

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Комсомольский-на-Амуре государственный университет»

УТВЕРЖДАЮ

Декан факультета Компьютерных технологий

(наименование факультета)

И.А. Трещёв

(подпись, ФИО)

« _____ » _____ 20__ г.

ПРОГРАММА

государственной итоговой аттестации (ГИА)

Специальность	<i>10.05.03 «Информационная безопасность автоматизированных систем»</i>
Специализация	<i>Анализ безопасности информационных систем</i>
Квалификация выпускника	<i>Специалист по защите информации</i>
Год начала подготовки (по учебному плану)	<i>2023</i>
Форма обучения	<i>очная</i>
Технология обучения	<i>традиционная</i>

Трудоемкость, з.е.	Выпускающая кафедра
<i>9</i>	<i>Информационная безопасность автоматизированных систем</i>

Комсомольск-на-Амуре 2022

Образовательная программа рассмотрена и одобрена на заседании кафедры
«Информационная безопасность автоматизированных систем» Протокол №
6 от «11» апреля 2022 г.

Заведующий кафедрой ИБАС В.А.Челухин

СОГЛАСОВАНО

Начальник УМУ Поздеева Е.Е.

1 Общие положения

1.1 Цель государственной итоговой аттестации

Государственная итоговая аттестация проводится государственной экзаменационной комиссией в целях определения соответствия результатов освоения обучающимися основной образовательной программы «Анализ безопасности информационных систем» по специальности 10.05.03 «Информационная безопасность автоматизированных систем», разработанной в Комсомольском-на-Амуре государственном университете, требованиям федерального государственного образовательного стандарта высшего образования (ФГОС ВО), утвержденного приказом Минобрнауки России № 1457 от 26 ноября 2020 года.

1.2 Формы государственной итоговой аттестации

Государственная итоговая аттестации по специальности

10.05.03 «Информационная безопасность автоматизированных систем»

включает:

- а) подготовку к сдаче и сдачу государственного экзамена;
- б) подготовку к процедуре защиты и защиту выпускной квалификационной работы (ВКР).

1.3 Нормативная база итоговой аттестации

1.3.1 Итоговая аттестация осуществляется в соответствии с нормативным документом университета **СТО У.016-2018 Итоговая аттестация студентов. Положение**. В указанном документе определены и регламентированы:

- общие положения по итоговой аттестации;
- правила и порядок организации и процедура проведения итоговой аттестации; - обязанности и ответственность руководителя выпускной квалификационной работы;
- результаты государственной итоговой аттестации;
- порядок апелляции государственной итоговой аттестации; - документация по государственной итоговой аттестации.

1.3.2 Оформление выпускной квалификационной работы осуществляется в соответствии с требованиями **РД 013-2016 Текстовые студенческие работы. Правила оформления**.

2 Общее описание профессиональной деятельности выпускников

Области профессиональной деятельности и сферы профессиональной деятельности, в которых выпускники, освоившие программу специалитета (далее - выпускники), могут осуществлять профессиональную деятельность:

- обеспечение безопасности (в сфере обеспечения безопасности информации в автоматизированных системах, обладающих информационно-технологическими ресурсами, подлежащими защите).

Выпускники могут осуществлять профессиональную деятельность в других областях профессиональной деятельности и (или) сферах профессиональной деятельности при условии соответствия уровня их образования и полученных компетенций требованиям к квалификации работника.

Типы задач профессиональной деятельности выпускников

- проектная;
- контрольно-аналитическая.

Перечень основных объектов профессиональной деятельности выпускников:

- автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите

- информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите

систем

- технологии обеспечения информационной безопасности автоматизированных

систем

- системы управления информационной безопасностью автоматизированных

3 Требования к результатам освоения образовательной программы

В результате освоения образовательной программы у выпускника должны быть сформированы универсальные (таблица 1) и общепрофессиональные компетенции (таблица 2), установленные ФГОС ВО, а также профессиональные компетенции (таблица 3), установленные образовательной программой специалитета, сформированные на основе профессиональных стандартов, соответствующих профессиональной деятельности выпускников, а также на основе анализа требований к профессиональным компетенциям, предъявляемых к выпускникам на рынке труда, обобщения отечественного и зарубежного опыта, проведения консультаций с ведущими работодателями, объединениями работодателей отрасли.

Таблица 1 – Универсальные компетенции выпускника

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции выпускника
Системное и критическое мышление	УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, выработать стратегию действий

Разработка и реализация проектов	УК-2. Способен управлять проектом на всех этапах его жизненного цикла
Командная работа и лидерство	УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
Коммуникация	УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия
Межкультурное взаимодействие	УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности
Безопасность жизнедеятельности	УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов
Экономическая культура, в том числе финансовая грамотность	УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности
Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции выпускника
Гражданская позиция	УК-10. Способен формировать нетерпимое отношение к коррупционному поведению

Таблица 2 – Общепрофессиональные компетенции выпускника

Код и наименование общепрофессиональной компетенции выпускника
--

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 программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности

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

ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные 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

ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах 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 создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ

ОПК-8. Способен применять методы научных исследований при проведении разработок в области защиты информации и автоматизированных системах

ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности

ОПК-11. Способен разрабатывать компоненты систем защиты информации автоматизированных систем

ОПК-12. Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем

ОПК-13. Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем
ОПК-14. Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений
Код и наименование общепрофессиональной компетенции выпускника
ОПК-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем
ОПК-16. Способен анализировать основные этапы и закономерности исторического развития России, её место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма
ОПК-7.1. Способен использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем
ОПК-7.2. Способен разрабатывать методики и тесты для анализа степени защищенности информационной системы и её соответствия нормативным требованиям по защите информации
ОПК-7.3. Способен проводить анализ защищенности и верификацию программного обеспечения информационных систем

Таблица 3 – Профессиональные компетенции выпускника

Основание (профессиональный стандарт)	Код и наименование профессиональной компетенции
Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 года № 522н (зарегистрировано в	ПК-1: Способен проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем
	ПК-2: Способен проводить анализ защищенности информационной инфраструктуры автоматизированной системы
	ПК-3: Способен проводить анализ технической документации информационной инфраструктуры автоматизированной системы

Минюсте России 28.09.2016 № 43857)	ПК-4: Способен анализировать программные, архитектурнотехнические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах
	ПК-5: Способен контролировать безотказное функционирование технических средств защиты информации
	ПК-6: Способен проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов

4 Объем, структура и содержание государственной итоговой аттестации

Общая трудоемкость государственной итоговой аттестации составляет 9 зачетных единиц, 324 академических часа. Распределение объема государственной итоговой аттестации представлено в таблице 4.

Таблица 4 – Объем государственной итоговой аттестации по составу

Элемент ГИА	Контролируемые результаты освоения образовательной программы	Форма проведения	Трудоемкость (в часах)
Подготовка к сдаче и сдача государственного экзамена			
Вопросы и практические задания государственного экзамена	УК1, УК2, УК3, УК4, УК5, УК6, УК8, УК9, УК-10, ОПК-3, ОПК-16,	Опосредованно*	108
	ОПК-1, ОПК-4, ОПК-7, ОПК-8, ОПК-10, ОПК-11, ОПК-13, ОПК-7.1, ОПК-7.2, ПК-3, ПК-4	Подготовка ответа на теоретические вопросы, выполнение практического задания	
Подготовка к процедуре защиты и защита выпускной квалификационной работы			

Выпускная квалификационная работа	ОПК-2, ОПК-3, ОПК-5, ОПК-6, ОПК-7, ОПК-8, ОПК-9, ОПК-10, ОПК-11, ОПК-12, ОПК-13, ОПК-14, ОПК-15, ОПК-7.1, ОПК-7.2, ОПК-7.3, ПК-1, ПК-2, ПК3, ПК-4, ПК5, ПК-6	Защита выпускной квалификационной работы	216
Итого	–	–	324

* На основании результатов промежуточной аттестации по дисциплинам / практикам учебного плана

5 Программа государственного экзамена и рекомендации обучающимся по подготовке к нему

5.1 Виды проведения государственного экзамена Устный

экзамен.

5.2 Оценочные материалы для проведения ГЭ

Билет по проверке общепрофессиональных и профессиональных компетенций состоит из 3 теоретических вопросов по разным дисциплинам и 2 практических заданий / задач

В структуру государственного экзамена входят вопросы по учебным дисциплинам (модулям), результаты освоения которых имеют определяющее значение для профессиональной деятельности выпускников:

- Программно-аппаратные средства обеспечения информационной безопасности
- Системы интеллектуальной защиты информации
- Техника и технология атак злоумышленников в распределённых информационных системах
- Аппараты и средства перехвата информации,
- Анализ защищённости распределённых информационных систем
- Тестирование на проникновение и анализ безопасности, анализ и защита вебприложений
- Разработка и эксплуатация автоматизированных систем в защищённом исполнении

Перечень вопросов и типовых практических заданий (задач), критерии и показатели оценивания представлены в разделе 7.

5.3 График подготовки, организации и проведения ГЭ

Таблица 5 – График подготовки, организации и проведения ГЭ

Виды работ	Сроки	Ответственный исполнитель
Формирование программы государственного экзамена по специальности	За 7 мес. до ГЭ по КУГ	Зав. кафедрой, Ведущие преподаватели
Подготовка вопросов к государственному экзамену	За 6 мес. до ГЭ по КУГ	Зав. кафедрой, Преподаватели кафедры
Выдача вопросов государственного экзамену выпускникам	За 6 мес. до ГЭ по КУГ	Зав. кафедрой
Организация обзорных лекций и консультаций по специальности	За 3 мес. до ГЭ по КУГ	Преподаватели кафедры
Подготовка и утверждение комплектов билетов	За 3 мес. до ГЭ по КУГ	Председатель ГЭК, Зав. кафедрой
Утверждение расписания государственного экзамена и информирование обучающихся	За 1 мес. до ГЭ по КУГ	Ведущий специалист УМУ, зав. кафедрой
Приказ о допуске обучающихся к государственному экзамену	Не позднее 3 дней до ГЭ	Декан факультета
Проведение государственного экзамена	По приказу	ГЭК

5.4 Рекомендации обучающимся по подготовке к ГЭ Государственный экзамен - это завершающий этап подготовки специалиста, механизм выявления и оценки результатов обучения и установления соответствия уровня профессиональной подготовки выпускников требованиям ФГОС ВО по специальности.

Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к государственному экзамену, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На государственном экзамене обучающийся демонстрирует то, что он приобрел в процессе обучения.

В период подготовки к государственному экзамену студенты вновь обращаются к учебнометодическому материалу и закрепляют знания. Подготовка к государственному экзамену включает в себя два этапа: самостоятельная работа в течение всего периода обучения; непосредственная подготовка в дни, предшествующие государственному экзамену по темам учебных дисциплин, выносимым на государственную аттестацию.

При подготовке к государственному экзамену студентам целесообразно использовать материалы лекций, учебно-методические комплексы, основную и дополнительную литературу.

Особо следует обратить внимание на умение использовать программу государственной итоговой аттестации в части ГЭ, раздел 7. Она включает в себя вопросы для государственного экзамена. Поэтому студент, заранее изучив содержание государственного экзамена, сможет лучше сориентироваться в вопросах, стоящих в его билете.

Формулировка вопросов экзаменационного билета совпадает с формулировкой перечня рекомендованных для подготовки вопросов государственного экзамена.

Как соотносить конспект лекций и учебники при подготовке к экзамену? Было бы ошибкой главный упор делать на конспект лекций, не обращаясь к учебникам и, наоборот недооценивать записи лекций. Рекомендации здесь таковы. При проработке той или иной темы курса сначала следует уделить внимание конспектам лекций, а затем учебникам или интернетисточникам. Дело в том, что "живые" лекции обладают рядом преимуществ: они более оперативно иллюстрируют состояние научной проработки того или иного теоретического вопроса, дают ответ с учетом новых теоретических разработок, т.е. отражают самую "свежую" информацию. Для написания же и опубликования печатной продукции нужно время. Отсюда изложение некоторого учебного материала быстро устаревает.

Традиционно студенты задают вопрос, каким пользоваться учебником при подготовке к экзамену? Однозначно ответить на данный вопрос нельзя. Не бывает идеальных учебников, они пишутся представителями различных школ, научных направлений, и поэтому в каждом из них есть свои достоинства и недостатки, чему-то отдается предпочтение, что-то недооценивается либо вообще не раскрывается. Отсюда, для сравнения учебной информации и полноты картины необходим конспект лекций, а также в обязательном порядке использовать как минимум два учебных источника.

