.2.1 Виды деятельности выпускников
эксплуатационная;
проектно-технологическая;
организационно-управленческая.

1.2.2 Типы задач профессиональной деятельности
Выпускник, освоивший программу бакалавриата, в соответствии с видами профессиональной деятельности, на которые ориентирована программа бакалавриата, должен быть готов решать следующие профессиональные задачи:

эксплуатационная деятельность:

установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;

администрирование подсистем информационной безопасности объекта;

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

проектно-технологическая деятельность:

сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;

проведение проектных расчетов элементов систем обеспечения информационной безопасности;

участие в разработке технологической и эксплуатационной документации;

проведение предварительного технико-экономического обоснования проектных расчетов;

организационно-управленческая деятельность:

осуществление организационно-правового обеспечения информационной безопасности объекта защиты;

организация работы малых коллективов исполнителей;

участие в совершенствовании системы управления информационной безопасностью;

изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;

контроль эффективности реализации политики информационной безопасности объекта защиты.

1.2.3. Требования к профессиональной подготовленности выпускника, необходимые для выполнения им задач профессиональной деятельности

Компетенции выпускника, формируемые в процессе освоения данной ОП ВО, определяются на основе ФГОС ВО по соответствующему направлению подготовки 10.03.01 Информационная безопасность.

Результаты освоения ОП ВО определяются приобретаемыми выпускником компетенциями, т.е. его способностью применять знания, умения, опыт и личностные

качества в соответствии с задачами профессиональной деятельности.

а) Универсальные компетенции и индикаторы их достижения

Категория (группа) универсальных компетенций	Код и наименование универсальной компетенции	Код и наименование индикатора достижения универсальной компетенции
Системное критическое мышление	УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	ИД-1УК-1- знает принципы сбора, отбора и обобщения информации ИД-2УК-1- умеет соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности ИД-3УК-1- имеет практический опыт работы с информационными источниками, опыт научного поиска, создания научных текстов
Разработка и реализация проектов	УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	ИД-1УК-2- знает необходимые для осуществления профессиональной деятельности правовые нормы ИД-2УК-2- умеет определять круг задач в рамках избранных видов профессиональной деятельности, планировать собственную деятельность исходя из имеющихся ресурсов; соотносить главное и второстепенное, решать поставленные задачи в рамках избранных видов профессиональной деятельности ИД-3УК-2- имеет практический опыт применения нормативной базы и решения задач в области избранных видов профессиональной деятельности
Командная работа и лидерство	УК-3 Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	ИД-1УК-3- знает различные приемы и способы социализации личности и социального взаимодействия ИД-2УК-3- умеет строить отношения с окружающими людьми, с коллегами ИД-3УК-3- имеет практический опыт участия в командной работе, в социальных проектах, распределения ролей в условиях командного взаимодействия
Коммуникация	УК-4 Способен осуществлять деловую коммуникацию в устной и письменной формах на	ИД-1УК-4- знает литературную форму государственного языка, основы устной и письменной коммуникации на иностранном языке, функциональные стили

	<p>государственном языке Российской Федерации и иностранном(ых) языке(ах)</p>	<p>родного языка, требования к деловой коммуникации ИД-2УК-4- умеет выражать свои мысли на государственном, родном и иностранном языке в ситуации деловой коммуникации ИД-3УК-4- имеет практический опыт составления текстов на государственном и родном языках, опыт перевода текстов с иностранного языка на родной, опыт говорения на государственном и иностранном языках</p>
<p>Межкультурное взаимодействие</p>	<p>УК-5 Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах</p>	<p>ИД-1УК-5. Знает закономерности и особенности социально-исторического развития различных культур в социально-историческом, этическом и философском контекстах ИД-2УК-5. Умеет понимать, воспринимать и анализировать разнообразие общества в социально-историческом, этическом и философском контекстах ИД-3УК-5. Владеет способами адекватного восприятия межкультурного разнообразия общества в социально-историческом, этическом и философском контекстах ИД4УК-5 Демонстрирует толерантное восприятие социальных и культурных различий, уважительное и бережное отношение к историческому наследию и культурным традициям. ИД5УК-5 Находит и использует необходимую для саморазвития и взаимодействия с другими людьми информацию о культурных особенностях и традициях различных социальных групп. ИД6УК-5 Проявляет в своём поведении уважительное отношение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России в контексте мировой истории и культурных традиций мира. ИД7УК-5 Сознательно выбирает ценностные ориентиры и</p>

		гражданскую позицию; аргументировано обсуждает и решает проблемы мировоззренческого, общественного и личностного характера
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-6 Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни	ИД-1УК-6- знает основные принципы самовоспитания и самообразования, профессионального и личностного развития, исходя из этапов карьерного роста и требований рынка труда ИД-2УК-6- умеет планировать свое рабочее время и время для саморазвития. формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, индивидуально-личностных особенностей ИД-3УК-6- имеет практический опыт получения дополнительного образования, изучения дополнительных образовательных программ
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-7 Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	ИД-1УК-7- знает основы здорового образа жизни, здоровьесберегающих технологий, физической культуры ИД-2УК-7- умеет выполнять комплекс физкультурных упражнений ИД-3УК-7- имеет практический опыт занятий физической культурой
Безопасность жизнедеятельности	УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных	ИД-1УК-8. знает основные природные и техно- сферные опасности, их свойства и характеристики, характер воздействия вредных и опасных факторов на человека и природную среду, принципы, методы и средства защиты от них; ИД-2УК-8. - умеет создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в

	ситуаций и военных конфликтов	том числе при угрозе и возникновении чрезвычайных ситуаций и воен-ных, конфликтов; ИД-3УК-8 - владеет понятийно-терминологическим аппаратом, законодательными и правовыми основами в области безопасности жизнедеятельности; принципами, методами и средствами защиты природной среды и человека в повседневной жизни и в профессиональной деятельности, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов.
Экономическая культура, в том числе финансовая грамотность	УК-9 Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	ИД-1 УК-9 - знает принципы и способы обоснования экономических решений в различных областях жизнедеятельности; ИД-2УК-9- умеет анализировать возможные альтернативные решения на основе знаний об экономике и финансах; ИД-3УК-9 - владеет навыками выбора обоснованных экономических решений из нескольких альтернатив в различных жизненных ситуациях, требующих знаний в области экономики и финансов
Гражданская позиция	УК-10 Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	ИД-1 УК-10 - знает: понятие и виды коррупции, антикоррупционное законодательство, способы противодействия коррупции; правовые и организационные основы противодействия экстремистской деятельности; правовые основы и основные принципы противодействия терроризму; ИД-2 УК-10 - умеет: использовать полученные знания для понимания тенденции развития антикоррупционной политики государства, выявления, предупреждения и пресечения экстремистской деятельности, профилактики терроризма и борьбы с ним; анализировать юридические факты и возникающие в связи с ними отношения,

