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)
Я.Ю. Григорьев
(подпись, ФИО)
«27» 05 20 19 г.

ПРОГРАММА
государственной итоговой аттестации (ГИА)

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Обеспечение информационной безопасности распределенных информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2019*
Форма обучения	*очная*
Технология обучения	*традиционная*

Трудоемкость, з.е.	Обеспечивающее подразделение
9	*Кафедра ИБАС – Информационная безопасность автоматизированных систем*

Комсомольск-на-Амуре 2019

Разработчик рабочей программы:

к.ф.-м.н., доцент		А.Ю. Лошманов
(должность, степень, ученое звание)	(подпись)	(ФИО)

Программа ГИА обсуждена и одобрена
на заседании кафедры «Информационная безопасность автоматизированных систем»

Протокол № 9
«06» 05 2019г

Заведующий кафедрой
ИБАС
(наименование кафедры)

	А.Ю. Лошманов
(подпись)	(ФИО)

1 Общие положения

1.1 Цель государственной итоговой аттестации

Целью государственной итоговой аттестации является установление уровня подготовки выпускника к выполнению профессиональных задач и соответствия его подготовки требованиям федерального государственного образовательного стандарта высшего образования (ФГОС ВО), утвержденного приказом Минобрнауки России от 01.12.2016 №1509, и основной профессиональной образовательной программы высшего образования (ОПОП ВО), разработанной в Комсомольском-на-Амуре государственном университете.

1.2 Состав государственной итоговой аттестации

Государственная итоговая аттестации по направлению подготовки (10.05.03) «Информационная безопасность автоматизированных систем» включает:

а) государственный экзамен;

б) защиту выпускной квалификационной работы (ВКР).

1.3 Нормативная база итоговой аттестации

1.3.1 Итоговая аттестация осуществляется в соответствии с нормативным документом. 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.

2 Характеристика выпускника

2.1 Область профессиональной деятельности выпускников включает:

Область профессиональной деятельности выпускников, освоивших программу специалитета, включает сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением информационной безопасности автоматизированных систем в условиях существования угроз в информационной сфере.

2.2 Объектами профессиональной деятельности выпускников являются:

- 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 действующие информационно-технологические ресурсы, подлежащие защите;
- технологии обеспечения информационной безопасности автоматизированных систем
- системы управления информационной безопасностью автоматизированных систем.

2.3 Виды профессиональной деятельности

Основной профессиональной образовательной программой по направлению подготовки
10.05.03"Информационная безопасность автоматизированных систем" специализация «Обеспечение информационной безопасности распределенных информационных систем»
предусматривается подготовка выпускников к следующему(им) виду (видам) профессиональной деятельности:

- научно-исследовательская;
- проектно-конструкторская;
- контрольно-аналитическая;
- организационно-управленческая;
- эксплуатационная.

2.4 Профессиональные задачи

При разработке и реализации программы специалитета организация ориентируется на все виды профессиональной деятельности, к которым готовится специалист.

Выпускник, освоивший программу специалитета, в соответствии с видом (видами) профессиональной деятельности, на который (которые) ориентирована программа специалитета, должен быть готов решать следующие профессиональные задачи (ПЗ), представленные в таблице 1.

Таблица 1 – Профессиональные задачи

Кодовое обозначение	Содержание профессиональных задач
научно-исследовательская деятельность	
ПЗ1	сбор, обработка, анализ и систематизация научно-технической информации по проблематике информационной безопасности автоматизированных систем;
ПЗ2	подготовка научно-технических отчетов, обзоров, докладов, публикаций по результатам выполненных исследований;
ПЗ3	моделирование и исследование свойств защищенных автоматизирован-

Кодовое обозначение	Содержание профессиональных задач
	ных систем;
ПЗ4	анализ защищенности информации в автоматизированных системах и безопасности реализуемых информационных технологий;
ПЗ5	разработка эффективных решений по обеспечению информационной безопасности автоматизированных систем;
проектно-конструкторская деятельность	
ПЗ6	сбор и анализ исходных данных для проектирования защищенных автоматизированных систем;
ПЗ7	разработка политик информационной безопасности автоматизированных систем;
ПЗ8	разработка защищенных автоматизированных систем в сфере профессиональной деятельности, обоснование выбора способов и средств защиты информационно-технологических ресурсов автоматизированных систем;
ПЗ9	выполнение проектов по созданию программ, комплексов программ, программно-аппаратных средств, баз данных, компьютерных сетей для защищенных автоматизированных систем;
ПЗ10	разработка систем управления информационной безопасностью автоматизированных систем;
контрольно-аналитическая	
ПЗ11	контроль работоспособности и эффективности применяемых средств защиты информации;
ПЗ12	выполнение экспериментально-исследовательских работ при сертификации средств защиты информации и аттестации автоматизированных систем;
ПЗ13	проведение инструментального мониторинга защищенности автоматизированных систем и анализа его результатов;
организационно-управленческая деятельность	
ПЗ14	организация работы коллектива, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ;
ПЗ15	организационно-методическое обеспечение информационной безопасности автоматизированных систем;
ПЗ16	организация работ по созданию, внедрению, эксплуатации и сопровождению защищенных автоматизированных систем;
ПЗ17	контроль реализации политики информационной безопасности;
эксплуатационная деятельность	
ПЗ18	реализация информационных технологий в сфере профессиональной деятельности с использованием защищенных автоматизированных систем;
ПЗ19	администрирование подсистем информационной безопасности автоматизированных систем;
ПЗ20	мониторинг информационной безопасности автоматизированных систем; управление информационной безопасностью автоматизированных систем;
ПЗ21	обеспечение восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций;
в соответствии со специализациями "Обеспечение информационной безопасности распределенных информационных систем"	

Кодовое обозначение	Содержание профессиональных задач
П322	разработка и исследование моделей информационно-технологических ресурсов, модели угроз и модели нарушителей информационной безопасности в распределенных информационных системах;
П323	удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах;
П324	аудит защищенности информационно-технологических ресурсов;
П325	координация деятельности подразделений и специалистов по защите информации в организациях, в том числе на предприятиях и в учреждениях;

3 Результаты освоения образовательной программы

В результате освоения образовательной программы у выпускника должны быть сформированы компетенции:

Общекультурные компетенции

способностью использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1);

способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2);

способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3);

способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);

способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);

способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);

способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7);

способностью к самоорганизации и самообразованию (ОК-8);

способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9).

общепрофессиональными компетенциями:

способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач (ОПК-1);

способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники (ОПК-2);

способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3);

способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах (ОПК-4);

способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-5);

способностью применять нормативные правовые акты в профессиональной деятельности (ОПК-6);

способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-7);

способностью к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8).

Профессиональные компетенции по видам деятельности:

научно-исследовательская деятельность

способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке (ПК-1);

способностью создавать и исследовать модели автоматизированных систем (ПК-2);

способностью проводить анализ защищенности автоматизированных систем (ПК-3);

способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);

способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);

способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);

способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);

проектно-конструкторская деятельность:

способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);

способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);

способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-10);

способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);

способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);

способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13);

контрольно-аналитическая деятельность:

способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);

способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15);

способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16);

способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);

организационно-управленческая деятельность:

способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18);

способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);

способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);

способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);

способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);

способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);

эксплуатационная деятельность:

способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);

способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);

способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26);

способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);

способностью управлять информационной безопасностью автоматизированной системы (ПК-28).

в соответствии со специализацией:

специализация N 7 "Обеспечение информационной безопасности распределенных информационных систем":

способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах (ПСК-7.1);

способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах (ПСК-7.2);

способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем (ПСК-7.3);

способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах (ПСК-7.4);

способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении (ПСК-7.5);

4 Объем, структура и содержание государственной итоговой аттестации

Элемент ГИА	Содержание контролируемых результатов	Форма проведения	Трудоемкость (в часах)
Государственный экзамен			
Тест по проверке сформированности ОК	Общекультурные компетенции (ОК1, ОК2, ОК3, ОК4, ОК5, ОК6, ОК8, ОК9)	Компьютерное тестирование	36
Вопросы и практические задания государственного экзамена	ОПК-3, ОПК-4, ПК-2, ПК-10, ПК-11, ПК-13, ПК-14, ПК-15, ПК-17, ПК-19, ПК-20, ПК-21, ПК-24, ПК-28, ПСК-7.2	Подготовка ответа на теоретические вопросы, выполнение практического задания	72
Подготовка и защита выпускной квалификационной работы			
Выпускная квалификационная работа	ОПК-1, ОПК-2, ОПК-5, ОПК-5, ОПК-7, ОПК-8, ПК-1, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-12, ПК-16, ПК-18, ПК-22, ПК-23, ПК-25, ПК-27, ПСК-7.1, ПСК-7.3, ПСК-7.4, ПСК-7.5	Защита выпускной квалификационной работы	216
Итого	-	-	**324**

