МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СЕРВИСА»
(ФГБОУ ВО «ПВГУС»)

Кафедра «Прикладная информатика в экономике»

УТВЕРЖДАЮ
Проректор по УРиКО, д.э.н., профессор
_____ О.Н. Наумова
от «28» 06 2018 г.

ПРОГРАММА
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

по основной профессиональной образовательной программе высшего образования
направленности (профиля) «Организация и технология защиты информации»
направления подготовки 10.03.01 «Информационная безопасность»
квалификация бакалавр

Тольятти 2018 г.

Программа государственной итоговой аттестации по основной профессиональной образовательной программе (далее – ОПОП или образовательная программа) направленности (профиля) «Экономика предприятий и организаций» направления подготовки 10.03.01 «Информационная безопасность» разработана в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 «Информационная безопасность», утвержденного приказом Минобрнауки РФ от 01.12.2016 г. №1515 (зарегистрировано в Минюсте России 20 декабря 2016 г. № 44821).

Программа государственной итоговой аттестации разработана с учетом:

- Профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Министерством труда и социальной защиты РФ от 15 сентября 2016 г. N 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный №43857.

Разработал: к.э.н., доцент (подпись) Т.А. Раченко

СОГЛАСОВАНО:
Руководитель ОПОП, к.э.н., доцент (подпись) Т.А. Раченко

СОГЛАСОВАНО:

Генеральный директор ООО «Технология Безопасности» (подпись) М.В. Байкалов

МП

Директор ООО ЧОО «Калибр-П» (подпись) А.В. Приженцев

МП

Рассмотрено на заседании кафедры «Прикладная информатика в экономике»
протокол № 12 от «22» июня 2018г.
И. о. заведующего кафедрой, д.э.н., профессор В.А Бердников

Содержание

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1.Цель и задачи государственной итоговой аттестации (ГИА)

Государственная итоговая аттестация, завершающая освоение основной профессиональной образовательной программы, является обязательной и представляет собой форму оценки степени и уровня освоения обучающимися образовательной программы.

Целью государственной итоговой аттестации является определение соответствия результатов освоения обучающимися основной образовательной программы направленности (профиля) «Организация и технология защиты информации» направления подготовки 10.03.01 «Информационная безопасность» требованиям федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 «Информационная безопасность» (уровень бакалавриата).

Задачей ГИА является оценка степени и уровня освоения обучающимся образовательной программы, характеризующих его подготовленность к самостоятельному выполнению видов профессиональной деятельности.

Область профессиональной деятельности выпускников, освоивших программу бакалавриата, включает сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере.

Объектами профессиональной деятельности выпускников, освоивших программу бакалавриата, являются:

- объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, информационные ресурсы и информационные технологии в условиях существования угроз в информационной сфере;
- технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах;
- процессы управления информационной безопасностью защищаемых объектов.

Виды профессиональной деятельности, к которым готовятся выпускники, освоившие образовательную программу прикладного бакалавриата:

эксплуатационная;

проектно-технологическая;

экспериментально-исследовательская;

организационно-управленческая.

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

эксплуатационная деятельность:

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

администрирование подсистем информационной безопасности объекта;

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

автоматизированных систем;

проектно-технологическая деятельность:

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

проведение проектных расчетов элементов систем обеспечения информационной

безопасности;

участие в разработке технологической и эксплуатационной документации;

проведение предварительного технико-экономического обоснования проектных расчетов;

экспериментально-исследовательская деятельность:

сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;

проведение экспериментов по заданной методике, обработка и анализ их результатов;

проведение вычислительных экспериментов с использованием стандартных программных средств;

организационно-управленческая деятельность:

осуществление организационно-правового обеспечения информационной безопасности объекта защиты;

организация работы малых коллективов исполнителей;

участие в совершенствовании системы управления информационной безопасностью;

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

контроль эффективности реализации политики информационной безопасности объекта защиты.