		противодействовать экстремизму, терроризму, коррупционному поведению в профессиональной деятельности; ИД-3 УК-10 – владеет: юридической терминологией в сфере противодействия коррупции, экстремистской деятельности, терроризму; навыками работы с правовыми и правоприменительными актами
--	--	--

б) Общепрофессиональные компетенции и индикаторы их достижения

Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ИД-1ОПК-1- знает понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности РФ, основы государственной информационной политики, источники и классификацию угроз информационной безопасности, понятия информационного противоборства, информационной войны и формы их проявлений в современном мире, понятие манипулирования как средства скрытого управления личностью и обществом ИД-2ОПК-1- умеет классифицировать угрозы информационной безопасности, ИД-3ОПК-1 - имеет практический опыт применения простейших способов обеспечения собственной информационно-психологической безопасности в различных коммуникативных ситуациях, в том числе при работе в сети Интернет
ОПК-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе, отечественного производства, для решения задач профессиональной деятельности	ИД-1ОПК-2. знает: состав, назначение функциональных компонентов и программного обеспечения персонального компьютера, формы и способы представления данных в персональном компьютере, типовые структуры и принципы организации компьютерных сетей назначение, функции и обобщённую структуру операционных систем назначение и основные компоненты систем баз данных ИД-2ОПК-2 умеет: применять типовые программные средства сервисного назначения и пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет, составлять SQL запросы и осуществлять удалённый доступ к базам данных, определять состав компьютера: тип процессора и его

	<p>параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств ИД-3ОПК-2. владеет: навыками поиска информации в глобальной информационной сети Интернет</p>
<p>ОПК-3. Способен использовать необходимые математические методы для решения задач профессиональной деятельности;</p>	<p>ИД-1ОПК-3- знать: основные понятия теории пределов и непрерывности функций одной и нескольких действительных переменных, основные методы дифференциального исчисления функций одной и нескольких действительных переменных, основные методы интегрального исчисления функций одной и нескольких действительных переменных, основные методы исследования числовых и функциональных рядов, основные задачи теории функций комплексного переменного, основные типы обыкновенных дифференциальных уравнений и методы их решения, основные понятия теории вероятностей, числовые и функциональные характеристики распределений случайных величин и их основные свойства, основные понятия теории случайных процессов, основы линейной алгебры над произвольными полями и свойства векторных пространств, основные понятия, составляющие предмет дискретной математики, основные понятия теории информации (энтропия, взаимная информация, источники сообщений, каналы связи, коды), понятие пропускной способности канала связи, прямую и обратную теоремы кодирования (без доказательства), основные методы оптимального кодирования источников информации (код Хаффмана) и помехоустойчивого кодирования каналов связи (линейные коды, циклические коды, код Хэмминга). ИД-2ОПК-3- уметь: исследовать функциональные зависимости, возникающие при решении стандартных прикладных задач, использовать типовые модели и методы математического анализа при решении стандартных прикладных задач, применять стандартные вероятностные и статистические модели к решению типовых прикладных задач, использовать расчетные формулы и таблицы при решении стандартных вероятностно-статистических задач, исследовать простейшие геометрические объекты по их уравнениям в различных системах координат, решать основные задачи линейной алгебры, в частности системы линейных уравнений над полями, применять стандартные методы дискретной математики к решению типовых задач, вычислять теоретико-информационные характеристики</p>

	<p>источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность), решать типовые задачи кодирования и декодирования</p> <p>ИД-ЗОПК-3- иметь навыки: типовых расчетов с использованием основных формул дифференциального и интегрального исчисления, навыками использования справочных материалов по математическому анализу, навыками самостоятельного решения комбинаторных задач</p>
<p>ОПК-4. Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности;</p>	<p>ИИД-1ОПК-4- знает: основополагающие принципы механики, основополагающие принципы термодинамики и молекулярной физики, основные законы электричества и магнетизма, основы теории колебаний и оптики, основополагающие принципы квантовой физики;</p> <p>ИД-2ОПК-4- знает: основные законы электротехники, элементы электрических цепей, методы анализа электрических цепей в переходных и установившихся режимах в частотной и временной областях, основополагающие принципы работы элементов и функциональных узлов электронной аппаратуры средств защиты информации;</p> <p>ИД-3ОПК-4- уметь: решать базовые прикладные физические задачи, измерять параметры электрической цепи;</p> <p>ИД-4ОПК-4- иметь навыки: теоретического и экспериментального исследования объектов профессиональной деятельности</p>
<p>ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;</p>	<p>ИД-1ОПК-5 знает: основы законодательства Российской Федерации, систему нормативных правовых актов, нормативных и методических документов в области информационной безопасности и защиты информации, правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации, правовые основы организации делопроизводства, виды и состав документации современной организации;</p> <p>ИД-2 ОПК-5 умеет: формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации, обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, определять</p>

	<p>виды документов, необходимых для оформления управленческих действий в профессиональной деятельности, грамотно составлять и оформлять служебные документы.</p> <p>ИД-3 ОПК-5 владеет: действиями (навыками) по применению нормативных правовых актов, нормативных и методических документов, регламентирующие деятельность по защите информации в сфере профессиональной деятельности</p>
<p>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;</p>	<p>ИД-1ОПК-6 знает: систему стандартов и нормативных правовых актов уполномоченных федеральных органов исполнительной власти по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, систему нормативных правовых актов уполномоченных федеральных органов исполнительной власти по аттестации объектов информатизации и сертификации средств защиты информации, систему правовых и организационных мер, направленных на защиту документальных материалов ограниченного доступа;</p> <p>ИД-2 ОПК-6 умеет: определить политику контроля доступа работников к информации ограниченного доступа, формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации;</p> <p>ИД-3 ОПК-6 владеет: действиями (навыками) по применению нормативных правовых актов, нормативных и методических документов, регламентирующие деятельность по защите информации ограниченного доступа в сфере профессиональной деятельности, используя нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;</p>
<p>ОПК-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности;</p>	<p>ИД-1ОПК-7- знать: области и особенности применения языков программирования высокого уровня, язык программирования высокого уровня (структурное, объектно-ориентированное программирование), базовые структуры данных, основные алгоритмы сортировки и поиска данных, основные комбинаторные и теоретико-графовые алгоритмы, общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения</p> <p>ИД-2ОПК-7- уметь: работать с интегрированной</p>