Надо ли делать письменные пометки, прорабатывая тот или иной вопрос? Однозначного ответа нет. Однако, для того, чтобы быть уверенным на экзамене, необходимо при подготовке тезисно записать ответы на наиболее трудные, с точки зрения студента, вопросы. Запись включает дополнительные (моторные) ресурсы памяти.

Представляется крайне важным посещение студентами проводимой перед государственным экзаменом консультации. Здесь есть возможность задать вопросы преподавателю по тем разделам и темам, которые недостаточно или противоречиво освещены в учебной, научной литературе или вызывают затруднение в восприятии.

Важно, чтобы студент грамотно распределил время, отведенное для подготовки к государственному экзамену. В этой связи целесообразно составить календарный план подготовки к экзамену, в котором в определенной последовательности отражается изучение или повторение всех экзаменационных вопросов. Подготовку к экзамену студент должен вести ритмично и систематично.

Зачастую студенты выбирают "штурмовой метод", когда подготовка ведется хаотично, материал прорабатывается бессистемно. Такая подготовка не может выработать прочную систему знаний. Поэтому знания, приобретенные с помощью подобного метода, в лучшем случае закрепляются на уровне представления.

Во время экзамена за отведенное для подготовки время студент должен сформулировать четкий ответ по каждому вопросу билета. Во время подготовки рекомендуется не записывать на лист ответа все содержание ответа, а составить развернутый план, которому необходимо следовать во время сдачи экзамена.

Отвечая на экзаменационные вопросы, необходимо придерживаться определенного плана ответа, который не позволит студенту уйти в сторону от содержания поставленных вопросов. При

ответе на экзамене допускается многообразие мнений. Приветствуется, если студент не читает с листа, а свободно излагает материал, ориентируясь на заранее составленный план.

К выступлению выпускника на государственном экзамене предъявляются следующие требования:

- ответ должен строго соответствовать объему вопросов билета;
- ответ должен полностью исчерпывать содержание вопросов билета;
- ответ должен соответствовать определенному плану, который рекомендуется огласить в начале выступления;
- выступление на государственном экзамене должно соответствовать нормам и правилам публичной речи, быть четким, обоснованным, логичным.

Во время ответа на поставленные вопросы надо быть готовым к дополнительным или уточняющим вопросам. Дополнительные вопросы задаются членами государственной комиссии в рамках билета и связаны, как правило, с неполным ответом. Уточняющие вопросы задаются, чтобы конкретизировать мысли студента. Полный ответ на уточняющие вопросы лишь усиливает эффект общего ответа студента.

Итоговая оценка знаний предполагает дифференцированный подход к студенту, учет его индивидуальных способностей, степень усвоения и систематизации основных теоретических положений, понятий и категорий. Оценивается так же культура речи, грамотное комментирование, приведение примеров, умение связывать теорию с практикой, творчески применять знания к неординарным ситуациям, излагать материал доказательно, полемизировать там, где это необходимо.

6 Выпускная квалификационная работа и рекомендации обучающимся по подготовке к защите и защите ВКР

Выпускная квалификационная работа специалиста по направлению подготовки 10.05.03 «Информационная безопасность автоматизированных систем» представляет собой законченную разработку, в которой должны быть изложены вопросы информационной безопасности автоматизированных систем.

6.1 Вид выпускной квалификационной работы

ВКР выполняется в виде дипломного проекта.

Тематика ВКР, критерии и показатели оценивания приведены в разделе 7. **6.2**

Цель выполнения выпускной квалификационной работы Выполнение

ВКР имеет своей целью:

- систематизацию, закрепление и углубление полученных теоретических и практических знаний по специальности 10.05.03 «Информационная безопасность автоматизированных систем»;

- развитие навыков обобщения практических материалов, критической оценки теоретических положений и выработки своей точки зрения по рассматриваемой проблеме;
- развитие умения аргументировано излагать свои мысли и формулировать предложения;
- выявление у обучающихся творческих возможностей и готовности к практической деятельности в условиях современной экономики.

6.3 Перечень рекомендуемой литературы для выполнения ВКР Список

основной литературы

1. Технические средства и методы защиты информации: Учебник для вузов [Электронный ресурс]/ А.П. Зайцев, А.А. Шелупанов, Р.В.Мещеряков; Под ред. А.П.Зайцева - 7 изд., исправ. - М.: Гор. линия-Телеком, 2019. - 442с.//ZNANIUM.COM : электронная библиотечная система- Режим доступа: <http://znanium.com/catalog/product/390284>, ограниченный. – Загл. с экрана

2. Технические средства и методы защиты информации [Электронный ресурс]/ Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. - М.:Гор. линия-Телеком, 2018. - 616 с.:

://ZNANIUM.COM : электронная библиотечная система- Режим доступа: <http://znanium.com/catalog/product/560580>, ограниченный. – Загл. с экрана

3. Методы и средства обеспечения программно-аппаратной защиты информации:

Научно-техническое издание [Электронный ресурс]/ Астайкин А.И., Мартынов А.П., Николаев Д.Б. - Саров:ФГУП"РФЯЦ-ВНИИЭФ", 2017. - 214 с.//ZNANIUM.COM : электронная библиотечная система- Режим доступа: <http://znanium.com/catalog/product/950073>, ограниченный.

–
Загл. с экрана

4. Челухин, В.А. Комплексное обеспечение информационной безопасности автоматизированных систем: Учебное пособие для вузов / В. А. Челухин. - Комсомольск-наАмуре: Изд-во Комсомольского-на-Амуре гос.техн.ун-та, 2021. - 207с. - Библиогр.: с.201-207. - 273-00. 5. Программно-аппаратная защита информации: Учебное пособие / Хорев П.Б., - М.:Форум, НИЦ ИНФРА-М, 2019. - 352 с.: 60x90 1/16. - (Высшее образование) ISBN 978-5-00091-004-7 - Режим доступа: <http://znanium.com/catalog/product/489084>

6. Аппаратные и программные средства защиты информации: Учебное пособие /

Душкин А.В., Кольцов А., Кравченко А. - Воронеж: Научная книга, 2018. - 232 с. ISBN 978-54446-0746-6 - Режим доступа: <http://znanium.com/catalog/product/923168>

7. Кузин, А.В. Компьютерные сети: Учебное пособие / А.В. Кузин. - 3-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2018. - 192 с.: ил.; Режим доступа: <http://znanium.com/catalog/product/450375>

8. Исаченко, О.В. Программное обеспечение компьютерных сетей: Учебное пособие /

О.В. Исаченко. - М.: ИНФРА-М, 2018. - 117 с.: Режим до-ступа:

<http://znanium.com/catalog/product/232661> 9. Могильников, Е. В. Вычислительные машины, системы и сети телекоммуникаций: учеб. пособие / Е.В. Могильников — Комсомольск-на-Амуре.: ГОУ ВПО Комсомольский-на-Амуре гос.техн.ун-т, 2019. – 155 с. // Виртуальная библиотека ИНИТ. – Режим доступа: <http://www.initkms.ru/library/readbook/1101388/1>, свободный. – загл.с экрана

Список дополнительной литературы

10. Козунова, С.С. Система управления информационной безопасностью предприятия [Электронный ресурс] / С.С.Козунова // Евразийский союз ученых. - 2016. - № 28-2. - С. 22-23.- Режим доступа : http://elibrary.ru/query_results.asp?pagenum=3.

11. Шашло, Н.В. Комплексный подход к обеспечению экономической безопасности предприятий [Электронный ресурс] / Н.В.Шашло // Фундаментальные исследования. - 2016.- № 11-3.- С. 668-672. – Режим доступа : http://elibrary.ru/query_results.asp?pagenum=3.

12. Мэйволд Э. Безопасность сетей [Электронный ресурс]/ Мэйволд Э., 2015.— 571 с.
//

IPRbooks: электронно-библиотечная система. – Режим доступа: <http://www.iprbookshop.ru/73727.html>, ограниченный. – Загл. с экрана.

13. Зиангирова Л.Ф. Вычислительные системы, сети и телекоммуникации

[Электронный ресурс] / Зиангирова Л.Ф. — 2015.— 150 с. // IPRbooks: электронно-библиотечная система. – Режим доступа: <http://www.iprbookshop.ru/67231.html>, ограниченный. – Загл. с экрана.

14. Т.И. Немцова Программирование на языке высокого уровня. Программирование на языке Object Pascal: Учеб. пос. [Электронный ресурс] / Т.И. Немцова и др.; Под ред. Л.Г. Гагариной - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014 - 496с.: ил. // ZNANIUM.COM : электроннобиблиотечная система.- Режим доступа: <http://znanium.com/catalog/product/472870>, ограниченный. – Загл. с экрана

15.Защита информации: Учебное пособие [Электронный ресурс]/ А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.//ZNANIUM.COM : электронная библиотечная система- Режим доступа: <http://znanium.com/catalog/product/474838>, ограниченный. – Загл. с экрана

16.Защита информации ограниченного доступа от утечки по техническим каналам: Справочное пособие [Электронный ресурс]/ Бузов Г.А. - М.:Гор. линия-Телеком, 2015. - 586 с.//ZNANIUM.COM : электронная библиотечная система- Режим доступа: <http://znanium.com/catalog/product/895240>, ограниченный. – Загл. с экрана

17.Новиков С.Н. Методы защиты информации [Электронный ресурс] : учебное пособие / С.Н. Новиков, О.И. Солонская. — Электрон. текстовые данные. — Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2009. — 121 с. — 22278397. — Режим доступа: <http://www.iprbookshop.ru/54767.html> 18. Информационная безопасность и защита информации [Электронный ресурс] : учебно-методический комплекс / . — Электрон.

текстовые данные. — Алматы: Нур-Принт, 2012. — 98 с. — 9965-756-05-8. — Режим доступа: <http://www.iprbookshop.ru/67055.html> 19.

Система защиты информации от несанкционированного доступа «СТРАЖ NT». Версия 2.0. Описание применения. – 53 с. (прилагается на компакт диске с программным обеспечением, хранится на факультете компьютерных технологий)

20. Система защиты информации от несанкционированного доступа «Dallas Lock 8.0». Руководство по эксплуатации. – 88 с. (прилагается на компакт диске с программным обеспечением, хранится на факультете компьютерных технологий)

21. Система защиты информации «Secret Net 7». Автономный вариант для Windows 2000. Руководство по администрированию. – 142 с. (прилагается на компакт диске с программным обеспечением, хранится на факультете компьютерных технологий)

22. Мельников В. П. Защита информации: учебник для вузов / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе; Под ред. В. П. Мельникова. – М.: Академия, 2014. – 296 с.

6.4 График подготовки, организации и проведения защиты ВКР Таблица

6 – График подготовки, организации и проведения защиты ВКР

Виды работ	Сроки	Ответственный исполнитель
Представление тем ВКР, выбор темы и руководителя ВКР	за 7 мес. до защиты ВКР по КУГ	Преподаватели кафедры, Обучающиеся
Подача заявления о закреплении темы и руководителя ВКР	за 6 мес. до защиты ВКР по КУГ	Обучающийся
Подготовка приказа по утверждению тем и руководителей ВКР	за 6 мес. до защиты ВКР по КУГ	Зав. кафедрой Руководители ВКР
Составление и утверждение заданий на ВКР и календарного графика на ВКР	за 6 мес. до защиты ВКР по КУГ	Руководители ВКР, Зав. кафедрой
Организация консультаций и нормоконтроль	В течение преддипломной практики и выполнения ВКР по КУГ	Зав. кафедрой

Контроль за ходом выполнения ВКР I этап (30%) II этап (80%) III этап (100%)	I этап (30%) - начало преддипломной практики по КУГ II этап (80%) - окончание преддипломной практики по КУГ III этап (100%) за неделю до защиты ВКР по приказу	Руководители ВКР, Зав. кафедрой
Утверждение и предоставление дат защиты ВКР	за 1 мес. до защиты ВКР по КУГ	Зав. кафедрой, Секретарь ГЭК
Назначение рецензентов	за 1 месяц до защиты ВКР	Руководители ВКР, Зав. кафедрой
Представление на кафедру письменного отзыва о работе обучающегося в период подготовки ВКР (далее - отзыв).	после завершения подготовки обучающимся ВКР за 7 дней до защиты ВКР	Руководители ВКР,
Получение отзыва руководителя, рецензии	за 5 календарных дней до защиты ВКР	Обучающийся
Подготовка проекта приказа о допуске к защите ВКР	не позднее 3 дней до защиты ВКР	Зав. кафедрой Секретарь ГЭК
Передача в ГЭК ВКР, отзыва и рецензии	не позднее 2 дней до защиты ВКР	Обучающийся, руководитель ВКР
Защита ВКР в ГЭК	По приказу	Зав. кафедрой Секретарь ГЭК

6.5 Рекомендации обучающимся по подготовке к защите ВКР

6.5.1 Планирование самостоятельной работы выпускников

Таблица 7 – График организации самостоятельной работы выпускников по подготовке к защите ВКР

Этапы работ	Срок
1. Сбор, изучение и систематизация учебной, научно-технической литературы, учебно-методической документации и патентной информации.	По согласованию с руководителем ВКР
2. Разработка общей части (введения, теоретической главы) работы.	