1.2. Допуск к ГИА и итог аттестации

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

Результаты каждого государственного аттестационного испытания определяются оценками "отлично", "хорошо", "удовлетворительно", "неудовлетворительно". Оценки "отлично", "хорошо", "удовлетворительно" означают успешное прохождение государственного аттестационного испытания.

Успешное прохождение государственной итоговой аттестации является основанием для выдачи обучающемуся документа о высшем образовании и о квалификации образца, установленного Министерством образования и науки Российской Федерации.

1.3. Итоговые результаты освоения образовательной программы

Результаты освоения образовательной программы определяются приобретаемыми выпускником компетенциями, т.е. его способностью применять знания, умения и личные качества в соответствии с задачами профессиональной деятельности.

В набор требуемых результатов освоения образовательной программы включаются все общекультурные и общепрофессиональные компетенции, а также профессиональные компетенции, отнесенные к тем видам профессиональной деятельности, на которые ориентирована образовательная программа.

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

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

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

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

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

способность 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);

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

способность 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);

способность к самоорганизации и самообразованию (ОК-8);

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

общепрофессиональными компетенциями:

способность анализировать физические явления и процессы для решения профессиональных задач (ОПК-1);

способность применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2);

способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач (ОПК-3);

способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4);

способность использовать нормативные правовые акты в профессиональной деятельности (ОПК-5);

способность применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности (ОПК-6);

способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7).

профессиональными компетенциями:

способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);

способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);

способность администрировать подсистемы информационной безопасности объекта защиты (ПК-3);

способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);

способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5);

способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6);

способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7);

способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8);

способность осуществлять подбор, изучение и обобщение научно-технической

литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9);

способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10);

способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов (ПК-11);

способность принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12);

способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13);

способность организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14);

способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15).

Выпускник, освоивший программу бакалавриата, должен обладать **профессионально-специализированными компетенциями** в соответствии с направленностью (профилем) программы:

способностью разработать комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение и последующее сопровождение (ПСК-1);

способностью организовать контроль защищенности объекта в соответствии с нормативными документами (ПСК-2).

Выпускник, освоивший программу бакалавриата, должен обладать **дополнительными профессиональными компетенциями**, установленными выпускающей кафедрой дополнительно к компетенциям ФГОС ВО:

способностью развивать (организовывать) предпринимательсто в различных сферах деятельности (ПКВ-1).

При прохождении ГИА обучающиеся должны демонстрировать следующие итоговые результаты освоения компетенций:

Код и наименование компетенции	**Трудовые действия/ практический опыт**	**Необходимые умения**	**Необходимые знания**
Общекультурные компетенции			
ОК-1. Способность использовать основы философских знаний для формирования мировоззренческой позиции	Выполнение задач профессиональной деятельности на основе системы ценностно-мотивационных установок на значимость нравственных качеств личности; формулирование целей и задач, выводов и собственной позиции по профессиональным проблемам	Ориентироваться в наиболее общих философских проблемах бытия, познания, ценностей, свободы и смысла жизни как основах формирования культуры гражданина и профессиональной компетентности. Ставить цели и задачи, строить планы их достижения, в т.ч. на основе сформированной мировоззренческой позиции, соответствующей современному уровню развития науки и общественной практики	Принципы и условия формирования личности, свободы и ответственности за сохранение жизни, культуры, окружающей среды. Методологические основы исследования процессов и явлений