	<p>средой разработки программного обеспечения, разрабатывать программы для работы с файлами как с источником данных, применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач</p> <p>ИД-3ОПК-7- иметь навыки: программирования, отладки и тестирования прототипов программно-технических комплексов задач</p>
<p>ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;</p>	<p>ИД-1ОПК-8- знать: статус и порядок работы основных правовых информационно-справочных систем, способы поиска и работы с источниками научно-технической информации, принципы и правила построения суждений и оценок, цели, задачи и основные методы научных исследований;</p> <p>ИД-2ОПК-8- уметь: обобщать, анализировать и систематизировать научную информацию в области информационной безопасности, различать факты, интерпретации, оценки и аргументированно отстаивать свою позицию в процессе коммуникации</p> <p>ИД-3ОПК-8-иметь навыки: осуществления подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;</p>
<p>ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;</p>	<p>ИД-1ОПК-9- знать: основные понятия и задачи криптографии, математические модели криптографических систем, основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и криптографические протоколы, национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения</p> <p>ИД-2ОПК-9-уметь: использовать СКЗИ для решения задач профессиональной деятельности</p> <p>ИД-3ОПК-9- владеть навыками: применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности</p>
<p>ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать</p>	<p>ИД-1ОПК-10- знать: цели и задачи управления информационной безопасностью, основные документы по стандартизации в сфере управления информационной безопасностью, принципы формирования политики информационной безопасности объекта информатизации, принципы</p>

<p>и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;</p>	<p>организации информационных систем в соответствии с требованиями по защите информации, особенности комплексного подхода к обеспечению информационной безопасности организации</p> <p>ИД-2ОПК-10- уметь: разрабатывать модели угроз и модели нарушителя объекта информатизации, оценивать информационные риски объекта информатизации, определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите, разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации</p> <p>ИД-3ОПК-10- иметь навыки: участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;</p>
<p>ОПК-11. Способен проводить эксперименты по заданной методике и обработку их результатов;</p>	<p>ИД-1ОПК-11 знает: методику проведения экспериментов и методику обработки их результатов.</p> <p>ИД-1ОПК-11 умеет: проводить эксперименты по заданной методике и обработку их результатов</p> <p>ИД-1ОПК-11 владеет: практическими навыками проведения экспериментов по заданной методике</p>
<p>ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;</p>	<p>ИД-1ОПК-12-знать: жизненные циклы управляемых процессов: жизненный цикл изделия, жизненный цикл программного продукта, реализуемого в информационной системе, требования Единой системы конструкторской документации и Единой системы программной документации в части разработки технической документации, методы, показатели и критерии технико-экономического обоснования проектных решений при разработке систем и средств обеспечения защиты информации с учетом действующих нормативных и методических документов,</p> <p>ИД-2ОПК-12- уметь: разрабатывать основные показатели технико-экономического обоснования соответствующих проектных решений;</p> <p>ИД-3ОПК-12- иметь навыки: владения подготовкой исходных данных для проектирования подсистем, средствами обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений</p>
<p>ОПК-13. Способен анализировать основные этапы и закономерности</p>	<p>ИД-1ОПК-13знать: периодизацию, основные факты, явления и процессы всемирной и отечественной истории,</p>

<p>исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма.</p>	<p>особенности исторического пути России, ее место и роль в мировом сообществе в контексте всеобщей истории ИД-2ОПК-13уметь: анализировать основные этапы и законо-мерности исторического развития России, в том числе для формирования гражданской позиции и развития патриотизма ИД-3ОПК-13владеть: навыками анализа причинно-следственных связей в развитии российского государства и общества; места человека в историческом процессе и политической организации общества; навыками уважительного и бережного отношения к историческому наследию и культурным традициям России</p>
<p>ОПК-4.1 Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах.</p>	<p>ИД-1ОПК-4.1 знать: руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации, содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации ИД-2ОПК-4.1 уметь: определять подлежащие защите информационные ресурсы автоматизированных систем, разрабатывать политики безопасности информации автоматизированных систем, определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы, осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации ИД-3ОПК- 4.1владеть навыками проведения организационных мероприятий по обеспечению безопасности информации в автоматизированных системах</p>
<p>ОПК-4.2 Способен администрировать операционные системы, системы управления базами данных, вычислительные сети</p>	<p>ИД-1ОПК-4.2 знать: типовые средства, методы и протоколы идентификации, аутентификации и авторизации, критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем, содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем ИД-2ОПК-4.2 умеет: создавать, удалять и изменять учетные записи пользователей автоматизированной системы, устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации, регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах, применять типовые</p>

	<p>программные средства резервирования и восстановления информации в автоматизированных системах, документировать действия по устранению неисправностей в работе системы защиты информации автоматизированной системы</p> <p>ИД-3ОПК-4.2 владеет: навыками установки обновлений программного обеспечения автоматизированной системы, навыками обнаружения и устранения неисправностей в работе системы защиты информации автоматизированной системы</p>
<p>ОПК-4.3 Способен выполнять работу по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем</p>	<p>ИД-1ОПК-4.3 знать: основные меры по защите информации в автоматизированных системах, содержание эксплуатационной документации автоматизированной системы</p> <p>ИД-2ОПК-4.3 уметь: устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации, проводить анализ доступных информационных источников с целью выявления известных уязвимостей используемых в системе защиты информации программных и программно-аппаратных средств</p> <p>ИД-3ОПК-4.3 владеть: навыками осуществления автономной наладки технических и программных средств системы защиты информации автоматизированной системы</p>
<p>ОПК-4.4 Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем</p>	<p>ИД-1ОПК-4.4 знать: критерии оценки защищенности автоматизированной системы, знать технические средства контроля эффективности мер защиты информации</p> <p>ИД-1ОПК-4.4 уметь: осуществлять контроль обеспечения уровня защищенности в автоматизированных системах, контролировать события безопасности и действия пользователей автоматизированных систем, документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы</p> <p>ИД-1ОПК-4.4 владеть: навыками оценки защищенности автоматизированных систем с помощью типовых программных средств</p>

в) Профессиональные компетенции и индикаторы их достижения

Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
<p>ПК-1 Способен выполнять работы по установке и настройке средств</p>	<p>ИД-1ПК-1- знать: известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации,</p>