5 Фонд оценочных средств для проведения ГИА

Таблица 3 – Паспорт фонда оценочных средств

Код контролируемой компетенции	Контролируемые результаты (знания, умения, навыки)	Наименование оценочного средства*	Показатели оценки
ОК-1: способность использовать основы философских знаний для формирования мировоззренческой позиции	З(ОК-1) основных принципов, законов и категории философии в их логической целостности и последовательности; У(ОК-1) воспринимать и анализировать мировоззренческие, социально и личностно значимые философские проблемы; Н(ОК-1) навыками выражения и обоснования собственной мировоззренческой позиции.	Тест по проверке сформированности ОК	Количество правильно выполненных заданий теста
ОК-2: способность анализировать основные этапы и закономерности исторического развития общества для формирования гражданской позиции	З(ОК-2) основных политических и социально-экономических направлений, этапов и закономерностей исторического развития общества и современного положения России в мире; У(ОК-2) анализировать, высказывать и обосновывать свою гражданскую позицию по вопросам исторического и социально-политического развития общества; Н(ОК-2) способами оценивания исторического опыта и навыками научной аргументации при отстаивании собственной позиции по вопросам истории.	Тест по проверке сформированности ОК	Количество правильно выполненных заданий теста
ОК-3: способность использовать основы экономических знаний в различных сферах деятельности	З(ОК-3) теорий и концепций, историю эволюции экономической теории; У(ОК-3) проблемы и закономерности функционирования институтов современной экономики на макро- и микроуровне; Н(ОК-3) навыком применения институционального анализа при диагностике развития социально-экономических систем.	Тест по проверке сформированности ОК	Количество правильно выполненных заданий теста
ОК-4: способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия	З(ОК-4) основ лексики и грамматики иностранного языка, формы межличностного и межкультурного общения; терминологии предметной области на английском языке; У(ОК-4) применять нормы деловой культуры, русского и иностранного языка для устного и письменного общения; Н(ОК-4) устной и письменной иностранной речью на уровне необходи-	Тест по проверке сформированности ОК	Количество правильно выполненных заданий теста

Код контролируемой компетенции	Контролируемые результаты (знания, умения, навыки)	Наименование оценочного средства*	Показатели оценки
	мом и достаточном для решения коммуникативных задач в профессиональной деятельности.		
ОК-5: способность работать в коллективе, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия	З(ОК-5) психологии личности и межличностного общения; этические нормы и психологические особенности работы в коллективе; У(ОК-5) анализировать собственное поведение и поведение окружающих; выбирать оптимальный стиль взаимодействия; Н(ОК-5) обеспечивать бесконфликтные межличностные взаимоотношения в соответствии с этнокультурными особенностями делового общения; навыками делового общения и публичных выступлений, ведения переговоров и совещаний, проведения бизнес-презентаций.	Тест по проверке сформированности ОК	Количество правильно выполненных заданий теста
ОК-6: способность использовать основы правовых знаний в различных сферах деятельности	З(ОК-6) особенностей конституционного строя, правового положения граждан, основные положения отраслевых юридических и специальных наук; У(ОК-6) анализировать, толковать и правильно применять правовые нормы; Н(ОК-6) навыками анализа различных правовых явлений, юридических фактов, правовых норм и правовых отношений.	Тест по проверке сформированности ОК	Количество правильно выполненных заданий теста
ОК-7: способность к самоорганизации и самообразованию	З(ОК-7) основ самоменеджмента, самоорганизации, мотивации для эффективной профессиональной деятельности; У(ОК-7) самостоятельно организовывать свое личное время; Н(ОК-7) навыками планирования своей деятельности и формирования образовательной траектории, самостоятельной творческой работы, самоорганизации.	Тест по проверке сформированности ОК	Количество правильно выполненных заданий теста
ОК-8: способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности	З(ОК-8) научно-практических основ физической культуры, основ здорового образа жизни; У(ОК-8) самостоятельно выбирать и применять способы и средства для поддержания здоровья и работоспособности в социальной и профессиональной деятельности; Н(ОК-8) методами физического воспитания, средствами укрепления здоровья и способами поддержания хорошей	Тест по проверке сформированности ОК	Количество правильно выполненных заданий теста

Код контролируемой компетенции	Контролируемые результаты (знания, умения, навыки)	Наименование оценочного средства*	Показатели оценки
	физической формы для обеспечения полноценной социальной и профессиональной деятельности.		
ОК-9: способность использовать приемы первой помощи, методы защиты в условиях чрезвычайных ситуаций	З(ОК-9) основных факторов негативного воздействия человека на окружающую среду и методы обеспечения экологической безопасности; У(ОК-9) оценивать степень опасности возможных последствий аварий, катастроф и стихийных бедствий для производственного персонала и населения, оказывать первую помощь пострадавшим; Н(ОК-9) навыками использования приемов оказания первой помощи, защиты производственного персонала и населения от возможных последствий аварий, катастроф и стихийных бедствий.	Тест по проверке сформированности ОК	Количество правильно выполненных заданий теста
ОПК-1: способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач	З(ОПК-1) основных физических явлений, каналов утечки информации У(ОПК-1) оценивать необходимость применения соответствующего математического аппарата для формализации решения профессиональных задач Н(ОПК-1) применения математического аппарата при формализации решении профессиональных задач	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5
ОПК-2: способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использо-	З(ОПК-2) основных приемов корректного применения математического аппарата при решении профессиональных задач У(ОПК-2) корректно применять при решении профессиональных задач соответствующий математический аппарат Н(ОПК-2) использования математического аппарата для решения профессиональных задач	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5

Код контролируемой компетенции	Контролируемые результаты (знания, умения, навыки)	Наименование оценочного средства*	Показатели оценки
ванием вычислительной техники			
ОПК-3: способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности ОПК-4: способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах	З(ОПК-3) в области использования современных языков и систем программирования У(ОПК-3) разрабатывать оконные приложения в Windows Н(ОПК-3) разработки приложений с использованием WinAPI З(ОПК-4) основных подходов к поиску информации в компьютерных системах, сетях, библиотечных фондах У(ОПК-4) использовать ЭВМ для поиска информации в компьютерных системах, сетях, библиотечных фонда Н(ОПК-4) поиска информации в компьютерных системах, сетях, библиотечных фондах	теоретический вопрос билета к государственному экзамену, задача билета к государственному экзамену	см. п. 6.4
ОПК-5: способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	З(ОПК-5) основных методов проведения научных исследований У(ОПК-5) применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами Н(ОПК-5) применения научных методов в профессиональной деятельности	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5
ОПК-6: способностью применять нормативные правовые акты в профессиональной деятельности	З(ОПК-6) основных нормативных актов в области информационной безопасности У(ОПК-6) применять на практике основные нормативные акты Н(ОПК-6) использования нормативных актов в профессиональной деятельности.	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5

Код контролируемой компетенции	Контролируемые результаты (знания, умения, навыки)	Наименование оценочного средства*	Показатели оценки
ОПК-7: способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций	З(ОПК-7) основ защиты производственного персонала в условиях чрезвычайных ситуаций У(ОПК-7) использовать средства для обеспечения отказоустойчивости работы автоматизированных систем Н(ОПК-7) в области обеспечения отказоустойчивости работы автоматизированных систем	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5
ОПК-8: способностью к освоению новых образцов программных, технических средств и информационных технологий	З(ОПК-8) основных тенденций в развитии программных и технических средств, информационных технологий У(ОПК-8) осваивать новые образцы программных, технических средств и информационных технологий Н(ОПК-8) поиска информации о новых программных, технических средствах, информационных технологиях	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5
ПК-1: способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	З(ПК-1) методов поиска, изучения систематизации и обобщения информации на иностранном языке У(ПК-1) осуществлять поиск, изучение, обобщение и систематизацию информации на иностранном языке Н(ПК-1) работы с научно-технической информацией, нормативными и методическими материалами в сфере профессиональной деятельности на иностранном языке	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5
ПК-2: способностью создавать и исследовать модели автоматизированных систем	З(ПК-2) нормативно-методических документов по классификации автоматизированных систем У(ПК-2) создавать и исследовать модели автоматизированных систем Н(ПК-2) классификации и разработки документации для автоматизированных систем в сфере профессиональной деятельности	теоретический вопрос билета к государственному экзамену, практическое задание билета к государственному экзамену	см. п. 6.4
ПК-3: способностью проводить анализ защищенности автоматизированных систем	З(ПК-3) методов проведения анализа защищенности распределенных информационных систем У(ПК-3) строить план анализа защищенности распределенных информационных систем	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5

Код контролируемой компетенции	Контролируемые результаты (знания, умения, навыки)	Наименование оценочного средства*	Показатели оценки
	Н(ПК-3) проведения анализа защищенности распределенных информационных систем		
ПК-4: способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	З(ПК-4) основных моделей угроз и модели нарушителя информационной безопасности У(ПК-4) разрабатывать модели угроз и модель нарушителя информационной безопасности распределенных информационных систем Н(ПК-4) анализа моделей угроз и модели нарушителя информационной безопасности распределенных информационных систем	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5
ПК-5: способностью проводить анализ рисков информационной безопасности автоматизированной системы	З(ПК-5) методов и способов анализа риской информационной безопасности автоматизированных систем У(ПК-5) проводить анализ рисков информационной безопасности автоматизированных систем Н(ПК-5) расчета интегральных показателей для рисков и выделения основных направлений снижения рисков.	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5
ПК-6: способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	З(ПК-6) механизмов функционирования автоматизированных систем и основных технологий обработки информации У(ПК-6) проводить анализ выбора решений по обеспечению эффективного применения автоматизированных систем Н(ПК-6) обоснования выбора решений по обеспечению эффективного применения автоматизированных систем	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5
ПК-7: способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	З(ПК-7) принципов формирования научно-технической документации У(ПК-7) проводить поиск информации для разработки научно-технической документации, научно-технических отчетов, обзоров, публикаций Н(ПК-7) разработки научно-технической документации, научно-технических отчетов, обзоров, публикаций	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5