Код и наименование компетенции	Трудовые действия/ практический опыт	Необходимые умения	Необходимые знания
ОК-2. Способность использовать основы экономических знаний в различных сферах деятельности	Выполнение задач профессиональной деятельности с учетом оценки экономических последствий принимаемых решений	Использовать основы знаний микро-, макро- и отраслевой экономики при решении профессиональных задач	Основные экономические категории, закономерности и процессы, протекающие на микро, макро и отраслевом уровнях
ОК-3. Способность анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма	Выполнение задач профессиональной деятельности на основе анализа современных процессов и явлений, происходящих в обществе, в т.ч. с исторической точки зрения и с учетом сформированной гражданской позиции	Устанавливать причинно-следственные связи между событиями и явлениями в обществе. Выражать и обосновывать свою позицию по отношению к историческому прошлому и настоящему, в т.ч. в сфере профессиональной деятельности. Ориентироваться в современной экономической, политической и культурной ситуации в России и мире.	Закономерности и этапы исторического процесса основные события и процессы мировой и отечественной экономической истории, историю и законы развития общественных процессов
ОК-4. Способность использовать основы правовых знаний в различных сферах деятельности	Выполнение задач профессиональной деятельности на основе анализа нормативной и правовой документации	Применять правовые знания в профессиональной деятельности;	Основные законы РФ, основные нормативные правовые документы. Основные нормативные и правовые документы в соответствии с направлением и профилем подготовки
ОК-5. Способность 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	Профессиональное мастерство, навыки применения полученных теоретических знаний в практической деятельности	Использовать методы научного познания в профессиональной области, получать новые знания и умения для достижения цели, использовать профессиональную информацию для самосовершенствования и гармоничного развития личности	Основы профессиональной деятельности и мотивы повышения квалификации
ОК-6. Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	Выполнение задач профессиональной деятельности с учетом норм делового поведения. Организация конструктивного межличностного взаимодействия	Работать в коллективе, выстраивать эффективные коммуникации с коллегами и руководством.	Основные принципы работы в коллективе; служебные обязанности сотрудников коллектива, основы межкультурной коммуникации применительно к общению с людьми разного возраста, статуса,

Код и наименование компетенции	Трудовые действия/ практический опыт	Необходимые умения	Необходимые знания
			культурной принадлежности
ОК-7. Способность 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	Представление и защита результатов выполненных работ в сфере профессиональной деятельности с учетом требований литературной и деловой письменной и устной речи на русском языке, публичной и научной речи, с использованием аргументации и теоретической доказательной базы Использование профессиональной лексики на русском и иностранном языках в заданном контексте	Аргументировано и четко строить свою речь; осуществлять перевод специальной литературы с иностранного языка. Использовать иностранный язык в межличностном общении и профессиональной деятельности	Основные правила грамматики русского языка, основные принципы построения монологических текстов и диалогов, терминологическую лексику, стиль делового общения, теорию логики и аргументации. Основы лексики и грамматики иностранного языка
ОК-8. Способность к самоорганизации и самообразованию	Осознанный выбор и построение индивидуальной траектории интеллектуального, общекультурного и профессионального развития	Самостоятельно приобретать и использовать новые знания и умения, расширять и углублять собственную профессиональную компетентность. Использовать профессиональную информацию для самосовершенствования и гармоничного развития личности	Профессиональные функции в соответствии с направлением и уровнем подготовки. Методы и формы самоорганизации и самообразования с целью достижения поставленной цели
ОК-9. Способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности	Выполнение социальной и профессиональной деятельности на основе самостоятельного методически правильного использования методов физического воспитания и укрепления здоровья для достижения должного уровня физической подготовленности и обеспечения полноценной социальной и профессиональной деятельности	Использовать средства и методы физической культуры и ЗОЖ для физического самосовершенствования, формирования здорового образа жизни, для обеспечения полноценной социальной и профессиональной деятельности. Рационально распределять время на все этапы решения профессиональных задач	Роль физической культуры и здорового образа жизни в современном обществе Методы и средства физической культуры и здорового образа жизни (ЗОЖ)
Общепрофессиональные компетенции			