<p>защиты информации в автоматизированных системах</p>	<p>основные меры по защите информации в автоматизированных системах ИД-2ПК-1- уметь: применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации, проводить анализ структурных и функциональных схем защищенной автоматизированной системы ИД-3ПК-1 — иметь навык эксплуатации программно- аппаратных и технических средств защиты информации</p>
<p>ПК-2 Способен принимать участие в организации и проведения аудита защищенности информации в автоматизированных системах</p>	<p>ИД-1ПК-2- знать: методы контроля эффективности защиты информации от утечки по техническим каналам ИД-2ПК-2- уметь: разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем ИД-3ПК-2 - иметь навык применения инструментальных средств контроля защищенности информации в автоматизированных системах</p>
<p>ПК-3 Способен выполнять комплекс задач администрирования систем защиты информации автоматизированных систем</p>	<p>ИД-1ПК-3- знать: принципы формирования политики информационной безопасности в автоматизированных системах, программно- аппаратные средства защиты информации автоматизированных систем ИД-2ПК-3- уметь: создавать, удалять и изменять учетные записи пользователей автоматизированной системы, устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации ИД-3ПК-3 — иметь навык установки и настройки операционных систем, систем управления базами данных, компьютерных сетей и программных систем с учетом требований по обеспечению защиты информации, управления полномочиями пользователей автоматизированной системы</p>
<p>ПК-4 Способен участвовать в работах по разработке организационно- распорядительных документов по защите информации в автоматизированных системах</p>	<p>ИД-1ПК-4-знать: основные угрозы безопасности информации и модели нарушителя в автоматизированных системах, принципы построения средств защиты информации от утечки по техническим каналам, нормативные правовые акты в области защиты информации ИД-2ПК-4- уметь: применять нормативные документы по противодействию технической разведке, контролировать эффективность принятых мер по защите информации в автоматизированных системах ИД-3ПК-4 - иметь навыки определения правил и</p>

	процедур управления системой защиты информации автоматизированной системы, определение правил и процедур реагирования на инциденты
ПК-5 Способен управлять защитой информации в автоматизированных системах	ИД-1ПК-5- знать: методы защиты информации от утечки по техническим каналам, национальные, межгосударственные и международные стандарты в области защиты информации, основные угрозы безопасности информации и модели нарушителя в автоматизированных системах ИД-2ПК-5- уметь: Оценивать информационные риски в автоматизированных системах, классифицировать и оценивать угрозы безопасности информации ИД-3ПК-5 - иметь навык анализа воздействия изменений конфигурации автоматизированной системы на ее защищенность, анализ изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации
ПК-6 Способен внедрять организационные меры по защите информации в автоматизированных системах	ИД-1ПК-6-знать: организационные меры по защите информации ИД-2ПК-6- уметь: реализовывать правила разграничения доступа персонала к объектам доступа, анализировать программные и аппаратные решения при проектировании системы защиты информации с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах ИД-3ПК-6 - иметь навык: подготовки документов, определяющих правила и процедуры контроля обеспеченности уровня защищенности информации, содержащейся в информационной системе, осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации
ПК-7 Способен обосновывать необходимость защиты информации в автоматизированной системе	ИД-1ПК-7 знает: обоснование необходимости защиты информации в автоматизированной системе. ИД-2ПК-7 умеет определяет угрозы безопасности информации, обрабатываемой автоматизированной системой ИД-3ПК-7 владеет навыками: разработки архитектуры системы защиты информации автоматизированной системы.

г) Дополнительные профессиональные компетенции и индикаторы их достижения

Код и наименование дополнительной профессиональной	Код и наименование индикатора достижения дополнительной профессиональной компетенции
--	--

компетенции	
ДПК 1 – Способность решать личные задачи в процессе реализации индивидуальной образовательной траектории	ИД1ДПК-1 знать стратегии достижения личностных целей в процессе реализации индивидуальной образовательной траектории. ИД2ДПК-1 уметь оценивать свои потребности, возможности, способности, перспективы, интересы, усилия в решении личностных задач с целью формирования индивидуальной образовательной траектории. ИД3ДПК-1 владеть методами решения личностных задач в процессе реализации индивидуальной образовательной траектории
ДПК 2 – Способность к самостоятельной постановке целей к профессиональному саморазвитию в процессе реализации индивидуальной образовательной траектории	ИД1ДПК-2 знать свои потребности и мотивы в профессиональном саморазвитии. ИД2ДПК-2 уметь самостоятельно ставить перед собой личные цели в процессе получения новых знаний, планировать результат, понимать свой стиль обучения, свои сильные и слабые стороны, личные интересы в реализации индивидуальной траектории. ИД3ДПК-2 владеть: навыками постановки образовательной цели, самоанализа, самоконтроля, рефлексии, выбора пути (вариантов) реализации поставленной цели, решения личностных задач в процессе реализации индивидуальной образовательной траектории.
ДПК 3 – Способность к критическому анализу и оценке современных научных достижений, проектированию и осуществлению комплексных исследований на основе целостного системного научного мировоззрения	ИД1ДПК-3 знать современные научные достижения и методы научно-исследовательской деятельности. ИД2ДПК-3 уметь применять методы критического анализа и оценки современных научных достижений, проектирования и осуществления комплексных исследований на основе целостного системного научного мировоззрения. ИД3ДПК-3 владеть навыками сбора, обработки, анализа и систематизации данных по теме исследования; навыками выбора методов и средств решения задач исследования

2 Требования к выпускной квалификационной работе

2.1. Вид выпускной квалификационной работы

Выпускная квалификационная работа выполняется в форме бакалаврской работы. Выпускная квалификационная работа (ВКР) представляет собой самостоятельное законченное исследование, написанное лично выпускником под руководством научного руководителя, свидетельствующее об умении выпускника работать с литературой, обобщать и анализировать фактический материал, используя теоретические знания и практические навыки, полученные при освоении профессиональной образовательной программы.

2.2. Структура выпускной квалификационной работы и требования к ее содержанию

Пояснительная записка бакалаврской работы включает в себя: титульный лист;

бланк «задание»;
реферат;
нормативные ссылки;
перечень обозначений и сокращений;
содержание;
введение;
основную часть, как правило, состоящую из не менее, чем трех разделов;
заключение, включающее выводы и предложения (рекомендации) по внедрению и использованию результатов ВКР;
библиографический список;
приложения (при необходимости).

Титульный лист

Номер титульного листа включается в общую нумерацию страниц пояснительной записки, однако номер страницы на нем не проставляется.