3. Технологические разработки. Этапы решения поставленной задачи. Подготовка аналитической и практической глав.
4. Написание заключения и аннотации.
5. Окончательное оформление расчетно-пояснительной записки и графических материалов.
6. Подготовка на проверку и подпись ВКР руководителю.
7. Подготовка на проверку и подпись ВКР заведующему кафедрой. Получение допуска к защите.

6.5.2 Структура ВКР. Требования к ее содержанию

Структура выпускной работы включает: введение, три главы, с разбивкой на параграфы, заключение, а также список использованной литературы и приложения. Объем работы – в пределах 70-80 печатных страниц.

Во введении обосновывается выбор темы, ее актуальность, формулируются цель и задачи исследования. Здесь отражается степень изученности рассматриваемых вопросов в научной и практической литературе, оговаривается предмет и объект исследования, конкретизируется круг вопросов, подлежащих исследованию. По объему введение не превышает 3 страниц.

Первая глава имеет теоретический характер. В ней на основе изучения литературы, дискуссионных вопросов, систематизации современных исследований рассматриваются возникновение, этапы исследования проблем, систематизируются позиции российских и зарубежных ученых и обязательно аргументируется собственная точка зрения обучающегося относительно понятий, проблем, определений, выводов.

Вторая и последующие главы носят аналитический и прикладной характер, раскрывающий содержание проблемы. В них на конкретном практическом материале освещается фактическое состояние проблемы на примере конкретного объекта. Достаточно глубоко и целенаправленно анализируется и оценивается действующая практика, выявляются закономерности и тенденции развития на основе использования собранных первичных документов, статистической и прочей информации за предоставленный для данного исследования период (как правило, не менее трех лет).

Содержание этих глав является логическим продолжением первой теоретической главы и отражает взаимосвязь теории и практики, обеспечивает разработку вопросов плана работы и выдвижение конкретных предложений по исследуемой проблеме.

Заключение содержит выводы по теме ВКР и конкретные предложения по исследуемым вопросам. Они должны непосредственно вытекать из содержания выпускной работы и излагаться лаконично и четко. По объему заключение не превышает 3-4 страниц.

7 Фонд оценочных средств для проведения ГИА

7.1 Паспорт фонда оценочных средств

Таблица 8 – Паспорт фонда оценочных средств

Код контролируемой компетенции	Индикаторы достижения компетенции	Наименование оценочного средства	Показатели оценки
<p>УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий</p>	<p>УК-1.1 Знает метод системного анализа, способы обоснования решения (индукция, дедукция, по аналогии) проблемной ситуации</p> <p>УК-1.2 Умеет применять методики поиска, сбора и обработки информации; осуществляет оценку адекватности информации о проблемной ситуации путём выявления диалектических и формальнологических противоречий в анализируемой информации</p> <p>УК-1.3 Владеет методами поиска, сбора и обработки, критического анализа и синтеза информации; навыком выбора методов критического анализа, адекватных проблемной ситуации; навыками разработки и обоснования плана действий по решению проблемной ситуации</p>	<p>Опосредованно, на основании результатов промежуточной аттестации по дисциплинам / практикам учебного плана</p>	<p>см. п. 7.2</p>
<p>УК-2. Способен управлять проектом на всех этапах его жизненного цикла</p>	<p>УК-2.1 Знает виды ресурсов и ограничений для реализации проекта; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность.</p> <p>УК-2.2 Формулирует цели, задачи, ожидаемые результаты проекта; разрабатывает план реализации проекта; использует нормативноправовую документацию в сфере профессиональной деятельности.</p> <p>УК-2.3 Владеет методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативноправовой документацией; навыками контроля и оценки эффективности реализации</p>	<p>Опосредованно, на основании результатов промежуточной аттестации по дисциплинам / практикам учебного плана</p>	<p>см. п. 7.2</p>

<p>УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели</p>	<p>УК-3.1 Знает основные приемы и нормы социального взаимодействия; основные понятия и методы конфликтологии, технологии межличностной и деловой коммуникации, принципы командной работы как основы организации и руководства работой команды, способы мотивации членов команды с учетом организационных возможно-</p>	<p>Опосредованно, на основании результатов промежуточной аттестации по дисциплинам / практикам учебного плана</p>	<p>см. п. 7.2</p>
---	--	---	-------------------

<p>Код контролируемой компетенции</p>	<p>Индикаторы достижения компетенции</p>	<p>Наименование оценочного средства</p>	<p>Показатели оценки</p>
--	---	--	---------------------------------

	<p>стей и личностных особенностей членов команды</p> <p>УК-3.2 Умеет устанавливать и поддерживать контакты, обеспечивающие успешную работу в команде; разрабатывать цели команды в соответствии с целями проекта; выбирать стратегию формирования команды и определять функциональные и ролевые критерии отбора участников</p> <p>УК-3.3 Имеет навыки организации и руководства работой команды, презентации результатов собственной и командной работы</p>		
--	---	--	--

<p>УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия</p>	<p>УК-4.1 Знает методики поиска, сбора и обработки информации с помощью информационно-коммуникационных технологий; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; особенности устного и письменного общения на русском и иностранном языках; правила и закономерности деловой устной и письменной коммуникации.</p> <p>УК-4.2 Умеет применять различные методы делового общения на русском и иностранном языках как в устной, так и в письменной форме; представляет информацию на русском и иностранном языке с помощью информационно-коммуникационных технологий</p> <p>УК-4.3 Владеет навыками чтения и перевода текстов на иностранном языке в профессиональном общении; навыками деловых коммуникаций в устной и письменной форме на русском и иностранном языках</p>	<p>Опосредованно, на основании результатов промежуточной аттестации по дисциплинам / практикам учебного плана</p>	<p>см. п. 7.2</p>
<p>УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия</p>	<p>УК-5.1 Знает закономерности и особенности социально-исторического развития различных культур в этическом и философском контексте.</p> <p>УК-5.2 Понимает и воспринимает разнообразие общества в социальноисторическом, этическом и философском контекстах.</p> <p>УК-5.3 Владеет навыками взаимодействия в мире культурного многообра-</p>	<p>Опосредованно, на основании результатов промежуточной аттестации по дисциплинам / практикам учебного плана</p>	<p>см. п. 7.2</p>

Код контролируемой компетенции	Индикаторы достижения компетенции	Наименование оценочного средства	Показатели оценки
--------------------------------	-----------------------------------	----------------------------------	-------------------

	<p>зия с использованием этических норм поведения; а также навыками толерантного восприятия межкультурного разнообразия общества в социально-историческом, этическом и философском контекстах.</p>		
<p>УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы её совершенствования на основе самооценки и образования в течение всей жизни</p>	<p>УК-6.1 Знает основные принципы самовоспитания и самообразования, профессионального и личностного развития, исходя из этапов карьерного роста и требований рынка труда. УК6.2 Формулирует цели личностного и профессионального развития и условия их достижения, исходя из индивидуально-личностных особенностей, поставленных жизненных целей и развития социальной ситуации. УК-6.3 Владеет технологиями приобретения, использования и обновления социокультурных и профессиональных знаний, умений и навыков; методиками саморазвития и самообразования</p>	<p>Опосредованно, на основании результатов промежуточной аттестации по дисциплинам / практикам учебного плана</p>	<p>см. п. 7.2</p>

<p>УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности</p>	<p>УК-7.1 Знает роль и значение физической культуры в жизни человека и общества; научно-практические основы физической культуры, а также систему профилактики вредных привычек и формирования здорового образа и стиля жизни.</p> <p>УК-7.2 Умеет применять на практике разнообразные средства физической культуры и спорта для сохранения и укрепления здоровья и психофизической подготовки; использует средства и методы физического воспитания для профессионально-личностного развития, физического самосовершенствования, формирования здорового образа и стиля жизни.</p> <p>УК-7.3 Владеет навыками поддержания здоровья и физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности.</p>	<p>Опосредованно, на основании результатов промежуточной аттестации по дисциплинам / практикам учебного плана</p>	<p>см. п. 7.2</p>
<p>УК-8. Способен создавать и поддерживать в повседневной жизни и в профессио-</p>	<p>УК-8.1 Знает классификацию и источники чрезвычайных ситуаций природного и техногенного происхождения; причины, признаки и последствия опасностей, методы защиты в условиях</p>	<p>Опосредованно, на основании результатов промежуточной аттестации по дисципли-</p>	<p>см. п. 7.2</p>

<p>Код контролируемой компетенции</p>	<p>Индикаторы достижения компетенции</p>	<p>Наименование оценочного средства</p>	<p>Показатели оценки</p>
--	---	--	---------------------------------

<p>нальной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов</p>	<p>чрезвычайных ситуаций, военных конфликтов; принципы организации безопасности труда на предприятии, технические средства защиты людей в условиях чрезвычайной ситуации, методы сохранения природной среды, факторы обеспечения устойчивого развития общества</p> <p>УК-8.2 Умеет поддерживать безопасные условия жизнедеятельности; обеспечивать условия труда на рабочем месте; выявлять признаки, причины и условия возникновения чрезвычайных ситуаций; оценивать вероятность возникновения потенциальной опасности и принимать меры по ее предупреждению.</p> <p>УК-8.3 Владеет методами прогнозирования возникновения опасных или чрезвычайных ситуаций; навыками по применению основных методов защиты в условиях чрезвычайных ситуаций.</p>	<p>плинам / практикам учебного плана</p>	
<p>УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности</p>	<p>УК-9.1 Знает базовые принципы функционирования экономики и экономического развития, цели и формы участия государства в экономике, методы личного экономического и финансового планирования, основные финансовые инструменты, используемые для управления личными финансами. УК9.2 Умеет анализировать информацию для принятия обоснованных экономических решений, применять экономические знания при выполнении практических задач.</p> <p>УК-9.3 Владеет способностью использовать основные положения и методы экономических наук при решении социальных и профессиональных задач.</p>	<p>Опосредованно, на основании результатов промежуточной аттестации по дисциплинам / практикам учебного плана</p>	<p>см. п. 7.2</p>

УК-10. Способен формировать нетерпимое отношение к коррупционному поведению	УК-10.1 Знает сущность коррупционного поведения и его взаимосвязь с социальными, экономическими, политическими и иными условиями; действующие правовые нормы, обеспечивающие борьбу с коррупцией в различных областях жизнедеятельности и способы профилактики коррупции. УК-10.2 Умеет анализировать, толковать и применять правовые нормы о		
---	---	--	--

Код контролируемой компетенции	Индикаторы достижения компетенции	Наименование оценочного средства	Показатели оценки
	противодействию коррупционному поведению. УК-10.3 Владеет навыками работы с законодательными и другими нормативными правовыми актами.		
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1 Знает понятие информационного общества, его характерные черты и признаки, основные тенденции развития; сущность информационной инфраструктуры; основные формы проявления информации, её свойства как объекта безопасности; угрозы и источники угроз информационной безопасности современного общества ОПК-1.2 Умеет выполнять поиск и анализ информации для принятия решений; умеет применять основные методы обеспечения информационной безопасности ОПК-1.3 Владеет навыками работы с компьютером как средством управления информацией; навыками использования облачных технологий для хранения и обработки информации; навыками защиты конфиденциальности и данных во всех объектах сетевой инфраструктуры, онлайн-приложениях и платформах	Теоретический вопрос, практическое задание (задача) ГЭ	см. п. 7.3

<p>ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности</p>	<p>ОПК-2.1 Знает теорию в области использования современных языков и систем программирования, особенности функционирования программных средств системного и прикладного назначений</p> <p>ОПК-2.2 Умеет разрабатывать оконные приложения, рационально использовать функциональные возможности программных средств системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности</p> <p>ОПК-2.3 Владеет навыками разработки приложений с использованием WinAPI; использования системного программного обеспечения для решения задач профессиональной деятельности</p>	<p>Доклад на защите ВКР, ответы на вопросы на защите ВКР</p>	<p>см. п. 7.4</p>
<p>ОПК-3. Способен</p>	<p>ОПК-3.1 Знает математические мето-</p>	<p>Опосредованно,</p>	<p>см. п. 7.2</p>