Код контролируемой компетенции	Контролируемые результаты (знания, умения, навыки)	Наименование оценочного средства*	Показатели оценки
ПК-8: способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	З(ПК-8) основ проектирования систем информационной безопасности автоматизированных систем У(ПК-8) разрабатывать проектные решения по обеспечению информационной безопасности автоматизированных систем Н(ПК-8) анализа проектных решений по обеспечению информационной безопасности автоматизированных систем.	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5
ПК-9: способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	З(ПК-9) основ построения защищенных автоматизированных систем У(ПК-9) участвовать в разработке автоматизированных систем Н(ПК-9) формирования документации на автоматизированную систему в защищенном исполнении	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5
ПК-10: способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности	З(ПК-10) в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем У(ПК-10) применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем при решении профессиональных задач Н(ПК-10) использования аппарата электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем при решении профессиональных задач	теоретический вопрос билета к государственному экзамену, задача билета к государственному экзамену	см. п. 6.4
ПК-11: способностью разрабатывать политику информационной безопасности автоматизированной системы	З(ПК-11) основных компонентов политики информационной безопасности автоматизированных систем У(ПК-11) проводить анализ и формировать сведения для разработки политики информационной безопасности автоматизированных систем	теоретический вопрос билета к государственному экзамену, практическое задание билета к государственному	см. п. 6.4

Код контролируемой компетенции	Контролируемые результаты (знания, умения, навыки)	Наименование оценочного средства*	Показатели оценки
	Н(ПК-11) разработки политики информационной безопасности автоматизированной системы.	экзамену	
ПК-12: способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	З(ПК-12) основ проектирования системы управления информационной безопасности автоматизированных систем У(ПК-12) проектировать систему управления информационной безопасности автоматизированных систем Н(ПК-12) использования средств проектирования системы управления информационной безопасности автоматизированных систем	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5
ПК-13: способностью участвовать в проектировании средств защиты информации автоматизированной системы	З(ПК-13) основ проектирования средств защиты информации автоматизированных систем У(ПК-13) проектировать средства защиты информации автоматизированных систем Н(ПК-13) использования средств проектирования средств защиты информации автоматизированных систем	теоретический вопрос билета к государственному экзамену, практическое задание билета к государственному экзамену	см. п. 6.4
ПК-14: способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	З(ПК-14) основных программно-аппаратных, криптографических и технических средств защиты информации применяемых в автоматизированных системах У(ПК-14) проводить контрольные проверки средств защиты информации Н(ПК-14) построения плана и отчета по результатам контрольных проверок работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации в автоматизированных системах	теоретический вопрос билета к государственному экзамену, практическое задание билета к государственному экзамену	см. п. 6.4
ПК-15: способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	З(ПК-15) основ сертификации средств защиты информации автоматизированных систем У(ПК-15) участвовать в проведении работ при сертификации средств защиты информации автоматизированных систем Н(ПК-15) проведения экспериментально-исследовательских работ при проведении сертификации средств защиты информации автоматизированных си-	теоретический вопрос билета к государственному экзамену, практическое задание билета к государственному экзамену	см. п. 6.4

Код контролируемой компетенции	Контролируемые результаты (знания, умения, навыки)	Наименование оценочного средства*	Показатели оценки
	стем		
ПК-16: способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации	З(ПК-16) основ проведения аттестации автоматизированных систем на соответствие требованиям по защите информации У(ПК-16) участвовать при проведении работ по аттестации автоматизированных систем на соответствие требованиям по защите информации Н(ПК-16) проведения экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом требований нормативных документов по защите информации	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5
ПК-17: способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	З(ПК-17) основ мониторинга защищенности информации в автоматизированных системах У(ПК-17) проводить инструментальный мониторинг защищенности информации в автоматизированных системах Н(ПК-17) выявления каналов утечки информации в автоматизированных системах	теоретический вопрос билета к государственному экзамену, практическое задание билета к государственному экзамену	см. п. 6.4
ПК-18: способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности	З(ПК-18) основ организации работы малых коллективов исполнителей У(ПК-18) вырабатывать управленческие решения в сфере профессиональной деятельности Н(ПК-18) реализации управленческих решений в сфере профессиональной деятельности	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5
ПК-19: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	З(ПК-19) основных тенденций по совершенствованию системы управления информационной безопасностью автоматизированных систем У(ПК-19) исследовать систему управления информационной безопасностью автоматизированных систем Н(ПК-19) выработки предложений по совершенствованию системы управления информационной безопасностью автоматизированных систем	теоретический вопрос билета к государственному экзамену, практическое задание билета к государственному экзамену	см. п. 6.4
ПК-20: способностью организовать разработку, внед-	З(ПК-20) основных документов на автоматизированные систем функционирующие с учетом требований по ин-	теоретический вопрос билета к государственному	см. п. 6.4

Код контролируемой компетенции	Контролируемые результаты (знания, умения, навыки)	Наименование оценочного средства*	Показатели оценки
рение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	формационной безопасности У(ПК-20) разрабатывать и внедрять автоматизированные системы с учетом требований по информационной безопасности Н(ПК-20) эксплуатации и сопровождения автоматизированной системы с учетом требований по информационной безопасности	экзамену, практическое задание билета к государственному экзамену	
ПК-21: способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	З(ПК-21) основных необходимых документов регламентирующих работу по обеспечению информационной безопасности автоматизированных систем У(ПК-21) разрабатывать документы регламентирующие работу по обеспечению информационной безопасности Н(ПК-21) анализа документации, регламентирующей работу по обеспечению информационной безопасности	теоретический вопрос билета к государственному экзамену, практическое задание билета к государственному экзамену	см. п. 6.4
ПК-22: способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	З(ПК-22) составляющих политики информационной безопасности организации У(ПК-22) формировать предложения по усилению эффективности реализации политики информационной безопасности организации Н(ПК-22) контроля эффективности реализации политики информационной безопасности организации	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5
ПК-23: способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	З(ПК-23) основных нормативно-методических документов по защите информации ограниченного доступа. У(ПК-23) вырабатывать правила, процедуры и методы по защите информации ограниченного доступа Н(ПК-23) формирования комплекса мер для защиты информации ограниченного доступа	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5
ПК-24: способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом	З(ПК-24) эффективных способов применения информационно-технологических ресурсов автоматизированных систем У(ПК-24) обеспечить эффективное применение информационно-технологических ресурсов автоматизированных систем Н(ПК-24) использования средств обес-	теоретический вопрос билета к государственному экзамену, практическое задание билета к государственному экзамену	см. п. 6.4

Код контролируемой компетенции	Контролируемые результаты (знания, умения, навыки)	Наименование оценочного средства*	Показатели оценки
требований информационной безопасности	печения эффективного применения информационно-технологических ресурсов автоматизированных систем		
ПК-25: способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	З(ПК-25) основных технологических ресурсов автоматизированных систем У(ПК-25) эффективно применять средства защиты информационно-технологических ресурсов автоматизированной системы Н(ПК-25) восстановления работоспособности при возникновении нештатных ситуаций	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5
ПК-26: способностью администрировать подсистему информационной безопасности автоматизированной системы	З(ПК-26) основных компонентов подсистемы информационной безопасности автоматизированных систем У(ПК-26) администрировать подсистему информационной безопасности автоматизированных систем Н(ПК-26) использования средств администрирования подсистемы информационной безопасности автоматизированных систем	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5
ПК-27: способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	З(ПК-27) частных политик информационной безопасности автоматизированных систем У(ПК-27) вырабатывать частную политику информационной безопасности автоматизированной системы Н(ПК-27) осуществления мониторинга и аудита информационной безопасности автоматизированных систем	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5
ПК-28: способностью управлять информационной безопасностью автоматизированной системы	З(ПК-28) основ управления информационной безопасностью автоматизированных систем У(ПК-28) управлять процессами обеспечения информационной безопасности автоматизированных систем	теоретический вопрос билета к государственному экзамену, практическое задание билета к	см. п. 6.4

Код контролируемой компетенции	Контролируемые результаты (знания, умения, навыки)	Наименование оценочного средства*	Показатели оценки
	Н(ПК-28) формирования процессов управления информационной безопасности автоматизированных систем	государственному экзамену	
ПСК-7.1: способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах	З(ПСК-7.1) базовых моделей угроз безопасности и моделей нарушителя У(ПСК-7.1) разрабатывать модели угроз и модель нарушителя информационной безопасности в распределенных информационных системах Н(ПСК-7.1) формирования исходных данных для модели угроз и нарушителя	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5
ПСК-7.2: способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах	З(ПСК-7.2) основных этапов реализации рисков и подходов к оценке рисков информационной безопасности в распределенных информационных системах У(ПСК-7.2) выделять в распределенной информационной системе основные и дополнительные риски Н(ПСК-7.2) формирования плана и проекта по снижению рисков в распределенной информационной системе	теоретический вопрос билета к государственному экзамену, практическое задание билета к государственному экзамену	см. п. 6.4
ПСК-7.3: способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем	З(ПСК-7.3) основных информационно-технологических ресурсов распределенных информационных систем У(ПСК-7.3) проводить аудит информационно-технологических ресурсов Н(ПСК-7.3) формирования плана и отчета о проведении аудита защищенности информационно-технологических ресурсов распределенных информационных систем	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5
ПСК-7.4: способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах	З(ПСК-7.4) основных приемов удаленного администрирования операционных систем и баз данных У(ПСК-7.4) проводить удаленное администрирование операционных систем и баз данных Н(ПСК-7.4) использования инструментальных средств для проведения удаленного администрирования операци-	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5