Как правило, титульный лист оформляется в последнюю очередь, когда весь текст ВКР уже готов. К оформлению титульного листа необходимо подходить особенно тщательно и аккуратно. Титульный лист оформляется в соответствии с локальными нормативными актами университета и должен быть оформлен на компьютере.

Задание

Задание является документом, определяющим содержание работы обучающегося и ожидаемые результаты в ходе ее выполнения.

Задание оформляется на стандартном бланке, получаемом на выпускающей кафедре.

При составлении задания указывается следующая информация о работе:

тема работы. Формулировка темы должна быть лаконичной, точной и конкретной. Тема в бланке «задание», на титульном листе бакалаврской работы должна совпадать с утвержденной в приказе.

исходные данные, лежащие в основе работы. Исходными данными ВКР могут служить:

техническое задание работы;

предыдущие наработки, выполненные данным обучающимся или другими людьми (необходимо указать конкретно, например, «математическая модель», которая может служить исходным материалом для имитационного моделирования);

экспериментальные, статистические или экспертные данные;

литературные обзоры по теме, научно-техническая, производственная, нормативная документация, материалы сети Интернет.

последовательность выполнения работы в виде перечня решаемых в ходе работы задач. Задачи должны формулироваться четко, конкретно, с указанием используемых при их решении методов и инструментальных сред.

Текст задания подписывается научным руководителем и студентом, утверждается заведующим выпускающей кафедрой. Оформлением задания завершается первый, подготовительный этап работы.

Реферат

Текст реферата содержит краткие сведения о ВКР, помогающие понять смысл описываемой в дальнейшем работы.

Реферат оформляется в соответствии с локальными нормативными актами университета и включает в себя следующую информацию:

сведения об объеме ВКР, количестве иллюстраций, таблиц, приложений и использованных источников;

перечень ключевых слов или словосочетаний (от 5 до 15), в наибольшей мере характеризующих содержание пояснительной записки. Ключевые слова записываются в именительном падеже и оформляются прописными буквами в единую строку перечислением через запятую;

текст объемом не более 15 строк, отражающий суть объекта исследования или разработки, цель работы, использованные методы, полученные результаты, информацию о внедрении, область применения, предложения о дальнейшем развитии

объекта исследования или разработки.

Нормативные ссылки

Среди используемых в процессе работы литературных источников существует особый тип изданий – стандарты, регламентирующие различные аспекты проектирования объекта исследования и требования к разработке программно- аппаратного обеспечения.

В области информатики и вычислительной техники действуют серии стандартов, определяющих порядок проектирования автоматизированных (информационных) систем, создания программной продукции и документации, разработки элементов вычислительной техники, организации взаимодействия человека с машиной.

В зависимости от широты применения все стандарты можно условно разделить на четыре группы: международные (например, ИСО, МЭК), государственные – ГОСТ, отраслевые (корпоративные) и стандарты предприятия. Используемые в ходе работы и подготовки ВКР стандарты должны быть указаны в виде перечня нормативных ссылок.

Определения, обозначения и сокращения

Изложение сути работы должно быть построено логично и построено так, чтобы любой читатель, изучая текст ВКР, максимально точно и однозначно воспринимал все используемые в нем понятия. Используемая терминология должна быть общепринятой в рассматриваемой предметной области. Как правило, терминология регламентирована соответствующими ГОСТ, в которых для каждого термина приводится его точное определение, а также обозначение или сокращение. Помимо ГОСТ общепринятую терминологию каждой предметной области определяют различные словари, справочники и отраслевые нормативные документы.

Использование сокращений и условных обозначений значительно облегчает текст ВКР, делая его более компактным и удобочитаемым.

Помимо таких общеизвестных сокращений, как ИС, БД, АСУ, ЭВМ и других, разрешается вводить и собственные сокращения, отражающие наиболее часто повторяющиеся термины. Для их ввода требуется дать их расшифровку непосредственно при первом упоминании в тексте ВКР (например, «...особое место в области автоматизированных систем (АС) уделяется ...»).

Все малораспространенные сокращения, встречающиеся в тексте не менее двух раз, должны быть сведены в отдельный перечень сокращений. Здесь же размещаются и обозначения основных переменных, используемых в математических формулах и выражениях.

Содержание

В содержании должны быть перечислены все смысловые элементы ВКР: введение, заключение, структурные элементы основной части (разделы, подразделы, пункты), библиографический список и приложения.

Названия элементов содержания должны полностью совпадать с названиями, приведенными в тексте ВКР с использованием шрифта основного текста без курсивного и полужирного выделения.

Введение

Во введении необходимо дать оценку современного состояния решаемой задачи, привести исходные данные для ее разработки или исследования, обосновать их необходимость, а также показать ее актуальность, научную новизну или практическую значимость, связь приведенных исследований с другими, ранее проведенными, работами или опубликованными материалами.

Поскольку введение является полноценным элементом основной части работы, его объем должен быть не менее одной страницы.

Основная часть

Составляющими основной части ВКР, как правило, являются: теоретические основы изучаемой проблемы; современное состояние конкретной предметной области.

При работе над теоретической частью определяются объект и предмет ВКР, круг рассматриваемых проблем. Проводится обзор используемых источников,

обосновывается выбор применяемых методов, технологий и др. Работа выпускника над теоретической частью позволяет руководителю оценить следующие общие компетенции: понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес; осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития; самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации

В зависимости от специфики работы число разделов основной части, их конкретные названия могут меняться. В виде самостоятельных разделов могут быть приведены расчеты экономической эффективности и/или безопасности жизнедеятельности.

Заключение

Заключение завершает описание ВКР, обобщая полученные результаты и констатируя их соответствие поставленным в начале работы задачам. Заключение должно быть составлено таким образом, чтобы знакомство только с ним, без чтения текста всей остальной работы, давало полное представление о всех этапах выполненной работы и, главное, – о ее результатах.

Как правило, заключение начинается фразой: «При выполнении ВКР были выполнены следующие этапы:» и приводятся решенные задачи с особенностями их выполнения.

Затем следует перечислить наиболее значимые результаты работы. Некоторые из них сопроводить комментариями или выводами. В завершении должна быть дана оценка полноты решения поставленных в работе задач. Необходимо также оценить степень завершенности созданного информационного продукта. Здесь же следует дать рекомендации по конкретному использованию полученных результатов, указать стадию их внедрения (к ВКР может прилагаться акт о внедрении), а также дать рекомендации по дальнейшему развитию данного направления работ в рамках этого или других проектов.

Заключение должно быть лаконичным, четким, понятным и уместиться на одной странице.