<p>Код контролируемой компетенции</p>	<p>Индикаторы достижения компетенции</p>	<p>Наименование оценочного средства</p>	<p>Показатели оценки</p>
<p>использовать математические методы, необходимые для решения задач профессиональной деятельности</p>	<p>ды, необходимые для решения задач профессиональной деятельности</p> <p>ОПК-3.2 Умеет использовать типовые математические методы и модели для решения задач профессиональной деятельности</p>	<p>на основании результатов промежуточной аттестации по дисциплинам / практикам учебного плана</p>	
	<p>ОПК-3.3 Владеет навыками решения стандартных математических задач, выполнения расчетов математических величин, применения математических методов для решения задач профессиональной деятельности</p>	<p>Доклад на защите ВКР, ответы на вопросы на защите ВКР</p>	<p>см. п. 7.4</p>

<p>ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности</p>	<p>ОПК-4.1 Знает основные понятия, законы и модели физики, основные физические явления, основные каналы утечки информации за счет существования физических полей; принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры</p> <p>ОПК-4.2 Умеет использовать физические законы, анализировать и применять модели явлений, процессов и объектов (включая схемы электронных устройств) при решении инженерных задач в профессиональной деятельности; проводить измерения и оценку параметров сигналов в информационных системах</p> <p>ОПК 4.3 Владеет основными методами теоретического и экспериментального исследования физических явлений и процессов, в том числе лежащих в основе микроэлектронной техники; навыками разработки и оптимизация электронных схем с учетом требований по защите информации</p>	<p>Теоретический вопрос, практическое задание (задача) ГЭ</p>	<p>см. п. 7.3</p>
<p>ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации</p>	<p>ОПК-5.1 Знает основные нормативные правовые акты в области защиты информации; национальные, межгосударственные и международные стандарты в области защиты информации</p> <p>ОПК-5.2 Умеет находить необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью правовых информа-</p>	<p>Доклад на защите ВКР, ответы на вопросы на защите ВКР</p>	<p>см. п. 7.4</p>

Код контролируемой компетенции	Индикаторы достижения компетенции	Наименование оценочного средства	Показатели оценки
--------------------------------	-----------------------------------	----------------------------------	-------------------

	<p>ционных систем; применять действующую законодательную базу в области информационной безопасности; разрабатывать проекты нормативных документов, регламентирующих работу по защите информации, а также положений, инструкций и других организационнораспорядительных документов. ОПК5.3 Владеет навыками использования нормативных актов в профессиональной деятельности.</p>		
<p>ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю</p>	<p>ОПК-6.1 Знает основные нормативные правовые акты, нормативные и методические документы ФСБ, ФСТЭК в области защиты информации ограниченного доступа</p> <p>ОПК-6.2 Умеет применять на практике основные нормативные правовые акты, нормативные и методические документы ФСБ, ФСТЭК в области защиты информации ограниченного доступа</p> <p>ОПК-6.3 Владеет навыками использования нормативных правовых актов, нормативных и методических документов ФСБ, ФСТЭК в области защиты информации ограниченного доступа при решении профессиональных задач</p>	<p>Доклад на защите ВКР, ответы на вопросы на защите ВКР</p>	<p>см. п. 7.4</p>
<p>ОПК-7. Способен создавать программы на языках общего назначения,</p>	<p>ОПК-7.1 Знает современные языки программирования общего назначения; основы структурного и модульного программирования; современные технологии и методы</p>	<p>Теоретический вопрос, практическое задание (задача) ГЭ</p>	<p>см. п. 7.3</p>

применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и спосо-	программирования; ОПК-7.2 Умеет формализовать поставленную задачу; применять соответствующий язык программирования при решении конкретных научных и практических задач; выбирать технологию и метод программирования для решения конкретной задачи ОПК-7.3 Владеет средствами разработки приложений для ОС реального режима работы микропроцессора; вла-	Доклад на защите ВКР, ответы на вопросы на защите ВКР	см. п. 7.4
--	--	---	------------

Код контролируемой компетенции	Индикаторы достижения компетенции	Наименование оценочного средства	Показатели оценки
бов организации программ	деет средствами разработки приложений для ОС защищенного режима работы микропроцессора; владеет методами разработки приложений для решения профессиональных задач; навыками использования типовых инструментальных средств программирования для решения профессиональных задач		
ОПК-8. Способен применять методы научных исследований при проведении разработок в области защиты информации и автоматизированных системах	ОПК-8.1 Знает основные перспективы развития науки и техники в области защиты информации и автоматизированных систем, основные методы проведения научных исследований ОПК-8.2 Умеет применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами; умеет применять методы и системы искусственного интеллекта при реализации практических разработок в области защиты информации в автоматизированных системах ОПК-8.3 Владеет навыками применения научных методов в	Теоретический вопрос, практическое задание (задача) ГЭ	см. п. 7.3
		Доклад на защите ВКР, ответы на вопросы на защите ВКР	см. п. 7.4

	профессиональной деятельности; навыки решения научно-технических		
	задач в области своей профессиональной деятельности		

<p>ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации</p>	<p>ОПК-9.1 Знает текущее состояние и тенденции развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации; порядок организации работ по технической защите конфиденциальной информации на объектах информатизации</p> <p>ОПК-9.2 Умеет планировать, организовывать и контролировать выполнение мероприятий по технической защите информации</p> <p>ОПК-9.3 Владеет методами проектирования и навыками эксплуатации систем и сетей передачи информации при решении задач профессиональной деятельности; навыками применения современных аппаратных устройств защиты информации и систем переда-</p>	<p>Доклад на защите ВКР, ответы на вопросы на защите ВКР</p>	<p>см. п. 7.4</p>
--	---	--	-------------------

Код контролируемой компетенции	Индикаторы достижения компетенции	Наименование оценочного средства	Показатели оценки
	<p>чи информации</p>		
<p>ОПК-10. Способен использовать средства</p>	<p>ОПК-10.1 Знает основы симметричной криптографии и криптографии с открытым ключом,</p>	<p>Теоретический вопрос, практическое</p>	<p>см. п. 7.3</p>

<p>криптографической защиты информации при решении задач профессиональной деятельности</p>	<p>основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах</p>	<p>задание (задача) ГЭ</p>	
	<p>ОПК-10.2 Умеет использовать инфраструктуру открытых ключей, разрабатывать и анализировать программные модели средств криптографической защиты информации</p> <p>ОПК-10.3 Владеет навыками и подходами к анализу безопасности криптографических протоколов</p>	<p>Доклад на защите ВКР, ответы на вопросы на защите ВКР</p>	<p>см. п. 7.4</p>

ОПК-11. Способен разрабатывать компоненты систем защиты информации автоматизированных систем	<p>ОПК-11.1 Знает программноаппаратные средства, используемые в качестве компонентов систем защиты информации в программном обеспечении автоматизированных систем; методы проектирования решений по обеспечению безопасности автоматизированных систем</p> <p>ОПК-11.2 Умеет проектировать защищенные распределенные информационные системы и компоненты систем защиты информации автоматизированных систем</p> <p>ОПК-11.3 Владеет навыками разработки компонентов систем защиты информации автоматизированных систем и защищенных распределенные информационные системы</p>	Теоретический вопрос, практическое задание (задача) ГЭ	см. п. 7.3
		Доклад на защите ВКР, ответы на вопросы на защите ВКР	см. п. 7.4
ОПК-12. Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	<p>ОПК-12.1 Знает принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей, операционных систем и баз данных; основы обеспечения информационной безопасности вычислительных сетей, операционных систем и баз данных</p> <p>ОПК-12.2 Умеет проектировать и администрировать компьютерные сети, реализовывать политику безопасности в сетях ЭВМ, операционных системах и базах данных</p> <p>ОПК-12.3 Владеет навыками построе-</p>	Доклад на защите ВКР, ответы на вопросы на защите ВКР	см. п. 7.4

Код контролируемой компетенции	Индикаторы достижения компетенции	Наименование оценочного средства	Показатели оценки
--------------------------------	-----------------------------------	----------------------------------	-------------------

	<p>ния и администрирования компьютерных сетей, администрирования операционных систем и баз данных с учетом требований по обеспечению безопасности</p>		
<p>ОПК-13. Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем</p>	<p>ОПК-13.1 Знает основные подходы к проведению анализа защищенности и тестирования систем защиты информации автоматизированных систем ОПК-13.2 Умеет выбирать программное и аппаратное обеспечение для проведения анализа защищенности и тестирования систем защиты информации; проводить анализ уязвимостей систем защиты информации автоматизированных систем</p> <p>ОПК-13.3 Владеет навыками проведения анализа защищенности автоматизированных систем, тестирования систем защиты информации автоматизированных систем, проведения анализа уязвимостей систем защиты информации автоматизированных систем</p>	<p>Теоретический вопрос, практическое задание (задача) ГЭ</p>	<p>см. п. 7.3</p>
		<p>Доклад на защите ВКР, ответы на вопросы на защите ВКР</p>	<p>см. п. 7.4</p>
	<p>информации автоматизированных систем</p>		

<p>ОПК-14. Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для техникоэкономического обоснования проектных решений</p>	<p>ОПК-14.1 Знает автоматизированные системы контроля информационной безопасности, систем защищенности и обеспечения их информационной безопасности</p> <p>ОПК-14.2 Умеет проводить подготовку исходных данных для техникоэкономического обоснования проектных решений</p> <p>ОПК-14.3 Владеет навыком разработки защищенных автоматизированных систем, их эксплуатации и внедрения с учетом требований по защите информации</p>	<p>Доклад на защите ВКР, ответы на вопросы на защите ВКР</p>	<p>см. п. 7.4</p>
<p>ОПК-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защи-</p>	<p>ОПК-15.1 Знает средства и системы защиты информации автоматизированных систем, основные принципы администрирования защищенных компьютерных систем</p> <p>ОПК-15.2 Умеет выполнять функции администратора безопасности защищенных компьютерных систем</p> <p>ОПК-15.3 Владеет средствами администрирования программноаппаратных комплексов защиты информации от</p>	<p>Доклад на защите ВКР, ответы на вопросы на защите ВКР</p>	<p>см. п. 7.4</p>

Код контролируемой компетенции	Индикаторы достижения компетенции	Наименование оценочного средства	Показатели оценки
ценности автоматизированных систем	несанкционированного доступа		

<p>ОПК-16. Способен анализировать основные этапы и закономерности исторического развития России, её место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма</p>	<p>ОПК-16.1 Знает основные тенденции в развитии российского государства, значимые факты и события из истории России в рассматриваемые периоды ОПК-16.2 Умеет анализировать и оценивать историческую информацию, факторы и механизмы исторических изменений ОПК-16.3 Владеет понятийно-терминологическим аппаратом в области истории</p>	<p>Опосредованно, на основании результатов промежуточной аттестации по дисциплинам / практикам учебного плана</p>	<p>см. п. 7.2</p>
<p>ОПК-7.1. Способен использовать программные и программноаппаратные средства для моделирования и испытания систем защиты информационных систем</p>	<p>ОПК-7.1.1 Знает программные и программноаппаратные средства для моделирования и испытания систем защиты информационных систем; методы применения программных и программноаппаратных средств для моделирования и испытания систем защиты информационных систем ОПК-7.1.2 Умеет выбирать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем ОПК-7.1.3 Владеет навыками применения программных и программноаппаратных средств для моделирования и испытания систем защиты информационных систем</p>	<p>Теоретический вопрос, практическое задание (задача) ГЭ</p>	<p>см. п. 7.3</p>
		<p>Доклад на защите ВКР, ответы на вопросы на защите ВКР</p>	<p>см. п. 7.4</p>
<p>ОПК-7.2. Способен разрабатывать методики и тесты для анализа степени защищенности</p>	<p>ОПК-7.2.1 Знает основные подходы к проведению анализа защищенности автоматизированных систем, знает существующие методики и тесты для анализа</p>	<p>Теоретический вопрос, практическое задание (задача) ГЭ</p>	<p>см. п. 7.3</p>

информационной системы и её соответствия нормативным требованиям по защите информации	<p>степени защищенности информационной системы и её соответствия нормативным требованиям по защите информации</p> <p>ОПК-7.2.2 Умеет строить план проведения анализа системы защиты автоматизированных систем; умеет разрабатывать методики и тесты для анализа степени защищенности информации-</p>	Доклад на защите ВКР, ответы на вопросы на защите ВКР	см. п. 7.4
---	--	---	------------