Код контролируемой компетенции	Контролируемые результаты (знания, умения, навыки)	Наименование оценочного средства*	Показатели оценки
	онных систем и баз данных в распределенных информационных системах		
ПСК-7.5: способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении	З(ПСК-7.5) методов и способов управления подразделениями и специалистами по защите информации У(ПСК-7.5) координировать деятельность подразделений и специалистов по защите информации Н(ПСК-7.5) проведения координационных мероприятий подразделений и специалистов по защите информации	Доклад на защите ВКР, ответы на вопросы на защите ВКР	ст. п. 7.5

6 Программа государственного экзамена и рекомендации обучающимся по подготовке к нему

6.1 Тест по проверке сформированности общекультурных компетенций

Элементом государственного экзамена является тест по проверке сформированности общекультурных компетенций. Проверка общекультурных компетенций проводится в форме тестирования. Тест содержит 20 вопросов. На выполнение теста отводится не более 45 минут.

Максимальное количество баллов – 20. За каждый верный ответ обучающийся получает 1 балл, за неверный – 0 баллов.

Оценка «зачтено» ставится при условии выполнения более 60 % заданий. В случае получения оценки «не зачтено» выставляется неудовлетворительная оценка за государственный экзамен.

Открытый банк тестовых заданий представлен в разделе УМКД в личном кабинете студента.

6.2 Форма проведения государственного экзамена

Письменный или устный экзамен

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

Билет по проверке общепрофессиональных профессиональных и профессионально-специализированных 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:

- Комплексное обеспечение информационной безопасности автоматизированных систем
- Основы информационной безопасности
- Языки программирования
- Информатика
- Техническая защита информации
- Программно-аппаратные средства обеспечения информационной безопасности
- Безопасность операционных систем.

Перечень вопросов и типовых практических заданий (задач) представлены таблице 4 и таблице 5 соответственно.

Таблица 4 – Перечень вопросов к государственному экзамену

№ вопроса	Содержание вопроса	Рекомендуемая литература *
Комплексное обеспечение информационной безопасности автоматизированных систем		
1	Методы и оборудование физической информационной безопасности. Службы информационной безопасности организации.	1. Челухин, В.А. Комплексное обеспечение информационной безопасности автоматизированных систем: Учебное пособие для вузов / В. А. Челухин. - Комсомольск-на-Амуре: Изд-во Комсомольского-на-Амуре гос.техн.ун-та, 2021. - 207с. - Библиогр.: с.201-207. 2. Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие для вузов / П. Б. Хорев. - М.: Форум, 2020. - 351с.: ил. - чз-1экз аб-4экз. 3. Грибунин, В.Г. Комплексная система защиты информации на предприятии: учебное пособие для вузов / В. Г. Грибунин, В. В. Чудовский. - М.: Академия, 2019. - 412с. - (Высшее профессиональное образование). 4. Мельников, В.П. Информационная безопасность и защита информации: учебное пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков; Под ред. С.А.Клейменова. - 4-е изд., стер., 2-е изд., стер. - М.: Академия, 2009; 2007; 2018. - 331с.
2	Что понимается под комплексной системой информационной безопасности. Рассмотреть на примере любой организации.	
3	Аттестация объектов информатизации. С учетом нормативно-технических документов по безопасности информации, утвержденных ФСТЭК (Гостехкомиссией) России	
4	Системы обнаружения уязвимостей сетей и анализаторы сетевых атак	
5	Классификация автоматизированных систем по информационной безопасности.	
6	Этапы развития информационной безопасности, перспективы развития, Технологии будущего.	
7	Системный подход к организации информационной безопасности предприятия. Организационные меры информационной безопасности.	
8	Уровни защиты информации. Раскрыть сущность каждого уровня	
9	Что понимается под комплексной системой информационной безопасности. Рассмотреть на примере любой организации.	
10	В чем суть системного подхода к организации информационной безопасности. Основные меры организационного уровня организации информационной безопасности	
Основы информационной безопасности		

1	Этапы развития информационной безопасности, перспективы развития, Технологии будущего.	1. Смоленский, М. Б. Информационное право : учебник для вузов / М. Б. Смоленский, М. В. Алексеева. – Ростов н/Д : Феникс, 2019. – 223 с. 2. Челухин, В. А. Комплексное обеспечение информационной безопасности автоматизированных систем : учебное пособие для вузов / В. А. Челухин. – Комсомольск-на-Амуре : Изд-во Комсомольского-на-Амуре гос. техн. ун-та, 2021. – 207 с. 3. Схиртладзе, А. Г. Интегрированные системы проектирования и управления : учебник для вузов / А. Г. Схиртладзе, Т. Я. Лазарева, Ю. Ф. Мартемьянов. – М.: Академия, 2018. – 348 с. 4. Баранова, Е. К. Информационная безопасность и защита информации [Электронный ресурс]: учеб. пособие / Е. К. Баранова, А. В. Бабаш. – 3-е изд., перераб. и доп. – М. : РИОР: ИНФРА – М, 2017. – 322 с. // ZNANIUM.COM. : электронно-библиотечная система. – Режим доступа: http:/www.znanium.com/catalog.php?, ограниченный. – Загл. с экрана. 5. Башлы, Н. П. Информационная безопасность и защита информации [Электронный ресурс] : учебник / Н. П. Башлы, А. В. Бабаш, Е. К. Баранова. – М. : РИОР, 2017. – 222 с. // ZNANIUM.COM. : электронно-библиотечная система. – Режим доступа: http:/www.znanium.com/catalog.php?, ограниченный. – Загл. с экрана. 6. Гришина, Н. В. Информационная безопасность предприятия [Электронный ресурс]: учеб. пособие / Н. В. Гришина. – 2-е изд., доп. –М. : ФОРУМ : ИНФРА-М, 2017. – 239 с. // ZNANIUM.COM. : электронно-библиотечная система. – Режим доступа: http:/www.znanium.com/catalog.php?, ограниченный. – Загл. с экрана.
2	Методы и оборудование физической информационной безопасности. Службы информационной безопасности организации.	
3	Системы обнаружения уязвимостей сетей и анализаторы сетевых атак.	
4	Международные законы и соглашения по информационной безопасности	
5	Программные методы защиты информации. Вирусная защита информации.	
6	Программная защита информации разработчика, особенности.	
7	Вирусы – классификация, стратегия распространения.	
8	Поясните, что такое «Политика информационной безопасности предприятия» и приведите основные пункты её.	
9	Поясните значение и суть руководящих документов ВСТЭК. Привести пример	
10	Какие меры организационного характера необходимо принять руководителю предприятия для обеспечения защиты информации?	
Языки программирования		
1	Отличие ООП от модульного программирования.	1. Немцова, Т. И. Программирование на языке С++ [Электронный ресурс]: учеб. пособие / Т.И. Немцова, С.Ю. Голова, А.И. Терентьев; Под ред. Л.Г. Гагариной. - М.: ИД ФОРУМ: ИНФРА-М, 2018. - 512 с. // ZNANIUM.COM : электронно-библиотечная система. – Режим
2	Отличия структуры С++ и класса С++.	
3	Понятие абстракции и примеры ее реализации в алгоритмических языках.	

		доступа: http://znanium.com/catalog.php#, ограниченный. – Загл. с экрана. 2.Кузин, А. В. Программирование на языке Си [Электронный ресурс] /А.В.Кузин, Е.В.Чумакова - М. : Форум, НИЦ ИНФРА-М, 2019. - 144 с. // ZNANIUM.COM : электронно-библиотечная система. – Режим доступа: http://znanium.com/catalog.php#, ограниченный. – Загл. с экрана. 3.Новиков, Ф.А. Дискретная математика для программистов: Учебное пособие для вузов / Ф. А. Новиков. - 2-е изд. - СПб.: Питер, 2004; 2003; 2001; 2000; 2020- 363с 4.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, 2021 - 496с.: ил. // ZNANIUM.COM : электронно-библиотечная система.- Режим доступа: http://znanium.com/catalog/product/472870, ограниченный. – Загл. с экрана
4	Понятие инкапсуляции и ее реализация в ООП.	
5	Уровни доступа класса.	
6	Объявление указателей на массивы. Доступ к элементам массивов (одномерных и многомерных) через указатели. Примеры.	
7	Регистры микропроцессора и их назначение. Вычисление полного адреса памяти.	
8	Понятие списка. Несвязанные и связанные списки.	
9	Указатель на функцию. Объявление указателя на функцию. Примеры.	
10	Модификация параметров операционной системы через указатели.	
Информатика		
1	Что такое информационная безопасность и что входит в её функции	. Серебренникова А.Г. Информатика [Электронный ресурс] : / А.Г. Серебренникова, А. С. Верещагина, Е. Г. Кравченко, Д. Н. Кузнецов. – Комсомольск-на-Амуре: ФГБОУ ВПО «КнАГТУ», 2014. – 174 с. // Виртуальная библиотека ИНИТ. – Режим доступа: http://initkms.ru/ library/readbook/1101570/1, свобод-ный. – Загл. с экрана. 2. Каймин В.А . Информатика [Электронный ресурс]: учебник / В.А. Каймин - 6-е изд. - М.: ИНФРА-М, 2021. - 285 с.: // ZNANIUM.COM : электронно-библиотечная систе-ма. – Режим доступа: http://www. znanium.com/catalog.php, ограниченный. – Загл. с экрана. 3. Сергеева И.И. Информатика [Электронный ресурс] : учебник / И.И. Сергеева, А.А. Музолевская, Н.В. Тарасова. – М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2019. – 384 с. // ZNANIUM.COM : электронно-библиотечная система. – Режим
2	Какие организации могут быть привлечены к проведению работ на предприятии по защите информации?	
3	Назначение и эксплуатация устройств бесперебойного питания.	
4	Биометрические системы контроля доступа.	
5	Программная защита информации пользователя	
6	Организация управления оперативной памятью в защищенном режиме работы процессора IBM PC.	
7	Технология сообщений в ОС Windows. Типы сообщений, системные функции обработки сообщений. Стандартные шаблоны программных	