Библиографический список

Библиографический список является важнейшим компонентом ВКР и предназначен для документального подтверждения интерпретируемого или цитируемого материала, а также для отражения эрудиции автора ВКР, степени его знакомства с актуальной литературой в рассматриваемой предметной области. Список должен содержать, как правило, перечень 25 – 30 литературных источников, материал которых был использован при создании ВКР. Особое внимание должно быть уделено изданиям последних лет. В них наиболее полно отражены современный подход к решению поставленной проблемы и практическое его применение, показаны новые и прогрессивные взгляды, которые следует использовать при изложении основных вопросов избранной темы.

Приложения

В приложения рекомендуется выносить вспомогательный материал, дополняющий текст ВКР, но не влияющий непосредственно на его восприятие и понимание. Приложения располагаются в конце ВКР в порядке появления соответствующих ссылок в тексте.

Каждое приложение должно иметь собственный заголовок (название), который отражает содержание этого приложения.

2.3 Примерная тематика и порядок утверждения тем выпускных квалификационных работ

1. Методы обнаружения вторжений и их применение в АС, обрабатывающих информацию конфиденциального характера.

2. Разработка практического руководства по обеспечению информационной безопасности на предприятии.

3. Исследование методов повышения стойкости стеганографических систем.

4. Анализ эффективности применения технических средств для оценки характеристик защищенности помещений.
5. Разработка методики выявления скрытых каналов передачи информации посредством побочных электромагнитных излучений.
6. Разработка требований для подготовки предприятия к лицензированию его длительности по технической защите конфиденциальной информации.
7. Разработка мер противодействия угрозам безопасности корпоративной информации со стороны сотрудников предприятия.
8. Разработка методики противодействия современным атакам на АС организации.
9. Разработка документации по использованию систем обнаружения вторжений в комплексных системах защиты информации.
10. Проектирование защищенной системы дистанционного обучения.
11. Проектирование и анализ распределенной системы видеонаблюдения на предприятии.
12. Анализ информационной безопасности в автоматизированных системах управления на предприятии.
13. Анализ возможностей использования средств защиты информации в соответствии с требованиями руководящих документов.
14. Разработка и внедрение методов управления риском утечки информации из корпоративной сети предприятия.
15. Подготовка и проведение аттестационных испытаний объекта информатизации по требованиям безопасности информации.
16. Аудит информационной безопасности предприятия на соответствие международным стандартам.
17. Разработка профиля защиты для Интернет-ресурса организации.
18. Разработка политики безопасности персональных данных при их обработке в базах данных организации.
19. Разработка политики управления инцидентами информационной безопасности на предприятии.

2.4 Учебно-методическое и информационное обеспечение

2.4.1 Рекомендуемая литература

1. Голиков, А. М. Основы информационной безопасности : учебное пособие / А. М. Голиков. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2007. — 288 с. — ISBN 978-5-868889-467-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/13957.html> (дата обращения: 22.03.2024). — Режим доступа: для авторизир. пользователей
2. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/544290> (дата обращения: 22.03.2024).
3. Кожуханов, Н. М. Правовые основы информационной безопасности : учебное пособие / Н. М. Кожуханов, Е. С. Недосекова. — Москва : Российская таможенная академия, 2013. — 88 с. — ISBN 978-5-9590-0725-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/69749.html> (дата обращения: 22.03.2024). — Режим доступа: для авторизир. пользователей
4. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2024. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/537000> (дата обращения: 22.03.2024).

5. Фомин, Д. В. Информационная безопасность [Электронный ресурс]: учеб.-метод. пособие / Д.В. Фомин; АмГУ, ФМИИ. – Благовещенск: Изд-во Амур. гос. ун-та, 2017. – 60 с. http://irbis.amursu.ru/DigitalLibrary/AmurSU_Edition/7371.pdf
6. Орлова, И. В. Информатика. Практические задания / И. В. Орлова. — 2-е изд., стер. — Санкт-Петербург : Лань, 2024. — 140 с. — ISBN 978-5-507-47294-9. — Текст : электронный // Лань : электронно- библиотечная система. — URL: <https://e.lanbook.com/book/358664> (дата обращения: 22.03.2024). — Режим доступа: для авториз. пользователей.
7. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/537247> (дата обращения: 22.03.2024).
8. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2024. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/543351> (дата обращения: 22.03.2024).
9. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2024. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/536225> (дата обращения: 22.03.2024).
10. Рассолов, И. М. Информационное право : учебник и практикум для вузов / И. М. Рассолов. — 7-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 427 с. — (Высшее образование). — ISBN 978-5-534-18043-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/535625> (дата обращения: 22.03.2024).
11. Кубанков, А. Н. Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект : учебное пособие / А. Н. Кубанков, Н. Н. Куняев ; под редакцией А. В. Морозов. — Москва : Всероссийский государственный университет юстиции (РПА Минюста России), 2014. — 78 с. — ISBN 978-5-89172-850-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/47262.html> (дата обращения: 22.03.2024). — Режим доступа: для авторизир. пользователей
12. Дождиков, В. Г. Краткий энциклопедический словарь по информационной безопасности / В. Г. Дождиков, М. И. Салтан. — Москва : Издательский дом ЭНЕРГИЯ, 2012. — 240 с. — ISBN 978-5-98908-050-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/121962.html> (дата обращения: 22.03.2024). — Режим доступа: для авторизир. пользователей
13. Спицын, В. Г. Информационная безопасность вычислительной техники : учебное пособие / В. Г. Спицын. — Томск : Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2011. — 148 с. — ISBN 978-5-4332-0020-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/13936.html> (дата обращения: 20.03.2024). — Режим доступа: для авторизир. пользователей
14. Криптография и безопасность цифровых систем : учебное пособие / В. Г. Грибунин, А. П. Мартынов, Д. Б. Николаев, В. Н. Фомченко ; под редакцией А. И. Астайкин. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2011. — 411 с. — ISBN 978-5-9515-0166-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/60851.html> (дата обращения: 20.03.2024). — Режим доступа: для авторизир. пользователей
15. Васин, Н. Н. Обеспечение безопасности сетей на маршрутизаторах и коммутаторах : методические указания по проведению лабораторных работ / Н. Н.