Код контролируемой компетенции	Индикаторы достижения компетенции	Наименование оценочного средства	Показатели оценки
	<p>онной системы и её соответствия нормативным требованиям по защите информации</p> <p>ОПК-7.2.3 Владеет навыком построения плана тестирования для проведения анализа защищенности; владеет методиками и навыками проведения тестов для анализа степени защищенности информационной системы и её соответствия нормативным требованиям по защите информации</p>		
ОПК-7.3. Способен проводить анализ защищенности и верификацию программного обеспечения информационных систем	<p>ОПК-7.3.1 Знает виды и порядок проведения анализа защищенности автоматизированных систем</p> <p>ОПК-7.3.2 Умеет выбирать программное и аппаратное обеспечение для проведения анализа защищённости автоматизированных систем</p> <p>ОПК-7.3.3 Владеет навыками проведения анализа защищенности и верификации программного обеспечения автоматизированных систем</p>	Доклад на защите ВКР, ответы на вопросы на защите ВКР	см. п. 7.4

<p>ПК-1: Способен проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем</p>	<p>ПК-1.1 Знает структурные и функциональные схемы защищенных автоматизированных систем</p> <p>ПК-1.2 Умеет проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем</p> <p>ПК-1.3 Владеет навыками выявления потенциальных уязвимостей информационной безопасности автоматизированных систем</p>	<p>Доклад на защите ВКР, ответы на вопросы на защите ВКР</p>	<p>см. п. 7.4</p>
<p>ПК-2: Способен проводить анализ защищенности информационной инфраструктуры автоматизированной системы</p>	<p>ПК-2.1 Знает способы проведения анализа защищенности информационной инфраструктуры автоматизированных систем</p> <p>ПК-2.2 Умеет выбирать способ проведения анализа защищенности информационной инфраструктуры автоматизированных систем</p> <p>ПК-2.3 Владеет навыками проведения анализа защищенности информационной инфраструктуры автоматизированных систем</p>	<p>Доклад на защите ВКР, ответы на вопросы на защите ВКР</p>	<p>см. п. 7.4</p>

Код контролируемой компетенции	Индикаторы достижения компетенции	Наименование оценочного средства	Показатели оценки
--------------------------------	-----------------------------------	----------------------------------	-------------------

<p>ПК-3: Способен проводить анализ технической документации информационной инфраструктуры автоматизированной системы</p>	<p>ПК-3.1 Знает методики проведения анализа технической документации информационной инфраструктуры автоматизированной системы</p> <p>ПК-3.2 Умеет выбрать методику проведения анализа технической документации информационной инфраструктуры автоматизированной системы</p> <p>ПК3.3 Владеет навыками проведения анализа технической документации информационной инфраструктуры автоматизированной системы</p>	<p>Доклад на защите ВКР, ответы на вопросы на защите ВКР</p>	<p>см. п. 7.4</p>
--	--	--	-------------------

<p>ПК-4: Способен анализировать программные, архитектурнотехнические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах</p>	<p>ПК-4.1 Знает программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем</p> <p>ПК-4.2 Умеет выбрать программные, архитектурнотехнические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах</p> <p>ПК-4.3 Владеет навыками анализа программных, архитектурнотехнических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах</p>	<p>Доклад на защите ВКР, ответы на вопросы на защите ВКР</p>	<p>см. п. 7.4</p>
---	---	--	-------------------

ПК-5: Способен контролировать безотказное функционирование технических средств защиты информации	<p>ПК-5.1 Знает способы контроля безотказного функционирования технических средств защиты информации</p> <p>ПК-5.2 Умеет выбрать способ контроля безотказного функционирования технических средств защиты информации</p> <p>ПК-5.3 Владеет навыками контроля безотказного функционирования технических средств защиты информации</p>	Доклад на защите ВКР, ответы на вопросы на защите ВКР	см. п. 7.4
ПК-6: Способен проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов	<p>ПК-6.1 Знает способы проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов</p> <p>ПК-6.2 Умеет выбрать способ проектирования подсистем безопасности информации с учетом действующих</p>	Доклад на защите ВКР, ответы на вопросы на защите ВКР	см. п. 7.4
	нормативных и методических документов		
Код контролируемой компетенции	Индикаторы достижения компетенции	Наименование оценочного средства	Показатели оценки
	ПК-6.3 Владеет навыками проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов		

7.2 Оценка уровня сформированности компетенций выпускника, контролируемых опосредованно в процессе ГИА на основании результатов промежуточной аттестации по дисциплинам и практикам учебного плана

Опосредованно в процессе ГИА в рамках государственного экзамена, на основании результатов промежуточной аттестации по дисциплинам и практикам учебного плана, оценивается уровень сформированности следующих компетенций: УК1, УК2, УК3, УК4, УК5, УК6, УК8, УК9, УК-10, ОПК-3, ОПК-16.

Критерии оценки данных компетенций:

- компетенция сформирована на **базовом уровне**, если средняя оценка промежуточной аттестации по дисциплинам и практикам учебного плана, направленным на ее формирование, меньше 4 баллов;

- компетенция сформирована на **высоком уровне**, если средняя оценка промежуточной аттестации по дисциплинам и практикам учебного плана, направленным на ее формирование не меньше 4 баллов.

Информация об уровне сформированности компетенций, контролируемых опосредованно в рамках государственного экзамена на основании результатов промежуточной аттестации по дисциплинам и практикам учебного плана, вносится в сводный оценочный лист выпускника (приложение 1).

7.3 Оценка уровня сформированности компетенций выпускника, контролируемых в процессе государственного экзамена

7.3.1 Перечень контрольных заданий или иных материалов, выносимых для проверки на ГЭ

Перечень вопросов и типовых практических заданий (задач) представлены таблице 9 и таблице 10 соответственно.

Таблица 9 – Перечень вопросов к государственному экзамену

№	Содержание вопроса	Рекомендуемая литература
Разработка и эксплуатация автоматизированных систем в защищённом исполнении		
1	Основные вектора атак злоумышленников на распределенные информационные системы. Анализ векторов, Defense in Depth. Конфиденциальность, целостность, доступность.	1. Челухин. В. А. Разработка и проектирование защищённых автоматизированных систем в области информационной безопасности./ Владимир Алексеевич Челухин. – [б.м.]:Издательские решения, 2020. – 78 с. 2. Челухин. В. А. Комплексное обеспечение информационной безопасности: Для студентов технических специальностей/ Владимир
2	Состав документации для автоматизированных систем в защищенном исполнении.	
3	Использование систем обнаружения и	

	предотвращения вторжений для обеспечения информационной безопасности распределенных информационных систем. Honeypot.	Алексеевич Челухин. – [б.м.]:Издательские решения, 2021. – 308 с.
4	Атаки на системы виртуализации на базе VmWare ESXi, Citrix XenServer, Microsoft HyperV. Способы защиты.	3. Челухин. В. А. Информационная безопасность предприятия: Москва2020/ Владимир Алексеевич Челухин. – [б.м.]:Издательские решения, 2020. – 144 с .
5	Требования к автоматизированным системам обрабатывающим информацию ограниченного доступа, не содержащей сведений составляющих государственную тайну.	Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программноаппаратные средства
6	Защита виртуальных инфраструктур в соответствии с требованиями ФСТЭК и ФСБ	[Электронный ресурс] : учебнометодическое пособие / Д.В. Фомин.
7	Основные направления защиты автоматизированных систем от утечки информации по техническим каналам. Программные и аппаратные средства обеспечения информационной безопасности.	— Электрон. текстовые данные. – Саратов : Вузовское образование, 2018. – 218 с. – Режим доступа: http://www.iprbookshop.ru/77317.html ,
8	Основные направления защиты автоматизированных систем от несанкционированного доступа. Программные и аппаратные средства обеспечения информационной безопасности	ограниченный. – Загл. с экрана.
9	Способы обеспечения отказоустойчивости защищенных автоматизированных систем. Резервирование основных компонентов и информационных узлов. Обеспечение QoS.	
10	Требования ФСТЭК к лицензиатам по технической защите конфиденциальной информации.	
Тестирование на проникновение и анализ безопасности, анализ и защита веб-приложений		
1	OSINT. Разведка и рефлексивная разведка.	1. Прутяну, Э. Как стать хакером:
2	Тестирование Web-приложений. Реверс прокси. Анализ заголовков.	сборник практических сценариев, позволяющих понять, как рассуждает злоумышленник :
3	OWASP Top 10 уязвимостей информационных систем	практическое руководство / Э. Прутяну ; пер. с англ. Д. А.
4	XSS. Основные виды. Способы эксплуатации.	Беликова. - Москва : ДМК Пресс, 2020. - 380 с. - ISBN 978-5-97060-802-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1094954
5	SQL injection. Виды, механизмы сканирования, способы и методы защиты.	
6	Планирование и анализ атак на сетевые устройства. Планирование и анализ атак на АРМ.	

7	Типовые уязвимости приложений для мобильных платформ. Реверс инжиниринг мобильных приложений.	(дата обращения: 07.02.2022). – Режим доступа: по подписке.
8	Анализ сетевого трафика. Методы sniffing и спуфинга. Инъекция пакетов.	2. Ховард, М. 19 смертных грехов, угрожающих безопасности программ. Как не допустить типичных ошибок / М. Ховард, Д.
9	Уязвимости операционных систем. Уязвимости протоколов. Атаки на VLAN.	Лебланк, Д. Виера. - Москва : ДМК Пресс, 2009. -
10	Тестирование сетевой безопасности.	288 с.: ил. - ISBN 5-9706-0027-X. - Текст : электронный. - URL: https://znanium.com/catalog/product/407173

		(дата обращения: 07.02.2022). – Режим доступа: по подписке. 3. Бирюков, А. А. Информационная безопасность: защита и нападение / А.А. Бирюков. - - 2-е изд., перераб. и доп. - Москва : ДМК Пресс, 2017. - 434 с. - ISBN 978-5-97060-435-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1028060 (дата обращения: 07.02.2022). – Режим доступа: по подписке.
--	--	---

Аппараты и средства перехвата информации, анализ защищённости распределённых информационных систем

1	Утечка информации по каналу высокочастотного облучения и высокочастотного навязывания и аппараты и средства перехвата.	.Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. – М.: Горячая линия– Телеком, 2005. – 416 с. 2.Хорев А.А. Техническая защита информации. Учебное пособие. 2008. - 436 с.ISBN978-59901488-1-9 3.Вильдяйкин
2	Утечка информации по каналу акустоэлектрических преобразований аппараты и средства перехвата.	Г.Ф. Аппараты и средства перехвата информации ISBN 978-5-0050-0021-7/. Создано в интеллектуальной издательской системе Ridero 2019 г. 4. Семенов Н. С. Компьютерные вирусы как средство электронной борьбы. Судостроение за рубежом. 1990. N 12. С. 48-61.
3	Утечка информации по виброакустическому каналу и аппараты и средства перехвата.	5. Каталог ANT (АНБ) // www.eff.org : каталог. 2014 01 июн. URL: https://www.eff.org/files/2014/01/06/20131230appelbaumnsa_ant_catalog.pdf (Дата обращения: 27.05.2017)

4	Утечка информации по акустическому каналу и аппараты и средства перехвата.	6. Утечка информации по каналам пэми и способы их защиты // www.appliedresearch.ru : журнал 2016 23 июл. URL https://www.applied-research.ru/ru/article/view?id=10110 (Дата обращения: 20.05.2017)	
5	Технические каналы утечки информации. Нелинейные преобразования. Использование нелинейных локаторов.		
6	Автоматизация процесса сканирования на наличие уязвимостей. Сканеры уязвимостей информационных систем		
7	Типовые уязвимости распределенных информационных систем		
8	Виды и способы атак на распределенные информационные системы		
9	Основные базы и банки данных уязвимостей распределенных информационных систем.		
10	Механизмы защиты распределенных информационных систем от возможных атак и эксплуатации уязвимостей, включая уязвимости zero day.		
Техника и технология атак злоумышленников в распределённых информационных системах			
1	Сканирование сети. Виды сканирования. Используемое программное и аппаратное обеспечение при проведении сканирования. Рекогнасцировка.		1. Бабин, С. А. Лаборатория хакера : практическое руководство / С. А. Бабин. - Санкт-Петербург : БХВ-Петербург, 2016. - 240 с. - (Глазами хакера). - ISBN 978-5-9775-3535-9.