	модулей обработки сообщений в ОС Windows.	доступа: http://www. znanium.com/catalog.php, ограниченный. – Загл. с экрана.
8	Структуры данных. Стек. Применение стека для вычисления арифметических выражений. Очередь и дек.	4. Гуриков С.Р. . Информатика [Электронный ресурс]: учебник / С.Р. Гуриков. - М.: Форум: НИЦ ИНФРА-М, 2018. - 464 с.: // ZNANIUM.COM : электронно-библиотечная си-стема. – Режим доступа: http://www. znanium.com/catalog.php, ограниченный. – Загл. с экрана
9	Реализация алгоритма перебора с помощью рекурсивной подпрограммы.	5. Кузин, А.В. Компьютерные сети: Учебное пособие / А.В. Кузин. - 3-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2017. - 192 с.: ил.; Режим доступа: http://znanium.com/catalog/product/450375
10	Деревья упорядоченные и неупорядоченные.	6. Исаченко, О.В. Программное обеспечение компьютерных сетей: Учебное пособие / О.В. Исаченко. - М.: ИНФРА-М, 2019. - 117 с.: Режим доступа: http://znanium.com/catalog/product/232661
		7. 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, 2008. – 155 с. // Виртуальная библиотека ИНИТ. – Режим доступа: http://www.initkms.ru/library/readbook/1101388/1, свободный. – загл.с экрана
		8. Демидович, Б.П. Основы вычислительной математики. Учебное пособие для втузов / Б.П. Демидович, И.А. Марон. — М.: 1963. — 660 с.: ил.
Техническая защита информации		
1	Электроакустические каналы утечки информации	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, 2020. - 442с.//ZNANIUM.COM : электронная библиотечная система- Режим доступа: http://znanium.com/catalog/product/390284, ограниченный. – Загл. с экрана
2	Оптико-электронный технический канал утечки информации.	
3	Параметрические каналы утечки информации	
4	Технические каналы утечки информации, обрабатываемой ТСПИ и передаваемой по каналам связи.	2.Технические средства и методы за-

		щиты информации [Электронный ресурс]/ Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. - М.:Гор. линия-Телеком, 2021. - 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", 2019. - 214 с.//ZNANIUM.COM : электронная библиотечная система- Режим доступа: http://znanium.com/catalog/product/950073, ограниченный. – Загл. с экрана 4.Баранова, Е. К. Основы информатики и защиты информации [Электронный ресурс] : Учеб. пособие / Е. К. Баранова. - М. : РИОР : ИНФРА-М, 2018. - 183 с.//ZNANIUM.COM : электронная библиотечная система- Режим доступа: http://znanium.com/catalog/product/415501, ограниченный. – Загл. с экрана 5.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, 2017. - 392 с.//ZNANIUM.COM : электронная библиотечная система- Режим доступа: http://znanium.com/catalog/product/474838, ограниченный. – Загл. с экрана
5	Электрические каналы утечки информации: наводки электромагнитных излучений ТСПИ, просачивание информационных сигналов в цепи электропитания, просачивание информационных сигналов в цепи заземления, съем информации по электрическим каналам утечки информации	
6	Оптико-электронный технический канал утечки информации	
7	Демаскирующие признаки радиоэлектронных средств, демаскирующие признаки акустических закладок.	
8	Средства радио и радиотехнической разведки: сканирующие компьютерные радиоприемники, радиопеленгаторы, анализаторы спектра, радиочастотметры	
9	Технические средства радиомониторинга и обнаружения закладных устройств: индикаторы поля, комплексы обнаружения закладок и радиомониторинга	
10	Технические каналы утечки информации, общие понятия, технические каналы утечки речевой информации.	
Программно-аппаратные средства обеспечения информационной безопасности		
1	Одноуровневая модель разграничения доступа, достоинства и недостатки.	1. Челухин, В.А. Комплексное обеспечение информационной безопасности автоматизированных систем: Учебное пособие для вузов / В. А. Челухин. - Комсомольск-на-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., - 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
2	Многоуровневая модель разграничения доступа, достоинства и недостатки	
3	Применение специализированных программных средств защиты информации, их достоинства и недостатки.	
4	Физические носители кодов паролей.	
5	Требования к специализированным средствам защиты информации от несанкционированного доступа.	

6	Механизмы организации контроля доступа до загрузки ОС. Механизмы доверенной загрузки ОС, реализованные в СЗИ.	3. 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. Аппаратно-программные средства защиты информации: Практикум / Душкин А.В., Дубровин А.С., Здольник В.В. - Воронеж:Научная книга, 2018. - 198 с.: ISBN 978-5-4446-1043-5 - Режим доступа: http://znanium.com/catalog/product/977192 1. 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, 2019. — 121 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/54767.html 2. Информационная безопасность и защита информации [Электронный ресурс] : учебно-методический комплекс / . — Электрон. текстовые данные. — Алматы: Нур-Принт, 2019. — 98 с. — 9965-756-05-8. — Режим доступа: http://www.iprbookshop.ru/67055.html 3. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2018. — 702 с. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html 4. 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)
7	Подсистемы защиты информации и их реализация в СЗИ от НСД «Dallas Lock».	
8	Организация защищенных вычислительных сетей на базе СЗИ сетевого действия.	
9	Протоколы и средства организации VPN на сетевом уровне. Назначение, область применения, аутентификация и шифрование данных в протоколах SKIP и IPSec.	
10	Организация защищенного документооборота с использованием криптографических средств, предоставляемых СКЗИ «КриптоПро».	
Безопасность операционных систем.		
1	Архитектура ОС. Режим ядра. Режим пользователя. Raid массивы.	1. Компьютерные сети: Учебное пособие [Электронный ресурс]/ Кузин

2	Семафор, мьютекс, монитор, виртуальная память, свопинг, кэш-память	А.В., Кузин Д.А. - 3-е изд., перераб. и доп. - 2019. - 192 с.: // ZNANIUM.COM: электронно-библиотечная система. - Режим доступа: http://znanium.com/catalog/product/536468, ограниченный, Загл. с экрана.
		2. Сети связи и системы коммутации: Учебное пособие [Электронный ресурс]/ Паринов А.В., Ролдугин С.В., Мельник В.А. 2019. - 178 с.// ZNANIUM.COM: электронно-библиотечная система - Режим доступа: http://znanium.com/catalog/product/923309, ограниченный, Загл. с экрана.
		3. Компьютерные сети: Учебное пособие [Электронный ресурс]/ Н.В. Максимов, И.И. Попов. - 3-е изд., испр. и доп. 2019. - 448 с.: ил.; // ZNANIUM.COM: электронно-библиотечная система - Режим доступа: http://znanium.com/catalog/product/163728, ограниченный, Загл. с экрана.
		4. Мэйволд Э. Безопасность сетей [Электронный ресурс]/ Мэйволд Э., 2018.— 571 с. // IPRbooks: электронно-библиотечная система. – Режим доступа: http://www.iprbookshop.ru/73727.html, ограниченный. – Загл. с экрана.
		5. Зиангирова Л.Ф. Вычислительные системы, сети и телекоммуникации [Электронный ресурс] / Зиангирова Л.Ф. — 2018.— 150 с. // IPRbooks: электронно-библиотечная система. – Режим доступа: http://www.iprbookshop.ru/67231.html, ограниченный. – Загл. с экрана.

3	База данных уязвимостей MS, приведите примеры уязвимостей Windows и Linux	
4	Кейлоггеры, руткиты, трояны, вирусы. Методы защиты.	
5	Современные средства анализа уязвимостей операционных систем. Примеры, план проведения сканирования.	
6	Банк данных уязвимостей ФСТЭК. Требования к лицензиатам ФСТЭК в части наличия программного обеспечения.	
7	Файловые системы. Основные виды и понятия. Обеспечение отказоустойчивости файловых систем.	
8	Защита виртуальных инфраструктур в современных операционных системах на примере.	
9	PKI и шифрование в современных операционных системах.	
10	Защита памяти ЭВМ механизмами современных операционных систем.	