- Васин. — Самара : Поволжский государственный университет телекоммуникаций и информатики, 2014. — 24 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: [https:// www.iprbookshop.ru/71860.html](https://www.iprbookshop.ru/71860.html) (дата обращения: 20.03.2024). — Режим доступа: для авторизир. пользователей
16. Ложников, П. С. Средства безопасности операционной системы ROSA Linux : учебное пособие / П. С. Ложников, А. О. Провоторский. — Омск : Омский государственный технический университет, 2017. — 94 с. — ISBN 978-5-8149-2502-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: [https:// www.iprbookshop.ru/78474.html](https://www.iprbookshop.ru/78474.html) (дата обращения: 20.03.2024). — Режим доступа: для авторизир. пользователей
17. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2024. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: [https:// urait.ru/bcode/539995](https://urait.ru/bcode/539995) (дата обращения: 20.03.2024).
18. Гостев, И. М. Операционные системы : учебник и практикум для вузов / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2024. — 164 с. — (Высшее образование). — ISBN 978-5-534-04520-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/537133> (дата обращения: 20.03.2024).
19. Основы защиты информации от утечки по техническим каналам : учебно-методическое пособие / А. А. Евстифеев, В. И. Ерошев, А. П. Мартынов [и др.]. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2019. — 267 с. — ISBN 978-5-9515-0426-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: [https:// www.iprbookshop.ru/101929.html](https://www.iprbookshop.ru/101929.html) (дата обращения: 20.03.2024). — Режим доступа: для авторизир. пользователей
20. Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие / А. М. Голиков. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. — 256 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: [https:// www.iprbookshop.ru/72090.html](https://www.iprbookshop.ru/72090.html) (дата обращения: 20.03.2024). — Режим доступа: для авторизир. пользователей
21. Николаев, Д. Б. Технические средства и методы обеспечения безопасности информации : учебное пособие / Д. Б. Николаев, А. П. Мартынов, В. Н. Фомченко. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2015. — 394 с. — ISBN 978-5-9515-0277-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: [https:// www.iprbookshop.ru/89887.html](https://www.iprbookshop.ru/89887.html) (дата обращения: 20.03.2024). — Режим доступа: для авторизир. пользователей
22. Креопалов, В. В. Технические средства и методы защиты информации : учебное пособие / В. В. Креопалов. — Москва : Евразийский открытый институт, 2011. — 278 с. — ISBN 978-5-374-00507-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: [https:// www.iprbookshop.ru/10871.html](https://www.iprbookshop.ru/10871.html) (дата обращения: 20.03.2024). — Режим доступа: для авторизир. пользователей
23. Чуянов, А. Г. Обеспечение информационной безопасности в компьютерных системах : учебное пособие / А. Г. Чуянов, А. А. Симаков. — Омск : Омская академия МВД России, 2012. — 204 с. — ISBN 978-5-88651-535-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: [https:// www.iprbookshop.ru/36015.html](https://www.iprbookshop.ru/36015.html) (дата обращения: 21.03.2024). — Режим доступа: для авторизир. пользователей
24. Комплексное обеспечение информационной безопасности автоматизированных систем : лабораторный практикум / М. А. Лапина, Д. М. Марков, Т. А. Гиш [и др.]. — Ставрополь : Северо-Кавказский федеральный университет, 2016. — 242 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/62945.html> (дата обращения: 21.03.2024). — Режим доступа: для авторизир. пользователей

25. Криптография и безопасность цифровых систем : учебное пособие / В. Г. Грибунин, А. П. Мартынов, Д. Б. Николаев, В. Н. Фомченко ; под редакцией А. И. Астайкин. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2011. — 411 с. — ISBN 978-5-9515-0166-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: [https:// www.iprbookshop.ru/60851.html](https://www.iprbookshop.ru/60851.html) (дата обращения: 21.03.2024). — Режим доступа: для авторизир. пользователей
26. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2024. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/536902> (дата обращения: 21.03.2024).
27. Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2024. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: [https:// urait.ru/bcode/536453](https://urait.ru/bcode/536453) (дата обращения: 21.03.2024).
28. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2024. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/536132> (дата обращения: 21.03.2024).
29. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2024. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/536733> (дата обращения: 21.03.2024).

2.4.2 Программное обеспечение и Интернет-ресурсы

№	Наименование	Описание
1	Google Chrome	Бесплатное распространение по лицензии google chromium http:// code.google.com/ intl/ ru/ chromium/terms.html на условиях https:// www.google.com/ chrome/ browser/privacy/eula_text.html .
2	LibreOffice	Бесплатное распространение по лицензии GNU LGPL https://ru.libreoffice.org/about-us/license/
3	Secret Net 6	Сублицензионный договор №34/02/ ИБиИТ/697 от 09.08.2013.
4	Операционная система Linux	GNU-лицензия (GNU General Public License)
5	Программный комплекс «КонсультантПлюс»	Лицензия коммерческая по договору №21 от 29 января 2015 года.
6	Страж-НТ	Сублицензионный договор №34/02/ ИБиИТ/697 от 09.08.2013.
7	Система защиты информации от несанкционированного доступа Dallas Lock	Договор о сотрудничестве с образовательным учреждением 127-17-153/1.
8	Ревизор 1 XP	Сублицензионный договор №34/02/ ИБиИТ/697 от

		09.08.2013.
9	Ревизор 2 ХР	Сублицензионный договор №34/02/ ИБиИТ/697 от 09.08.2013.
10	https://urait.ru	Электронная библиотечная система «Юрайт». Фонд электронной библиотеки составляет более 4000 наименований и постоянно пополняется новинками, в большинстве своем это учебники и учебные пособия для всех уровней профессионального образования от ведущих научных школ с соблюдением требований новых ФГОСов.
11	http://www.iprbookshop.ru	Электронно- библиотечная система IPRbooks — научно- образовательный ресурс для решения задач обучения в России и за рубежом. ЭБС IPRbooks в полном объеме соответствует требованиям законодательства РФ в сфере образования
12	http://www.intuit.ru/	Интернет университет информационных технологи, содержит бесплатные учебные курсы, учебники и методические пособия по всем направлениям подготовки

2.4.3 Профессиональные базы данных и информационные справочные системы

№	Наименование	Описание
1	http://www.consultant.ru/	Компьютерная справочная правовая система «Консультант-Плюс».
2	http://www.elibrary.ru	Научная электронная библиотека elibrary.
3	http://www.amursu.ru	Электронная информационно- образовательная среда АмГУ
4	http://www.ict.edu.ru/about	Портал "Информационно- коммуникационные технологии в образовании" входит в систему федеральных образовательных порталов и нацелен на обеспечение комплексной информационной поддержки образования в области современных информационных и телекоммуникационных технологий, а также деятельности по применению ИКТ в сфере образования.
5	Google Scholar	Поисковая система по полным текстам научных публикаций всех форматов и дисциплин

2.5 Порядок выполнения и представления в ГЭК выпускной квалификационной работы

Выполнение ВКР разбивается на следующие этапы:

подготовительный этап, в ходе которого решаются формальные вопросы выполнения работы – назначение научного руководителя, определение и обоснование темы ВКР, оформление листа задания;

исполнительный этап – непосредственное выполнение работы в соответствии с заданием;

подготовка текста ВКР;

оформление и получение материалов и документов, необходимых для защиты ВКР – отзыва руководителя, акта о внедрении результатов исследования, иллюстративных материалов, мультимедиа презентации, текста доклада.