2	Атаки на сетевую инфраструктуру. Атаки на IoT. Механизмы поиска уязвимостей в инфраструктуре IoT. Доверенные взаимодействия и операционные системы реального	- Текст : электронный. - URL: https://znanium.com/catalog/product/1860821 (дата обращения: 07.02.2022). –
---	--	--

	времени.	Режим доступа: по подписке.
3	Атаки типа MITM. Использование Фреймворков и ручное проведение атак.	2. Шелухин, О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии): Учебное пособие для вузов / О.И.
4	Атаки типа DoS и DDoS. Использование уязвимостей протоколов для реализации атак.	Шелухин, Д.Ж. Сакалема, А.С. Филинова. - Москва : Гор. линия-Телеком, 2013. - 220 с.: ил.; . ISBN 978-5-9912-0323-4, 500 экз. -
5	TCP hijacking. Подмена пакетов. Механизмы обхода межсетевых экранов, DLP системы.	Текст : электронный. - URL:
6	Атаки на Wi-Fi. Необходимое оборудование, виды атак WEP/WPA/WPA2. Несовершенство сетевых протоколов для беспроводных сетей. Атаки подменой точки доступа. Подходы к атакам на WPA3.	https://znanium.com/catalog/product/421968 (дата обращения: 07.02.2022). – Режим доступа: по подписке.
7	Вредоносные программы. Фишинг. Использование троянов при проведении атак на информационные системы. Ботнет сети. Социальная инженерия. Механизмы комплексной защиты информации на предприятии.	
8	Подходы к тактической и стратегической защите периметра предприятия от возможных атак внутренних и внешних злоумышленников	
9	Бинарные уязвимости. Аппаратные уязвимости микропроцессоров. Атаки на ключевую инфраструктуру. Эксплоиты.	
10	Повышение привилегий. Эскалация в рамках операционных систем, сетевых инфраструктур. Metasploit Framework. Специализированные дистрибутивы для анализа защищенности	
Системы интеллектуальной защиты информации		
1	Интеллектуальные системы видеонаблюдения и контроля доступа. Алгоритмы, производители. Задачи и функции видеоаналитики.	1 Антамошкин, О. А. Системы интеллектуальной защиты информации.

2	Системы интеллектуальной защиты информации в рамках цифровой экономики.	<p>Теория и практика [Электрон-ный ресурс] : учебник / О. А. Антамошкин. - Красноярск: Сиб. Федер. унт, 2012. - 247 с. // ZNANIUM.COM : электронно-библиотечная система. – Режим доступа: http://znanium.com/catalog.php#, ограниченный. – Загл. с экрана.</p> <p>2 Практическая Системы интеллектуальной защиты информации на основе учебного примера: Учебное пособие / Мацяшек Л.А., Лионг Б.Л., - 3-е изд., (эл.) - М.:БИНОМ. Лаб. знаний, 2015. - 959 с // ZNANIUM.COM : электронно-библиотечная система. – Режим доступа: http://znanium.com/catalog.php#, ограниченный. – Загл. с экрана. 3</p> <p>Объектно-ориентированное программирование с примерами на C#: Учебное пособие / Хорев П.Б. - М.: Форум, НИЦ ИНФРА-М, 2016. - 200 с // ZNANIUM.COM : электрон-</p>
3	Интеллектуальные системы обеспечения информационной безопасности на основе цифровых двойников.	
4	Высокопроизводительные вычисления и использование современных графических ускорителей в задачах глубокого обучения для защиты информации.	
5	Виды нейронных сетей и активационных функций. Применение различных сетей в системах защиты информации	
6	Морфологический, синтаксический и семантический анализ входных сообщений. Анализ больших данных в масштабе реального времени.	
7	Экспертные системы и нечеткие экспертные	
	системы для задач классификации и принятия решений в области обеспечения информационной безопасности.	

8	Технологии искусственного интеллекта для антифрода. Внешние и инсайдерские угрозы. Интеллектуальные системы защиты блокчейн-технологий	<p>но-библиотечная система. – Режим доступа: http://znanium.com/catalog.php#, ограниченный. – Загл. с экрана 4</p> <p>Введение в программную инженерию : Учебник / В.А. Антипов, А.А. Бубнов, А.Н. Пылькин, В.К. Столчев. — М.: КУРС: ИНФРА-М, 2017. — 336 с // ZNANIUM.COM : электронно-библиотечная система. – Режим доступа: http://znanium.com/catalog.php#, ограниченный. – Загл. с экрана.</p>
9	Кластеризация с помощью нейронных сетей. Использование в задачах классификации. Разработка приложений использующих кластеризацию в системах распознавания.	
10	Машинное зрение. Использование в системах интеллектуальной защиты информации. Подходы и библиотеки для создания приложений.	
Программно-аппаратные средства обеспечения информационной безопасности		

1	Одноуровневая модель разграничения доступа, достоинства и недостатки. Дискреционные модели доступа. Многомерные дискреционные модели доступа.	1. Челухин, В.А. Комплексное обеспечение информационной безопасности автоматизированных систем: Учебное пособие для вузов / В. А. Челухин. - Комсомольск-на-
2	Многоуровневая модель разграничения доступа, достоинства и недостатки. Мандатное управление доступом. Ролевое управление доступом. Мониторы безопасности.	Амуре: Изд-во Комсомольского-на-Амуре гос.техн.ун-та, 2021. - 207с. - Библиогр.: с.201-207. - 273-00. 2. Программно-аппаратная защита информации: Учебное пособие / Хорев П.Б.,
3	Сертификация средств программноаппаратной защиты информации. Направления сертификации ФСТЭК, ФСБ, включая сертификацию СВТ, НСД, СОВ, МЭ, СКЗИ.	- М.:Форум, НИЦ ИНФРА-М, 2019. - 352 с.: 60x90 1/16. - (Высшее образование) ISBN 978-5-00091-004-7 - Режим доступа: http://znanium.com/catalog/product/489084 3.
4	Реестр сертифицированных средств защиты информации ФСТЭК и ФСБ. Требования к лицензиатам уполномоченных органов по защите информации в части наличия программных средств.	Аппаратные и программные средства защиты информации: Учебное пособие / Душкин А.В., Кольцов А., Кравченко А. - Воронеж: Научная книга, 2019. - 232 с. ISBN 978-5-4446-0746-6 - Режим доступа: http://znanium.com/catalog/product/923168 4.
5	Низкоуровневый анализ машинного кода. Методы дизассемблирования, реверсинжиниринга исполняемых файлов. Основное программное обеспечение, используемое для анализа приложений, особенности исследований для различных операционных систем.	Аппаратно-программные средства защиты информации: Практикум / Душкин А.В., Дубровин А.С., Здольник В.В. - Воронеж: Научная книга, 2018. - 198 с.: ISBN 9785-4446-1043-5 - Режим доступа: http://znanium.com/catalog/product/977192 .
6	Механизмы организации контроля доступа до загрузки ОС. Механизмы доверенной загрузки ОС, реализованные в СЗИ. Виды и примеры АПМДЗ, особенности реализации для сетевых устройств.	
7	Подсистемы защиты информации и их реализация в СЗИ от НСД «Dallas Lock», Secret	
	Net Studio. Соответствие нормативным документам уполномоченных органов.	

8	Организация защищенных распределенных информационных систем с использованием современных средств защиты информации. Защита сетевого периметра предприятия от внутренних и внешних нарушителей. Системы обнаружения и предотвращения вторжений.
9	Протоколы и средства организации VPN на сетевом уровне. Назначение, область применения, аутентификация и шифрование данных в протоколах SKIP и IPSec. Виды и особенности VPN. TLS, SSL
10	Организация защищенного документооборота с использованием криптографических средств, предоставляемых СКЗИ «КриптоПро» и VipNet CSP.

Таблица 10 – Практические задания (задачи) выносимые на ГЭ

№ задания	Содержание задания
1	Реализовать приложение определяющее обладает ли пользователь административными привилегиями.
2	Реализовать приложение генерирующее пакет информации, содержащий в заголовке определенную пользователем информацию.
3	Реализовать скрипт проводящий анализ при помощи sqldump заданной базы данных.
4	Реализовать приложение «имитирующее» действия пользователя (нажатия клавиатуры, движение на нажатия мыши).
5	Разработать на PowerShell скрипт позволяющий загрузить информацию с удаленного сервера.
6	Разработать на PowerShell скрипт позволяющий получить реверсшелл.
7	Разработать на PowerShell скрипт позволяющий развернуть ftp сервер.
8	Сформировать регулярное выражение (возможно не одно) для разбора html страницы позволяющей выделить тэг <div>
9	Для командного интерпретатора Cisco IoS опишите действия по первичной настройке коммутатора.
10	Для командного интерпретатора bash разработайте скрипт позволяющий загрузить определенную страницу из сети Интернет содержащую параметр передаваемый методом GET и позволяющий подменить его.

11	По заданному IP адресу 192.168.1.1/24 опишите всю информацию которую можно получить и сценарий получения дополнительной информации для данной сети.
12	По заданному IP адресу 2001:db8:a::123/64 опишите всю информацию которую можно получить и сценарий получения дополнительной информации для данной сети.
13	Разработать политику информационной безопасности для автоматизированной системы класса 1а. Обязательно использовать сертифицированные средства защиты от утечки по техническим каналам, от НСД, средства анализа защищенности и мониторинга информационной безопасности. Определить риски ИБ(минимум 6), вероятности реализации рисков, рас-

	считать интегральный показатель рисков, определить систему управления информационной безопасности, разработать план периодических проверок, регламент работ по информационной безопасности.
14	Разработать политику информационной безопасности для автоматизированной системы класса 1б. Обязательно использовать сертифицированные средства защиты от утечки по техническим каналам, от НСД, средства анализа защищенности и мониторинга информационной безопасности. Определить риски ИБ(минимум 6), вероятности реализации рисков, рассчитать интегральный показатель рисков, определить систему управления информационной безопасности, разработать план периодических проверок, регламент работ по информационной безопасности.

15	Разработать политику информационной безопасности для автоматизированной системы класса 1в. Обязательно использовать сертифицированные средства защиты от утечки по техническим каналам, от НСД, средства анализа защищенности и мониторинга информационной безопасности. Определить риски ИБ(минимум 6), вероятности реализации рисков, рассчитать интегральный показатель рисков, определить систему управления информационной безопасности, разработать план периодических проверок, регламент работ по информационной безопасности.
16	Разработать политику информационной безопасности для автоматизированной системы класса 1г. Обязательно использовать сертифицированные средства защиты от утечки по техническим каналам, от НСД, средства анализа защищенности и мониторинга информационной безопасности. Определить риски ИБ(минимум 6), вероятности реализации рисков, рассчитать интегральный показатель рисков, определить систему управления информационной безопасности, разработать план периодических проверок, регламент работ по информационной безопасности.
17	Разработать политику информационной безопасности для автоматизированной системы класса 2а. Обязательно использовать сертифицированные средства защиты от утечки по техническим каналам, от НСД, средства анализа защищенности и мониторинга информационной безопасности. Определить риски ИБ(минимум 6), вероятности реализации рисков, рассчитать интегральный показатель рисков, определить систему управления информационной безопасности, разработать план периодических проверок, регламент работ по информационной безопасности.
18	Разработать политику информационной безопасности для автоматизированной системы класса 2б. Обязательно использовать сертифицированные средства защиты от утечки по техническим каналам, от НСД, средства анализа защищенности и мониторинга информационной безопасности. Определить риски ИБ(минимум 6), вероятности реализации рисков, рассчитать интегральный показатель рисков, определить систему управления информационной безопасности, разработать план периодических проверок, регламент работ по информационной безопасности.

Экзаменационный билет № 1 Государственный экзамен

1. Механизмы организации контроля доступа до загрузки ОС. Механизмы доверенной загрузки ОС, реализованные в СЗИ. Виды и примеры АПМДЗ, особенности реализации для сетевых устройств.

2. Кластеризация с помощью нейронных сетей. Использование в задачах классификации. Разработка приложений использующих кластеризацию в системах распознавания.

3. Технические каналы утечки информации. Нелинейные преобразования. Использование нелинейных локаторов.

4. Реализовать приложение определяющее обладает ли пользователь административными привилегиями.

5. Разработать политику информационной безопасности для автоматизированной системы функционирующей в рамках информационной системы обрабатывающей персональные данные УЗ1. Обязательно использовать сертифицированные средства защиты от утечки по техническим каналам, от НСД, средства анализа защищенности и мониторинга информационной безопасности. Определить риски ИБ (минимум 6), вероятности реализации рисков, рассчитать интегральный показатель рисков, определить систему управления информационной безопасности, разработать план периодических проверок, регламент работ по информационной безопасности.