Таблица 5.1 – Практические задачи выносимые на ГЭ

№ задания	Содержание задания
1	Реализовать оконное приложение использующее WinAPI функцию реализующую следующую задачу: Определить раскладку клавиатуры выделенного окна
2	Реализовать оконное приложение использующее WinAPI функцию реализующую следующую задачу: Вывести список всех доступных разрешений экрана монитора
3	Реализовать оконное приложение использующее WinAPI функцию реализующую следующую задачу: Отслеживать нажатия клавиш компьютерной мыши
4	Реализовать оконное приложение использующее WinAPI функцию реализующую следующую задачу: Отслеживать нажатия клавиш клавиатуры
5	Реализовать оконное приложение использующее WinAPI функцию реализующую следу-

	ющую задачу: Заблокировать компьютер
6	Реализовать оконное приложение использующее WinAPI функцию реализующую следующую задачу: Проверить является ли текущей пользователь администратором
7	Реализовать оконное приложение использующее WinAPI функцию реализующую следующую задачу: Открыть/закрыть лоток компакт-дисков
8	Реализовать оконное приложение использующее WinAPI функцию реализующую следующую задачу: Изменить обои рабочего стола
9	Реализовать оконное приложение использующее WinAPI функцию реализующую следующую задачу: Нажать на кнопку Пуск.
10	Реализовать оконное приложение использующее WinAPI функцию реализующую следующую задачу: Вызвать стандартное диалоговое окно форматирования дисков.
11	Реализовать оконное приложение использующее WinAPI функцию реализующую следующую задачу: Создать процесс
12	Реализовать оконное приложение использующее WinAPI функцию реализующую следующую задачу: Спрятать и показать кнопку Пуск

Таблица 5.2 – Практические задания выносимые на ГЭ

№ задания	Содержание задания
1	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, рассчитать интегральный показатель рисков, определить систему управления информационной безопасности, разработать план периодических проверок, регламент работ по информационной безопасности.
2	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.
3	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.
4	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.
5	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.
6	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.
7	Разработать политику информационной безопасности для автоматизированной системы класса 3а. 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.
8	Разработать политику информационной безопасности для автоматизированной системы функционирующей в рамках государственной информационной системы класса К1. 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.
9	Разработать политику информационной безопасности для автоматизированной системы функционирующей в рамках государственной информационной системы класса К2. 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.
10	Разработать политику информационной безопасности для автоматизированной системы функционирующей в рамках информационной системы обрабатывающей персональные данные УЗ3. 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.
11	Разработать политику информационной безопасности для автоматизированной системы функционирующей в рамках информационной системы обрабатывающей персональные данные УЗ2. 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.
12	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.

Пример экзаменационного билета:

Экзаменационный билет № 1 Государственный экзамен

1. Этапы развития информационной безопасности, перспективы развития, Технологии будущего.
2. Параметрические каналы утечки информации.
3. Защита памяти ЭВМ механизмами современных операционных систем.
4. Реализовать оконное приложение использующее WinAPI функцию реализующую следующую задачу: Создать процесс
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.

6.4 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;
- 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 6.

Таблица 6 – Показатели, критерии и уровни оценивания результатов ГЭ

Уровни оценивания	**Описание показателей и критериев оценивания**		
	Показатели оценивания	**Критерии оценки теоретической части экзамена**	**Критерии оценки расчетной задачи экзамена**
Высокий уровень – оценка «отлично»	- знание учебного материала (учебных дисциплин); - знание нормативно-законодательных 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 теоретиче-	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.	Правильно оформленное практическое задание, содержащее все необходимые части и корректно работающая программа из практических задач к ГЭ.
Средний уровень –		ответ удовлетворяет в основном требованиям на оцен-	Правильно оформленное

Уровни оценивания	Описание показателей и критериев оценивания		
	Показатели оценивания	Критерии оценки теоретической части экзамена	Критерии оценки расчетной задачи экзамена
оценка «хорошо»	ские знания для анализа конкретных производственных ситуаций и решения прикладных проблем; - общий (культурный) и специальный (профессиональный) язык ответа.	ку «5», но при этом имеет недостатки: 1. в изложении допущены небольшие пробелы, не исказившие содержание ответа; 2. допущены один – два недочета при освещении основного содержания ответа, исправленные по замечанию экзаменатора; 3. допущены ошибка или более двух недочетов при освещении второстепенных вопросов, которые легко исправляются по замечанию экзаменатора.	практическое задание, содержащее часть необходимых разделов и корректно работающая программа из практических задач к ГЭ.
Низкий уровень – оценка «удовлетворительно»	- знание учебного материала (учебных дисциплин); - знание нормативно-законодательных 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 ситуаций и решения прикладных проблем; - общий (культурный) и специальный (профессиональный) язык ответа.	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.	Оформленное практическое задание, содержащее в обязательном порядке модель функционирующая программа из практических задач к ГЭ реализующая часть поставленной задачи.
Недостаточный уровень - оценка «неудовлетворительно»		1. не раскрыто основное содержание учебного материала; 2. обнаружено незнание или непонимание большей или наиболее важной части учебного материала; 3. допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после наводящих вопросов. 4. не сформированы компетенции, умения и навыки.	выставляется при полностью неправильном решении

6.6 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 направлению подготовки.

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.

В период подготовки к государственному экзамену студенты вновь обращаются к учебно-методическому 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 рабочую программу государственной итоговой аттестации в части ГЭ. 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 интернет-источникам. 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 не-

полным 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.

7 Выпускная квалификационная работа

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

7.2 Цель выполнения выпускной квалификационной работы и предъявляемые к ней требования

Выполнение ВКР имеет своей **целью**:

- систематизацию, закрепление и углубление полученных теоретических и практических знаний по направлению подготовки;
- 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.

7.3 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 объекта информатизации на соответствие требованиям по защите информации для (на материалах конкретного предприятия).
2. Исследование … (наименование технического канала утечки информации) в (на материалах конкретного предприятия).
3. Аттестация ИСПДн класса …(указание класса) для (на материалах конкретного предприятия).
4. Комплексная система защиты информации (на материалах конкретного предприятия).
5. Выбор СЗИ (на материалах конкретного предприятия).
6. Исследование параметров (наименование технического канала утечки информации) (на материалах конкретного предприятия).
7. Проектирование защищенной автоматизированной системы (на материалах конкретного предприятия).
8. Управление рисками информационной безопасности на предприятии.
9. Разработка программного комплекса для расчета параметров защиты от утечки по каналу (наименование технического канала утечки информации).
10. Совершенствование системы защиты информации в соответствии с актуальными требованиями законодательства.
11. Обеспечение информационной безопасности распределенных информационных систем.
12. Создание и аттестация альтернативной измерительной площадки (на материалах конкретного предприятия).
13. Проектное управление информационной безопасностью.
14. Разработка программных комплексов защиты от НСД.
15. Разработка программно-аппаратных комплексов защиты от НСД.
16. Разработка программно-технических комплексов для удостоверяющих центров.
17. Разработка программного обеспечения для автоматизации процесса аудита информационной безопасности.
18. Разработка программно-технических комплексов для защиты от утечки по (наименование технического канала утечки информации).
19. Разработка системы контроля устранения выявленных в работе по информационной безопасности несоответствий (на материалах конкретного предприятия).
20. Разработка защищенных мобильных приложений.
21. Организация защищенного канала связи с использованием ГОСТ 28147-89.
22. Защита интеллектуальной собственности. Автоматизация формирования заявок на (патент, свидетельство о регистрации ПО и др.
23. Создание(модернизация) сервера в защищенном исполнении, в соответствии с требованиями по информационной безопасности.
24. Создание(модернизация) системы хранения данных в защищенном исполнении, в соответствии с требованиями по информационной безопасности.

25. Использование генетических алгоритмов в задачах защиты информации.
26. Создание(модернизация) средств контроля от утечки по (наименование технического канала утечки информации).
27. Выбор оптимальной структуры ПАСЗИ и ТСЗИ (на материалах конкретного предприятия).
28. Выбор оптимальной структуры средств контроля защищенности от утечек по техническим каналам, НСД для нужд лаборатории по аттестации ОИ.
29. Проектирование системы защиты информации (на материалах конкретного предприятия).
30. Разработка стратегического плана по развитию системы ЗИ (на материалах конкретного предприятия).
31. Разработка путей снижения рисков информационной безопасности (на материалах конкретного предприятия).
32. Разработка математических моделей для анализа защищенности информационной системы.
33. Разработка математических моделей для анализа защищенности информационной системы (на материалах конкретного предприятия).
34. Разработка системы управления информационной безопасностью (на материалах конкретного предприятия).
35. Криптоанализ отечественных и зарубежных алгоритмов шифрования.
36. Стеганографические алгоритмы сокрытия информации.
37. Оптимизация затрат на организацию и управление информационной безопасностью (на материалах конкретного предприятия).
38. Исследование защищенности сети предприятия (на материалах конкретного предприятия).
39. Разработка программного обеспечения для анализа исходных текстов приложений.
40. Особенности реализации угроз безопасность в ОС Windows или Unix.
41. Разработка программного обеспечения для имитации тестовых сигналов от различных устройств для проведения аттестации по требованиям информационной безопасности.
42. Разработка программного обеспечения для сопряжения (далее следует указание устройства, например R&S FSC3) с ПЭВМ и анализа полученных данных.
43. Разработка программного обеспечения для расчета опасных зон информативного сигнала по каналу ПЭМИ.
44. Исследование защищенной сети (на материалах конкретного предприятия) на наличие программно-аппаратных уязвимостей.
45. Исследование АЭП, возникающих в СВЧ зоне.
46. Исследование каналов ВЧО и ВЧН.
47. Оптимизация затрат на создание и аттестацию экранированной безэховой камеры.