Подготовленная пояснительная записка ВКР проходит нормоконтроль на выпускающей кафедре за три недели до защиты. Успешное прохождения

нормоконтроля визируется на титульном листе. Затем работа переплетается (брошюруется) автором.

Полностью завершенная и переплетенная ВКР предоставляется на отзыв руководителю не позднее, чем за две недели до начала государственной итоговой аттестации.

В установленные сроки (обычно за 3 дня до защиты) выпускник предоставляет заведующему выпускающей кафедрой для рассмотрения и допуска к защите законченные материалы ВКР, которые включают:

переплетенную и подписанную выпускником и руководителем пояснительную записку; протокол проверки на плагиат, подписанный руководителем;

отзыв руководителя;

печатный вариант слайдов презентации;

электронный носитель с ВКР (компакт-диск или флэш-накопитель).

После ознакомления с материалами ВКР заведующий кафедрой принимает решение о допуске студента к защите.

На основании представления заведующего кафедрой на обучающихся, успешно завершивших полный курс обучения по направлению подготовки «Информационная безопасность» и представивших бакалаврскую работу с положительным отзывом руководителя в установленный срок, деканат факультета готовит приказ о допуске обучающихся к защите в ГЭК не позднее, чем за неделю до защиты.

2.6 Порядок защиты выпускной квалификационной работы

Завершающим этапом является защита ВКР, которая осуществляется на заседании государственной экзаменационной комиссии (далее – ГЭК). Для проведения государственной итоговой аттестации (далее – ГИА) и апелляций по результатам ГИА создаются ГЭК и апелляционные комиссии.

Комиссии действуют в течение календарного года. Заседания комиссий правомочны, если в них участвуют не менее двух третей от числа членов комиссий. Заседания комиссий проводятся председателями комиссий.

Решения комиссий принимаются простым большинством голосов членов комиссий, участвующих в заседании. При равном числе голосов председательствующий обладает правом решающего голоса. Решения, принятые комиссиями, оформляются протоколами.

Персональный состав комиссии утверждается приказом ректора.

Не позднее, чем за 30 календарных дней до дня защиты, распорядительным актом по университету утверждается расписание государственных аттестационных испытаний, в котором указываются даты, время и место проведения государственных аттестационных испытаний. Расписание доводится до сведения обучающегося, членов ГЭК и апелляционных комиссий, секретарей ГЭК, руководителей ВКР.

Обучающимся и лицам, привлекаемым к ГИА, во время ее проведения запрещается иметь при себе и использовать средства связи.

Защита бакалаврской работы проводится на открытом заседании ГЭК.

Процедура защиты имеет форму публичной научной дискуссии, в которой могут принять участие не только официально назначенные выступающие, но и все члены комиссии и любой присутствующий. До начала защиты обучающийся предоставляет секретарю ГЭК необходимые сведения.

Процедура защиты ВКР обычно проходит по следующему сценарию.

1. Секретарь ГЭК приглашает к защите выпускника, зачитывая его фамилию, имя, отчество и тему ВКР.

2. Председатель предоставляет студенту слово для доклада.

3. Студент излагает доклад, в котором освещается постановка задачи, существо работы и полученные результаты. Длительность доклада не должна превышать 7 минут для ВКР.

4. После окончания доклада председатель предлагает членам комиссии задать вопросы по представленной работе.

5. После окончания ответов на вопросы, зачитывается отзыв руководителя, а также прочие документы, представленные в ГЭК (например, акты о внедрении).

6. Затем студенту предоставляется слово для ответов на замечания руководителя.

7. После ответов на замечания защита объявляется законченной.

На защите бакалаврских работ обучающиеся должны пользоваться иллюстративным материалом, оформленным в виде слайдов презентации, служащими для наглядности представления работы в процессе доклада.

Оценка бакалаврских работ производится на закрытом заседании ГЭК, после защиты всех работ, назначенных на данный день. Сообщение об оценке бакалаврской работы и присвоение соответствующей квалификации делается председателем ГЭК при завершении заседания.

Результаты защиты объявляются обучающимся в тот же день после оформления в установленном порядке протоколов заседания ГЭК.

В протоколе заседания ГЭК по защите ВКР фиксируется перечень заданных обучающемуся вопросов и характеристика ответов на них, мнения членов ГЭК о выявленном в ходе защиты уровне подготовленности обучающегося к решению профессиональных задач, а также о выявленных недостатках в теоретической и практической подготовке обучающегося.

2.7 Критерии выставления оценок (соответствия уровня подготовки выпускника требованиям ФГОС ВО) на основе выполнения и защиты им квалификационной работы

Оценка ВКР и решение о присвоении выпускнику соответствующей квалификации принимаются коллегиально на закрытом заседании ГЭК открытым голосованием.

Результаты защиты ВКР определяются оценками «отлично», «хорошо», «удовлетворительно», или устанавливается факт отрицательного результата защиты.

При выставлении оценки по защите ВКР ГЭК учитывает:

качество выполнения ВКР и самостоятельность выпускника;

обоснованность принятых решений;

актуальность решаемых задач;

оригинальность принятых решений;

качество оформления и грамотность изложения материалов ВКР;

умение логично, четко, грамотно, выразительно представлять доклад;

убедительность ответов на вопросы и умение защищать выдвинутые в ВКР научно-технические и практические предложения.

Кроме того, при выставлении окончательной оценки по защите ВКР ГЭК может учитывать:

мнение руководителя;

средний балл за весь период обучения,

внедрение результатов ВКР,

наличие публикаций по теме исследования и др.

В спорных случаях решение принимается большинством голосов, присутствующих членов ГЭК, при равном числе голосов голос председателя является решающим.

Критерии оценки ВКР представлены в фонде оценочных средств ГИА по направлениям подготовки 10.03.01 – Информационная безопасность.

При положительном результате ГЭК принимает решение о присвоении выпускнику квалификации «бакалавр» по соответствующему направлению подготовки и выдаче диплома о высшем образовании установленного образца.