7.3.2 Показатели и критерии оценки результатов ГЭ

При оценке уровня профессиональной подготовленности по результатам государственного экзамена необходимо учитывать следующие критерии:

- знание учебного материала (учебных дисциплин);
- знание нормативно-законодательных актов и различных информационных источников; - способность к абстрактному логическому мышлению;

Уровень сформированности компетенций / оценка	Описание показателей и критериев оценивания		
	Показатели оценивания	Критерии оценки теоретической части экзамена	Критерии оценки практического задания экзамена

<p>Высокий уровень – оценка «отлично»</p>	<ul style="list-style-type: none"> - знание учебного материала (учебных дисциплин); - знание нормативнозаконодательных актов и различных информационных источников; - способность к абстрактному логическому мышлению; - умение выделить проблемы; - умение определять и расставлять приоритеты; - умение аргументировать свою точку зрения; - умение применять теоретические знания для анализа конкретных производственных 	<p>1. полно раскрыто содержание материала билета; 2. материал изложен грамотно, в определенной логической последовательности, с точной терминологией; 3. показано умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации; 4. продемонстрировано усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость компетенций, умений и навыков; 5. ответ прозвучал самостоятельно, без наводящих вопросов; 6. допущены одна – две неточности при освещении второстепенных вопросов, которые исправляются по замечанию; 7. высокий уровень сформированности универсальных и общепрофессиональных компетенций</p>	<p>Задание выполнено верно и в полном объеме согласно предъявляемым требованиям, проведен правильный анализ, ны аргументированные выводы.</p>
---	---	---	---

- умение выделить проблемы;

- умение определять и расставлять приоритеты; - умение аргументировать свою точку зрения.

Описание показателей и критериев оценивания результатов государственного экзамена, а также шкалы оценивания приведены в таблице 11.

Таблица 11 – Показатели, критерии оценивания результатов ГЭ

Уровень сформированности компетенций / оценка	Описание показателей и критериев оценивания		
	Показатели оценивания	Критерии оценки теоретической части экзамена	Критерии оценки практического задания экзамена
Средний уровень – оценка «хорошо»	<p>ситуаций и решения прикладных проблем; - общий (культурный) и специальный (профессиональный) язык ответа;</p> <p>- уровень сформированности универсальных и общепрофессиональных компетенций</p> <p>-</p>	<p>ответ удовлетворяет в основном требованиям на оценку «5», но при этом имеет недостатки: 1. в изложении допущены небольшие пробелы, не искавшие содержание ответа;</p> <p>2. допущены один – два недочета при освещении основного содержания ответа, исправленные по замечанию экзаменатора;</p> <p>3. допущены ошибка или более двух недочетов при освещении второстепенных вопросов, которые легко исправляются по замечанию экзаменатора; 4. базовый или высокий уровень сформированности универсальных компетенций</p>	<p>Задание выполнено верно, но допущено несколько негрубых ошибок, не влияющих на результат.</p>

<p>Низкий уровень – оценка «удовлетворительно»</p>	<ul style="list-style-type: none"> - знание учебного материала (учебных дисциплин); - знание нормативнозаконодательных актов и различных информационных источников; - способность к абстрактному логическому мышлению; - умение выделить проблемы; - умение определять и расставлять приоритеты; 	<p>1. неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы достаточные умения для усвоенного материала; 2. имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, исправленные после наводящих вопросов; 3. при неполном знании теоретического материала выявлена недостаточная сформированность компетенций, умений и навыков, обучающийся не может применить теорию в новой ситуации; 4. базовый или высокий уровень сформированности универсальных компетенций</p>	<p>При выполнении задания допущены ошибки не существенно влияющие на конечный результат, но ход решения верный</p>
<p>Недостаточный уровень - оценка «неудовлетворительно»</p>	<ul style="list-style-type: none"> - умение аргументировать свою точку зрения; - умение применять теоретические знания для анализа конкретных производственных ситуаций и решения приклад- 	<p>1. не раскрыто основное содержание учебного материала; 2. обнаружено незнание или непонимание большей или наиболее важной части учебного мате-</p>	<p>Задание не выполнено или выполнено со значительными замечаниями</p>
<p>Описание показателей и критериев оценивания</p>			

Уровень сформированности компетенций / оценка	Показатели оценивания	Критерии оценки теоретической части экзамена	Критерии оценки практического задания экзамена
	<p>ных проблем; - общий (культурный) и специальный (профессиональный) язык ответа;</p> <p>- уровень сформированности универсальных и общепрофессиональных компетенций</p>	<p>риала; 3. допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после наводящих вопросов; 4. не сформированы компетенции, умения и навыки; 5. базовый уровень сформированности универсальных компетенций.</p>	

7.4 Оценка уровня сформированности компетенций выпускника, контролируемых в процессе защиты выпускной квалификационной работы

К выпускной квалификационной работе предъявляются следующие основные **требования:**

- раскрытие актуальности, теоретической и практической значимости темы; - правильное использование законодательных и нормативных актов, методических, учебных пособий, а также научных и других источников информации, их критическое осмысление, и оценка практических материалов по выбранной теме;
- демонстрация способности владения современными методами и методиками информационной безопасности автоматизированных систем;
- полное раскрытие темы выпускной квалификационной работы, аргументированное обоснование выводов и формулировка предложений, представляющих научный и практический интерес, с обязательным использованием практического материала; - раскрытие способностей обеспечения систематизации и обобщения собранных по теме материалов, развития навыков самостоятельной работы при проведении научного исследования.

7.4.1 Тематика выпускных квалификационных работ

При выборе темы необходимо учитывать ее актуальность в современных условиях, практическую значимость для учреждений, организаций и предприятий, где были получены первичные исходные данные для подготовки выпускной квалификационной работы.

При выборе темы целесообразно руководствоваться опытом, накопленным при написании курсовых работ, подготовки рефератов и докладов для выступления на семинарах и практических занятиях, конференциях, что позволит обеспечить преемственность научных и практических интересов.

Название темы выпускной квалификационной работы должно быть кратким, отражать основное содержание работы. В названии темы нужно указать объект и / или инструментарий, на которые ориентирована работа. В работе следует применять новые технологии и современные методы.

Примерная тематика ВКР:

- 1 Аттестация и анализ объекта информатизации на соответствие требованиям по защите информации для (на материалах конкретного предприятия).
- 2 Аттестация и анализ государственной информационной системы (на материалах конкретного предприятия).
- 3 Анализ комплексной системы защиты информации (на материалах конкретного предприятия).
- 4 Проектирование и анализ защищенной автоматизированной системы (на материалах конкретного предприятия).

5 Обеспечение информационной безопасности и анализ распределенной информационной системы(на материалах конкретного предприятия).

6 Организация аудита значимого объекта критической информационной инфраструктуры

7 Анализ безопасности распределенной платежной системы

8 Анализ безопасности и оценка рисков использования беспроводных технологий на предприятии

9 Разработка программного обеспечения для автоматизации процесса аудита информационной безопасности.

10 Разработка и анализ защищенных мобильных приложений.

11 Анализ безопасности распределенной информационной системы с cloud computing.

38

12 Использование генетических алгоритмов в задачах анализа защищенности информационных систем.

13 Разработка математических моделей для анализа защищенности информационной системы.

14 Разработка системы управления информационной безопасностью (на материалах конкретного предприятия).

15 Исследование моделей управления доступом для аудита информационной безопасности

16 Анализ защищенности сети предприятия (на материалах конкретного предприятия).

17 Разработка программного обеспечения для анализа исходных текстов приложений на наличие недекларированных возможностей.

18 Особенности реализации угроз безопасности в ОС Windows или Unix.

19 Разработка программного обеспечения для имитации тестовых сигналов от различных устройств для проведения аттестации и анализа по требованиям информационной безопасности.

20 Организация и анализ защищенности циркулирующего трафика в территориально-распределенной локальной вычислительной сети с использованием систем защиты Континент.

21 Организация и анализ защищенности циркулирующего трафика в территориально-распределенной локальной вычислительной сети с использованием систем защиты VipNet.

- 22 Математическое моделирование действий злоумышленника с использованием сетей Петри.
- 23 Оценка угроз безопасности с использованием системы уравнений Колмогорова.
- 24 Использование эвристических оценок возможности реализации угроз безопасности.
- 25 Анализ программно-математических воздействий на информацию защищенную (далее следует наименование криптографического алгоритма).
- 26 Анализ информационной безопасности в системах массового обслуживания.
- 27 Анализ системы мониторинга радио обстановки в реальном времени с учетом зашумленности канала.
- 28 Анализ и противодействие программно-математическим воздействиям на объект информатизации с использованием системы обнаружения вторжений, honeypot, систем искусственного интеллекта, экспертных систем.
- 29 Разработка программного обеспечения автоматизированного анализа информационных систем на наличие программных и аппаратных уязвимостей.
- 30 Анализ систем автоматического дизассемблирования исходных текстов программ.
- 31 Исследование способов защиты программного кода от дизассемблирования.
- 32 Анализ информационной безопасности в условиях использования высокоскоростных каналов передачи данных (терабит).

7.4.2 Показатели и критерии оценки ВКР

Выпускная квалификационная работа оценивается членами государственной экзаменационной комиссии по четырех-балльной шкале. Оценки выставляются государственной экзаменационной комиссией по каждому показателю согласно определенным критериям и шкалой оценки (таблица 12, 13). При оценке защиты выпускной квалификационной работы учитывается умение четко и логично излагать материалы работы, отвечать на вопросы по ее содержанию, оценивать свой вклад в решение проблемы, иллюстрировать грамотность оформления работы, мнение руководителя и членов ГЭК.

Таблица 12 – Качество и уровень ВКР (*исследовательская работа*)

Показатели оценивания	Уровень сформированности компетенций / оценка и описание критериев			
	Недостаточный уровень - «неудовлетворительно»	Низкий уровень - «удовлетворительно»	Средний уровень - «хорошо»	Высокий уровень - «отлично»
Актуальность темы и ее значимость	Актуальность исследования автором не обосновывается. Неясны цели и задачи работы (либо они есть, но абсолютно не согласуются с содержанием)	Актуальность либо вообще не сформулирована, либо сформулирована не в самых общих чертах – проблема не выявлена. Не четко сформулированы цель, задачи, предмет, объект исследования, методы, используемые в работе	Автор обосновывает актуальность направления исследования в целом, а не собственной темы. Сформулированы цель, задачи, предмет, объект исследования. Тема работы сформулирована более или менее точно.	Актуальность проблемы исследования обоснована анализом состояния действительности. Сформулированы цель, задачи, предмет, объект исследования, методы, используемые в работе.

Оценка методики исследований	Использована традиционная методика исследований	Использована как традиционная методика исследований, но и апробированная	Использована как традиционная и (или) апробированная методика исследований, но и традиционная с оригинальными элементами	Использована как традиционная и (или) апробированная методика исследований, но и традиционная с оригинальными элементами и (или) принципиально новая
-------------------------------------	---	--	--	--

Оценка теоретического содержания работы	Содержание и тема работы плохо согласуются между собой.	Содержание и тема работы не всегда согласуются между собой. Некоторые части работы не связаны с целью и задачами работы. Используются известные решения	Содержание, как целой работы, так и ее частей связано с темой работы, имеются небольшие отклонения. Логика изложения присутствует – одно положение вытекает из	Содержание, как целой работы, так и ее частей связано с темой работы. Тема сформулирована конкретно, отражает направленность работы. В каждой части присутствует обоснование, использования части в рамках
--	---	---	--	--

	Уровень сформированности компетенций / оценка и описание критериев			
Показатели оценивания	Недостаточный уровень - «неудовлетворительно»	Низкий уровень - «удовлетворительно»	Средний уровень - «хорошо»	Высокий уровень - «отлично»
			другого. Используются как известные решения, так и новые теоретические модели и решения.	данной темы. Используются новые теоретические модели и решения.

Разработка мероприятий по реализации работы	Освещен набор стандартных мероприятий	Освещен набор как стандартных мероприятий, так и мероприятий с элементами углубленной проработки отдельных мероприятий	Освещена углубленная проработка отдельных мероприятий	Освещена комплексная система мероприятий
Апробация и публикация результатов работы	Апробации и публикации не было	Был сделан доклад на внутривузовской конференции и (или) осуществлена публикация во внутривузовском журнале	Был сделан доклад на региональной конференции и (или) осуществлена публикация в региональном журнале	Был сделан доклад на всероссийской и (или) международной конференции и (или) осуществлена публикация в общероссийском журнале
Внедрение	Нет	Рекомендовано ГЭК к внедрению	Принято к внедрению	Внедрено
Качество оформления	Много нарушений правил оформления и низкая культура ссылок.	Представленная ВКР имеет отклонения и не во всем соответствует предъявляемым требованиям	Есть некоторые недочеты в оформлении работы, в оформлении ссылок.	Соблюдены все правила оформления работы.

Таблица 13 – Качество и уровень ВКР (проект)

Показатели оценивания	Уровень сформированности компетенций / оценка и описание критериев			
	Недостаточный уровень - «неудовлетворительно»	Низкий уровень - «удовлетворительно»	Средний уровень - «хорошо»	Высокий уровень - «отлично»
Актуальность темы и ее практическая значимость	Актуальность исследования автором не обосновывается. Неясны цели и задачи работы (либо они есть, но абсолютно не согласуются с содержанием)	Актуальность либо вообще не сформулирована, либо сформулирована не в самых общих чертах – проблема не выявлена. Не четко сформулированы цель, задачи, предмет, объект проектирования, методы, используемые в работе.	Автор обосновывает актуальность проектирования объекта в целом, а не собственной темы. Сформулированы цель, задачи, предмет, объект проектирования. Тема работы сформулирована более или менее точно.	Актуальность проблемы проектирования объекта обоснована анализом состояния действительности. Сформулированы цель, задачи, предмет, объект проектирования, методы, используемые в работе.