48. Систематизация и исследование оконечных устройств пожаро-охранных сигнализаций на подверженность АЭП.

49. Исследование затуханий информативного сигнала в ВОЛС.

50. Разработка устройства перехвата информативных сигналов по (далее следует наименование технического канала утечки информации).

51. Исследование пассивных средств защиты от утечки по (далее следует наименование технического канала утечки информации).

52. Разработка частной модели угроз безопасности (на материалах конкретной организации).

53. Оптимизация затрат на создание помещения для ведения конфиденциальных переговоров (на материалах конкретного предприятия).

54. Исследование возможности автоматизированного перехода от одной модели разграничения доступа к другой.

55. Исследование подходов к проектированию системы защиты информации на предприятии.

56. Организация защиты траффика в территориально-распределенной локальной вычислительной сети с использованием систем защиты Континент.

57. Организация защиты траффика в территориально-распределенной локальной вычислительной сети с использованием систем защиты VipNet.

58. Математическое моделирование действий злоумышленника с использованием сетей Петри.

59. Оценка угроз безопасности с использованием системы уравнений Колмогорова.

60. Построение интегральной оценки возможности реализации угроз безопасности.

61. Использование эвристических оценок возможности реализации угроз безопасности.

62. Оценка подходов к управлению информационной безопасностью (на материалах конкретного предприятия).

63. Моделирование системы пропускного контроля с использованием нейронных сетей.

64. Использование геоинформационных технологий для позиционирования на местности с целью определения допустимых границ контролируемой зоны.

65. Создание системы контроля доступа на ОИ в защищенном исполнении.

66. Аттестация и контроль систем видео-конференций для обмена конфиденциальной информацией, на соответствие требованиям по защите информации.

67. Исследование возможности программно-математических воздействий на информацию защищенную (далее следует наименование криптографического алгоритма).

68. Криптоанализ на сверхвысокопроизводительных ЭВМ.

69. Исследование сложности криптоанализа (отечественных или зарубежных алгоритмов) с учетом выполнения на сверхвысокопроизводительных ЭВМ.

70. Криптоанализ в реальном времени.

71. Проектирование защищенных автоматизированных систем с учетом распределенной информационной системы и функционирования в условиях повышенной готовности.

72. Управление информационной безопасностью в системах массового обслуживания.

73. Создание и эксплуатация систем массового обслуживания с одноразовыми паролями.

74. Разработка системы защиты с учетом использования ресурсов сети Интернет.

75. Создание инновационных разработок для (обеспечения обороноспособности, безопасности личности).

76. Разработка систем мониторинга радио обстановки в реальном времени с учетом зашумленности канала.

77. Исследование возможности демодуляции информативного сигнала на нестандартных каналах утечки информации.

78. Проектирование защищенной вычислительной сети предприятия с учетом использования беспроводных каналов передачи информации.

79. Исследование защищенности операционных систем с учетом наличия программных закладок.

80. Исследование возможности автономного питания средств защиты и средств измерений в условиях длительной эксплуатации.

81. Разработка программного обеспечения для автоматизированного расчета сопротивления на объекте информатизации.

82. Разработка программно-аппаратных комплексов автоматизированной поверки оборудования используемого при проведении аттестации объектов информатизации.

83. Противодействие программно-математическим воздействиям на объект информатизации с использованием системы обнаружения вторжений.

84. Разработка программного обеспечения для автоматизации деятельности по учету и периодическому контролю оборудования и программного обеспечения лабораторий по аттестации объектов информатизации.

85. Таксономии уязвимостей.

86. Исследование и моделирование рефлексивной разведки с учетом многоступенчатости информационного обмена.

87. Разработка программного обеспечения для автоматизации проведения расчетов при аттестации объекта информатизации.

88. Разработка программного обеспечения для автоматизации проведения спецпроверок или специсследований.

89. Создание (далее следует наименование технического средства) в защищенном исполнении.

90. Разработка программного обеспечения автоматизированного анализа информационных систем на наличие программных и аппаратных уязвимостей.

91. Проектирование и анализ систем автоматического дизассемблирования исходных текстов программ.

92. Исследование способов защиты программного кода от дизассемблирования.

93. Обеспечение информационной безопасности в условиях использования высокоскоростных каналов передачи данных (терабит).

94. Использование нейронных сетей в задачах криптоанализа.

95. Разработка программно-аппаратных комплексов для контроля системы разграничения доступа на ОИ.

96. Разработка программно-аппаратных комплексов для построения системы разграничения доступа на ОИ.

97. Разработка программно-аппаратных решений для фильтрации сетевого траффика.

98. Разработка программно-технических решений для фиксации и контроля исходного состояния программного комплекса ЭВМ.

99. Разработка программно-аппаратных комплексов контроля утечки информации по (далее следует наименование технического канала утечки информации).

ВКР выполняемые по предложенным ниже тематикам могут относиться к ДР или ДП, содержащим сведения составляющие государственную тайну.

100. Особенности реализации угроз безопасности в ОС подразделения ответственного за обработку сведений, составляющих государственную тайну.

101. Особенности аттестации помещений для обработки сведений, составляющих государственную тайну.

102. Организация защищенного обмена в ЛВС, предназначенной для обработки сведений составляющих государственную тайну.

103. Разработка системы управления документацией для подразделения ответственного за обработку сведений, составляющих государственную тайну.

104. Разработка программного обеспечения учета и контроля для подразделения ответственного за обработку сведений, составляющих государственную тайну.

105. Форма, порядок и подход к аттестации подразделения ответственного за обработку сведений, составляющих государственную тайну (на материалах конкретного предприятия).

106. Разработка программного обеспечения для проведения аттестации подразделения ответственного за обработку сведений, составляющих государственную тайну, с использованием (далее следует наименование оборудования, например Октава 110-ЭКО).

107. Оптимизация затрат на создание лаборатории по аттестации объектов, предназначенных для обработки сведений составляющих государственную тайну, по требованиям защиты информации.

108. Оптимизация затрат на создание подразделения ответственного за обработку сведений, составляющих государственную тайну (на материалах конкретного предприятия).

109. Разработка программного обеспечения для оценки утечки информации из подразделения ответственного за обработку сведений, составляющих государственную тайну по (далее следует наименование технического канала утечки информации).

110. Разработка системы управления средствами защиты информации для подразделения ответственного за обработку сведений, составляющих государственную тайну

7.5 Показатели и критерии оценки ВКР

Таблица 9 – Качество и уровень ВКР (*исследовательская работа*)

Показатели оценивания	Уровни оценивания 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 исследо- ваний	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. Использованы известные решения	Содержание, как целой работы, так и ее частей связано с темой работы, имеются небольшие отклонения. Логика изложения присутствует – одно положение вытекает из другого. Использованы как известные ре-	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

Показатели оценивания	Уровни оценивания и описание критериев			
	Недостаточный уровень - «неудовлетворительно»	**Низкий уровень - «удовлетворительно»**	**Средний уровень - «хорошо»**	**Высокий уровень - «отлично»**
			шения, так и новые теоретические модели и решения.	данной темы. Использованы 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 10 – Качество и уровень

Показатели оценивания	Уровни оценивания 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	Актуальность либо вообще не сформулирована, либо сформулирована не	Автор обосновывает актуальность проектирования	Актуальность проблемы проектирования объекта обос-

Показатели оценивания	Уровни оценивания и описание критериев			
	Недостаточный уровень - «неудовлетворительно»	**Низкий уровень - «удовлетворительно»**	**Средний уровень - «хорошо»**	**Высокий уровень - «отлично»**
	работы (либо они есть, но абсолютно не согласуются с содержанием)	в самых общих чертах – проблема не выявлена. Не четко сформулированы цель, задачи, предмет, объект проектирования, методы, используемые в работе.	объекта в целом, а не собственной темы. Сформулированы цель, задачи, предмет, объект проектирования. Тема работы сформулирована более или менее точно.	нована 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	Использованы как традиционные технологические, , управленче-	Использованы новые технологические, управленческие и т п. решения

Показатели оценивания	Уровни оценивания и описание критериев			
	Недостаточный уровень - «неудовлетворительно»	**Низкий уровень - «удовлетворительно»**	**Средний уровень - «хорошо»**	**Высокий уровень - «отлично»**
		элементы новых технологических, или управленческих и т п. решений	ские и т. п. решения, так и элементы новых технологических, 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 11 – Качество защиты ВКР

Показатели оценивания	Уровни оценивания и описание критериев			
	Недостаточный уровень - «неудовлетворительно»	**Низкий уровень - «удовлетворительно»**	**Средний уровень - «хорошо»**	**Высокий уровень - «отлично»**
Качество доклада на заседании ГЭК	Автор совсе 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 связано, но допускает незначительные неточности при ответах. Использует наглядный материал.	Автор уверенно владеет терминологией, защиту строит связано, 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.

Показатели оценивания	Уровни оценивания и описание критериев			
	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 и сводный оценочный лист по направлению подготовки/специальности (приложение 1).

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

7.6 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.