Уровень проектного решения – оригинальность	Использованы известные аналоги	Использованы как известные аналоги, так и оригинальное решение отдельных элементов	Использовано оригинальное решение отдельных элементов	Использовано принципиально новое решение
Уровень расчетно - теоретического раздела проекта	Использованы известные традиционные подходы	Использованы как известные традиционные подходы, так и оригинальные решения некоторых разделов	Использованы как оригинальные решения некоторых разделов, так и новые расчетные и (или) теоретические решения	Использованы новые расчетные и теоретические решения

Уровень разработки основного раздела проекта	Использованы традиционные технологические, управленческие и т. п. решения	Использованы как традиционные технологические, управленческие и т. п. решения, так и элементы новых технологических, или в управленческих и т. п. решений	Использованы как традиционные технологические, управленческие и т. п. решения, так и элементы новых технологических, управленческих и т. п. решений	Использованы новые технологические, управленческие и т. п. решения
Уровень разработки разделов сопровождения проекта	Использованы традиционные технологические, управленческие и т. п. решения	Использованы как традиционные технологические, управленческие и т. п. решения, так и элементы новых технологических,	Использованы как традиционные технологические, , управленческие и т. п. решения, так и элементы новых технологи-	Использованы новые технологические, управленческие и т. п. решения
Показатели оценивания	Уровень сформированности компетенций / оценка и описание критериев			
	Недостаточный уровень - «неудовлетворительно»	Низкий уровень - «удовлетворительно»	Средний уровень - «хорошо»	Высокий уровень - «отлично»
		или управленческих и т. п. решений	ческих, управленческих и т. п. решений	

Апробация и публикация результатов работы	Апробации и публикации не было	Был сделан доклад на внутривузовской конференции и (или) осуществлена публикация во внутривузовском журнале	Был сделан доклад на региональной конференции и (или) осуществлена публикация в региональном журнале	Был сделан доклад на всероссийской и (или) международной конференции и (или) осуществлена публикация общероссийском журнале
Внедрение	Нет	Рекомендовано ГЭК к внедрению	Принято к внедрению	Внедрено
Качество оформления	Много нарушений правил оформления и низкая культура ссылок. Автор не может назвать и кратко изложить содержание используемых источников. Использовано менее 5 источников литературы.	Представленная ВКР имеет отклонения и не во всем соответствует предъявляемым требованиям. Автор путается в содержании используемых источников. Использовано менее 10 источников литературы.	Есть некоторые недочеты в оформлении работы, в оформлении ссылок. Автор ориентируется в содержании используемых источников. Использовано более 10 источников литературы	Соблюдены все правила оформления работы. Автор легко ориентируется в содержании используемых источников. Использовано более 20 источников литературы

Таблица 14 – Качество защиты ВКР

Показатели оценивания	Уровень сформированности компетенций / оценка и описание критериев			
	Недостаточный уровень - «неудовлетворительно»	Низкий уровень - «удовлетворительно»	Средний уровень - «хорошо»	Высокий уровень - «отлично»

Качество доклада на заседании ГЭК	Автор совсем не ориентируется в терминологии работы, защиту строит не связно, допускает существенные ошибки	Автор, в целом, владеет терминологией, но допускает неточности и ошибки при толковании основных положений и результатов работы. Защита, прошла сбивчиво, неуверенно и нечетко.	Автор достаточно уверенно владеет терминологией, защиту строит связно, но допускает незначительные неточности при ответах. Использует наглядный материал.	Автор уверенно владеет терминологией, защиту строит связно, использует наглядный материал: презентации, схемы, таблицы и др.
Правильность и аргументированность ответов на вопросы	Автор обнаруживает неумение применять полученные знания в ответах на вопросы членов ГЭК	Автор показал слабую ориентировку в тех понятиях, терминах, которые использует в своей работе, и затрудняется в ответах на вопросы членов ГЭК.	Автор достаточно уверенно владеет содержанием работы, в основном, отвечает на поставленные вопросы, но допускает незначительные неточности при ответах.	Автор уверенно показывает свою точку зрения, опираясь на соответствующие теоретические положения, грамотно и содержательно отвечает на поставленные вопросы.
Эрудиция и знания в области профессиональной деятельности	Автор обнаруживает непонимание содержательных основ в области профессиональной деятельности и неумение применять полученные знания на практике.	Автор допускает неточности и ошибки при толковании основных положений и результатов работы, не имеет собственной точки зрения на проблему исследования.	Автор достаточно уверенно осуществляет содержательный анализ теоретических источников, но допускает отдельные неточности в теоретическом обосновании или допущены отступления в практической части от законов композиционного решения.	Автор уверенно осуществляет сравнительно-сопоставительный анализ разных теоретических подходов, практическая часть ВКР выполнена качественно и на высоком уровне.
Уровень сформированности компетенций / оценка и описание критериев				

Показатели оценивания	Недостаточный уровень - «неудовлетворительно»	Низкий уровень - «удовлетворительно»	Средний уровень - «хорошо»	Высокий уровень - «отлично»
Свобода владения материалом ВКР	Автор обнаруживает непонимание материалов ВКР и проявляет неумение применять полученные материалы даже с помощью членов комиссии.	Автор, в целом, владеет содержанием работы, но при этом показал слабую ориентировку в тех понятиях, терминах, которые использует в своей работе. Практическая часть ВКР выполнена некачественно	Автор достаточно уверенно владеет содержанием материалов работы, но допускает отдельные неточности при защите ВКР. Практическая часть ВКР выполнена качественно	Автор уверенно владеет содержанием работы, показывает свою точку зрения, опираясь на соответствующие теоретические положения.

Результаты оценивания вносятся в сводный оценочный лист обучающегося (приложение 2).

Итоговая оценка за ВКР выставляется студенту на основании среднеарифметической величины по всем показателям, входящим в сводный оценочный лист обучающегося.

8 Образовательные, научно-исследовательские и научно- производственные технологии, используемые при подготовке к ГИА

Для реализации компетентностного подхода используются как традиционные формы и методы обучения, так и интерактивные формы (круглый стол, взаиморецензирование, представление и обсуждение проектных разработок), направленные на формирование у выпускников навыков коллективной работы, умения анализировать, синтезировать, готовить публикации и доклады по результатам ВКР и презентовать их.

8.1 Современные профессиональные базы данных и информационные справочные системы

Каждому обучающимся обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, с которыми у университета заключен договор:

- Электронно-библиотечная система ZNANIUM.COM.
- Электронно-библиотечная система IPRbooks.
- Образовательная платформа Юрайт.
- Электронно-библиотечная система eLIBRARY.RU (периодические издания – «Сетевая электронная библиотека технических вузов» на платформе ЭБС «Лань».
- Информационно-справочные системы «Кодекс»/ «Техэксперт».

Актуальная информация по заключенным на текущий учебный год договорам приведена на странице Научно-технической библиотеки (НТБ) на сайте университета <https://knastu.ru/page/3244>

8.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

На странице НТБ можно воспользоваться интернет-ресурсами открытого доступа по укрупненной группе направлений и специальностей (УГНС) 10.00.00 Информационная безопасность:

<https://knastu.ru/page/539>

8.3 Лицензионное и свободно распространяемое программное обеспечение

Состав программного обеспечения, необходимого при подготовке выпускной квалификационной работы, приведён на сайте университета www.knastu.ru / *Наши университет*

*/ Образование / 10.05.03 «Информационная безопасность автоматизированных систем»/
Рабочий учебный план / Реестр ПО.*

Актуальные на текущий учебный год реквизиты / условия использования программного обеспечения приведены на странице ИТ-управления на сайте университета:

<https://knastu.ru/page/1928>

Актуальные на текущий учебный год реквизиты / условия использования программного обеспечения приведены на странице ИТ-управления на сайте университета:

<https://knastu.ru/page/1928>

9 Материально-техническое обеспечение ГИА

Аудитория, в которой проводится аттестационное испытание (государственный экзамен и защита ВКР) должна быть оснащена мультимедийным оборудованием (компьютер с доступом в «Интернет», проектор, колонки).

В случае проведения процедуры ГИА с применением дистанционных образовательных технологий должно быть дополнительно обеспечено оборудование (видео-камера, микрофоны и проч.) для фиксации хода проведения аттестационного испытания.

Для подготовки к ГЭ и выполнения ВКР обучающимся предоставляются помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационнообразовательной среде университета.

10 Сведения о внесённых изменениях на текущий учебный год

Учебный год	Решение кафедры (№ протокола, дата протокола)	Внесённые изменения

Сводный оценочный лист выпускника при проведении ГЭ

Компетенции выпускника, контролируемые **опосредованно** в рамках ГЭ на основании результатов промежуточной аттестации по дисциплинам и практикам учебного плана

Код компетенции	Дисциплины / практики, участвующие в формировании компетенции	Средняя оценка промежуточной аттестации	Уровень сформированности компетенции
УК-1	<ul style="list-style-type: none"> - Философия - Введение в профессиональную деятельность - Информационные технологии - Производственная практика (научно-исследовательская работа) - Производственная практика (преддипломная практика) 		
УК-2	<ul style="list-style-type: none"> - Экономика - Правоведение - Управление инновационными проектами 		
УК-3	<ul style="list-style-type: none"> - Теория и практика успешной коммуникации // Социальнопсихологические аспекты инклюзивного образования - Управление инновационными проектами - Руководство и управление службой безопасности 		
УК-4	<ul style="list-style-type: none"> - Русский язык и культура речи - Иностранный язык 		

УК-5	<ul style="list-style-type: none"> - Философия - История (всемирная история, история России) - Культурология - Теория и практика успешной коммуникации // 		
	Социальнопсихологические аспекты инклюзивного образования		
УК-6	<ul style="list-style-type: none"> - Введение в профессиональную деятельность - Теория и практика успешной коммуникации // Социальнопсихологические аспекты инклюзивного образования 		
УК-7	<ul style="list-style-type: none"> - Физическая культура и спорт - Элективные дисциплины по физической культуре и спорту 		
УК-8	<ul style="list-style-type: none"> - Безопасность жизнедеятельности - Учебная практика 		
	(ознакомительная практика)		
УК-9	<ul style="list-style-type: none"> - Экономика 		
УК-10	<ul style="list-style-type: none"> - Правоведение 		

ОПК-3	<ul style="list-style-type: none"> - Математический анализ - Теория вероятностей и математическая статистика - Средства автоматизированных вычислений - Линейная алгебра и аналитическая геометрия - Дискретная математика - Математическая логика и теория алгоритмов 		
ОПК-16	- История (всемирная история, история России)		
	-		
Оценка			

ОПК-1, ОПК-4, ОПК-7, ОПК-8, ОПК-10, ОПК-11, ОПК-13, ОПК-7.1, ОПК-7.2, ПК-3, ПК-4
Компетенции выпускника, контролируемые в рамках ГЭ

Код компетенции	Оценка теоретической части экзамена	Оценка практической части экзамена	Уровень сформированности компетенций	Оценка ГЭ
ОПК-1, , ОПК-4, ОПК-7, ОПК-8, ОПК-10, ОПК-11, ОПК-13, ОПК-7.1, ОПК-7.2, ПК-3, ПК-4				

Итоговая оценка определяется как среднее арифметическое оценок по всем компетенциям.

Форма сводного оценочного листа выпускника при защите ВКР

Компетенции выпускника, контролируемые в рамках ВКР:

ОПК-2, ОПК-3, ОПК-5, ОПК-6, ОПК-7, ОПК-8, ОПК-9, ОПК-10, ОПК-11, ОПК-12, ОПК-13, ОПК-14, ОПК-15, ОПК-7.1, ОПК-7.2, ОПК-7.3, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6

Показатель	Оценка			
	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»
Качество и уровень ВКР				
Актуальность тематик и ее значимость				
Оценка методики исследований				
Оценка теоретического содержания работы				
Разработка мероприятий по реализации работы				
Апробация и публикация результатов работы				
Внедрение				
Качество оформления				
Качество защиты ВКР				
Качество доклада на заседании ГЭК				
Правильность и аргументированность ответов на вопросы				
Эрудиция и знания в области профессиональной деятельности				
Свобода владения материалом ВКР				
Итоговая оценка ВКР*				

* Итоговая оценка ВКР формируется как среднеарифметическая величина оценок по показателям качества и уровня ВКР, качества защиты ВКР