7.7 Перечень рекомендуемой литературы для выполнения ВКР

1. Немцова, Т. И. Программирование на языке С++ [Электронный ресурс]: учеб. пособие / Т.И. Немцова, С.Ю. Голова, А.И. Терентьев; Под ред. Л.Г. Гагариной. - М.: ИД ФОРУМ: ИНФРА-М, 2021. - 512 с. // ZNANIUM.COM : электронно-библиотечная система. – Режим доступа: http://znanium.com/catalog.php#, ограниченный. – Загл. с экрана.

2. Кузин, А. В. Программирование на языке Си [Электронный ресурс] /А.В.Кузин, Е.В.Чумакова - М. : Форум, НИЦ ИНФРА-М, 2019. - 144 с. // ZNANIUM.COM : электронно-библиотечная система. – Режим доступа: http://znanium.com/catalog.php#, ограниченный. – Загл. с экрана.

3. Новиков, Ф.А. Дискретная математика для программистов: Учебное пособие для вузов / Ф. А. Новиков. - 2-е изд. - СПб.: Питер, 2004; 2003; 2001; 2000; 2020- 363с

4. 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

5. 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

6. 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

7. Челухин, В.А. Комплексное обеспечение информационной безопасности автоматизированных систем: Учебное пособие для вузов / В. А. Челухин. - Комсомольск-на-Амуре: Изд-во Комсомольского-на-Амуре гос.техн.ун-та, 2021. - 207с. - Библиогр.: с.201-207. - 273-00.

8. Программно-аппаратная защита информации: Учебное пособие / Хорев П.Б., - М.:Форум, НИЦ ИНФРА-М, 2019. - 352 с.: 60х90 1/16. - (Высшее образование) ISBN 978-5-00091-004-7 - Режим доступа: http://znanium.com/catalog/product/489084

9. Аппаратные и программные средства защиты информации: Учебное пособие / Душкин А.В., Кольцов А., Кравченко А. - Воронеж: Научная книга, 2018. - 232 с. ISBN 978-5-4446-0746-6 - Режим доступа: http://znanium.com/catalog/product/923168

10. Серебренникова А.Г. Информатика [Электронный ресурс] : / А.Г. Серебренни-кова, А. С. Верещагина, Е. Г. Кравченко, Д. Н. Кузнецов. – Комсо-мольск-на-Амуре: ФГБОУ ВПО «КнАГТУ», 2017. – 174 с. // Виртуальная библиотека ИНИТ. – Режим до-ступа: http://initkms.ru/ library/readbook/ 1101570/1, свобод-ный. – Загл. с экрана.

11. Каймин В.А . Информатика [Электронный ресурс]: учебник / В.А. Кай-мин - 6-е изд. - М.: ИНФРА-М, 2016. - 285 с.: // ZNANIUM.COM : электронно-библиотечная систе-ма. – Режим доступа: http://www. znanium.com/catalog.php, ограничен-ный. – Загл. с экрана.

12. Сергеева И.И. Информатика [Электронный ресурс] : учебник / И.И. Сергеева, А.А. Музолевская, Н.В. Тарасова. – М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2017. – 384 с. // ZNANIUM.COM : электронно-библиотечная система. – Режим доступа: http://www. znanium.com/catalog.php, ограничен-ный. – Загл. с экрана.

13. Гуриков С.Р. . Информатика [Электронный ресурс]: учебник / С.Р. Гуриков. - М.: Форум: НИЦ ИНФРА-М, 2017. - 464 с.: // ZNANIUM.COM : электронно-

библиотечная си-стема. – Режим доступа: http://www. znanium.com/catalog.php, ограничен-ный. – Загл. с экрана

14. 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

15. Исаченко, О.В. Программное обеспечение компьютерных сетей: Учеб-ное пособие / О.В. Исаченко. - М.: ИНФРА-М, 2018. - 117 с.: Режим до-ступа: http://znanium.com/catalog/product/232661

16. 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

17. Демидович, Б.П. Основы вычислительной математики. Учебное пособие для втузов / Б.П. Демидович, И.А. Марон. — М.: 1963. — 660 с.: ил.

18. Голицына, О.Л. Языки программирования : Учебное пособие / О.Л. Голицына, Т.Л. Партыка, И.И. Попов. - 2-е изд., перераб. и доп. - М.: Форум, 2019. - 400 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-91134-442-9 - Режим доступа: http://znanium.com/catalog/product/226043

19. Хусаинов, А. А. Структуры и алгоритмы обработки данных : учеб. пособие / А.А. Хусаинов, Н.Н. Михайлова. — Комсомольск-на-Амуре.: ГОУ ВПО Комсомольский-на-Амуре гос.техн.ун-т, 2007. – Ч.1. — 83 с. // Виртуальная библиотека ИНИТ. – Режим доступа: http://www.initkms.ru/library/readbook/1101030/1, свободный. – загл.с экрана

20. Хусаинов, А. А. Структуры и алгоритмы обработки данных : учеб. пособие / А.А. Хусаинов, Н.Н. Михайлова. — Комсомольск-на-Амуре.: ГОУ ВПО Комсомольский-на-Амуре гос.техн.ун-т, 2007. – Ч.2. — 91 с. // Виртуальная библиотека ИНИТ. – Режим доступа: http://www.initkms.ru/library/readbook/1101031/1, свободный. – загл.с экрана

21. 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.

22. Шашло, Н.В. Комплексный подход к обеспечению экономиче-ской 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.

23. Смоленский, М. Б. Информационное право : учебник для вузов / М. Б. Смоленский, М. В. Алексеева. – Ростов н/Д : Феникс, 2015. – 223 с.,

24. Сети связи и системы коммутации: Учебное пособие [Электронный ресурс]/ Паринов А.В., Ролдугин С.В., Мельник В.А. 2015. - 178 с.// ZNANIUM.COM: электронно-библиотечная система - Режим доступа: http://znanium.com/catalog/product/923309, ограниченный, Загл. с экрана.

25. Мэйволд Э. Безопасность сетей [Электронный ресурс]/ Мэйволд Э., 2015.— 571 c. // IPRbooks: электронно-библиотечная система. – Режим доступа: http://www.iprbookshop.ru/73727.html, ограниченный. – Загл. с экрана.

26. Зиангирова Л.Ф. Вычислительные системы, сети и телекоммуникации [Электронный ресурс] / Зиангирова Л.Ф. — 2015.— 150 c. // IPRbooks: электронно-библиотечная система. – Режим доступа: http://www.iprbookshop.ru/67231.html, ограниченный. – Загл. с экрана.

27. 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 : электронно-библиотечная система.- Режим доступа: http://znanium.com/catalog/product/472870, ограниченный. – Загл. с экрана

28. Царев, Р. Ю. Программирование на языке Си [Электронный ресурс] : учеб. пособие / Р. Ю. Царев. – Красноярск : Сиб. федер. ун-т, 2014. – 108 с. // ZNANIUM.COM : электронно-библиотечная система.- Режим доступа: http://znanium.com/catalog/product/510946, ограниченный. – Загл. с экрана

29. В.Д. Колдаев Численные методы и программирование: Учебное пособие[Электронный ресурс] / В.Д. Колдаев; Под ред. Л.Г. Гагариной. - М.: ИД ФОРУМ: НИЦ Инфра-М, 2013. - 336 с.: ил.; // ZNANIUM.COM : электронно-библиотечная система. - Режим доступа: http://znanium.com/catalog/product/370603, ограниченный. – Загл. с экрана

30. Баранова, Е. К. Основы информатики и защиты информации [Электронный ресурс] : Учеб. пособие / Е. К. Баранова. - М. : РИОР : ИНФРА-М, 2013. - 183 с.//ZNANIUM.COM : электронная библиотечная система- Режим доступа: http://znanium.com/catalog/product/415501, ограниченный. – Загл. с экрана

31. 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

32. 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

33. 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 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/54767.html

34. Информационная безопасность и защита информации [Электронный ресурс] : учебно-методический комплекс / . — Электрон. текстовые данные. — Алматы: Нур-Принт, 2012. — 98 c. — 9965-756-05-8. — Режим доступа: http://www.iprbookshop.ru/67055.html

35. 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 ком-пьютерных технологий)

36. 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)

37. 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)

38. 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.

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, взаимо рецензирование, 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.

9 Материально-техническое обеспечение ГИА

Таблица 7 – Материально-техническое обеспечение ГИА

Наименование оборудованных учебных кабинетов	**Адрес (местоположение) учебных кабинетов**
Специальные помещения: *Учебная аудитория для проведения занятий лекционного типа, текущего контроля и промежуточной аттестации, представления результатов самостоятельного исследования ВКР и др. на 30* рабочих мест, оборудованная специализированной (учебной) мебелью (столы, стулья, доска аудиторная комбинированная); набором демонстрационного оборудования для представления информации: *мультимедиа-проектор, компьютер*	ауд. 201 корп. 5
компьютерный класс (учебная аудитория) для групповых и индивидуальных консультаций, для проведения курсового проектирования (выполнения курсовых работ), организации самостоятельной работы, в том числе, научно-исследовательской, оборудованная учебной мебелью на 14 посадочных мест, компьютерами с неограниченным доступом к сети Интернет, включая доступ к ЭБС	ауд. 202 корп. 5

Лист регистрации изменений к РПД

	Номер протокола заседания кафедры, дата утверждения изменения	Количество страниц изменения	Подпись разработчика РПД
1	Протокол заседания кафедры ИБАС № 2 от 12.10.2021	11	