Код и наименование компетенции	Трудовые действия/ практический опыт	Необходимые умения	Необходимые знания
ОПК-1. Способность анализировать физические явления и процессы для решения профессиональных задач	Навыки использования знаний естественнонаучных дисциплин; навыками проведения физического эксперимента и обработки его результатов	- применять основные законы физики при решении прикладных задач; - анализировать физические явления и процессы в природе - использовать основные законы физики и естественнонаучных дисциплин - выявлять естественнонаучную сущность проблем - проводить инструментальные измерения физических величин - применять знания математики, физики и естествознания в инновационной деятельности -применять методы теории управления физических систем в инновационной деятельности - использовать информационные технологии в исследовании физических явлений и процессов в природе	основные понятия, законы и модели механики; основные понятия, законы и модели электричества и магнетизма; основные понятия, законы и модели теории колебаний и волн, оптики, квантовой физики, физики твердого тела, статистической физики и термодинамики; особенности физических эффектов и явлений, используемых для обеспечения информационной безопасности;
ОПК-2. Способность применять соответствующий математический аппарат для решения профессиональных задач	Владение методами количественного анализа процессов обработки, поиска и передачи информации. криптографической терминологией; навыками использования типовых криптографических алгоритмов; навыками использования ПЭВМ в анализе простейших шифров; навыками математического моделирования в криптографии; создания математических моделей, использования для решения профессиональных задач возможностей специального программного обеспечения	Применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации; использовать математические методы и модели для решения прикладных задач; использовать математические методы и модели теории вероятностей и математической статистики для решения прикладных задач; использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки; применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; уметь пользоваться научно-технической литературой в области криптографии; разрабатывать математические модели, применять для решения задач математического	Основные понятия и методы математического анализа; - основные понятия и методы аналитической геометрии; - основные понятия и методы линейной алгебры и теории алгебраических систем; - основные понятия и методы теории вероятностей и математической статистики; - математические методы обработки экспериментальных данных; - основные задачи и понятия криптографии; - требования к шифрам и основные характеристики шифров; - модели шифров и математические методы их исследования; - принципы построения криптографических алгоритмов, криптографические стандарты и их

Код и наименование компетенции	Трудовые действия/ практический опыт	Необходимые умения	Необходимые знания
		моделирования возможности специального программного обеспечения; - применять методы теории вероятностей и математической статистики в экспериментальных исследованиях.	использование в информационных системах; - основные понятия математического моделирования, основные приемы и методы построения математических моделей в экономике и других сферах деятельности.
ОПК-3. Способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач	Навыками чтения электронных схем. навыками проектирования и расчёта простейших аналоговых и цифровых схем. Навыки эксплуатации современного электронного оборудования.	- применять на практике методы анализа электрических цепей; - проводить расчёты типовых аналоговых и цифровых узлов радиоэлектронной аппаратуры.	- методы анализа электрических цепей; основы схемотехники; - принципы работы элементов современной радиоэлектронной аппаратуры и физические процессы, протекающие в них; основы схемотехники современной радиоэлектронной аппаратуры.
ОПК-4. Способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.	Навыки эксплуатации информационно-коммуникационных технологий; навыками обработки информации; навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями.	- использовать, обобщать и анализировать информацию; - использовать программные и аппаратные средства персонального компьютера; - использовать компьютерные технологии для решения профессиональных задач.	Основные информационные технологии, используемые в автоматизированных системах; информационные технологии сбора, накопления, обработки, передачи и распространения информации.
ОПК-5. Способность использовать нормативные правовые акты в профессиональной деятельности.	- навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; − навыками работы с нормативными правовыми актами; - навыками работы с нормативными правовыми актами; - навыками организации и обеспечения режима секретности; - методами организации и управления деятельностью служб защиты информации на предприятии; - методами формирования требований по защите информации.	применять нормативные правовые акты в профессиональной деятельности при построении модели управления рисками ИБ по различным методикам; - предпринимать необходимые меры по восстановлению нарушенных прав; - применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; - разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации;	- нормативные правовые акты в области защиты информации; - основы организационного и правового обеспечения информационной безопасности; - организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации.

Код и наименование компетенции	Трудовые действия/ практический опыт	Необходимые умения	Необходимые знания
ОПК-6. Способность применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности.	Выполнение задач профессиональной деятельности с учетом аргументированного обоснования принимаемых решений с точки зрения безопасности жизнедеятельности	Проводить идентификацию опасностей и их поражающих факторов в профессиональной деятельности; выбирать средства и способы защиты от поражающих факторов	Правила техники безопасности Методы профилактики чрезвычайных ситуаций (ЧС) и средства защиты Приемы и средства оказания первой помощи пострадавшим
ОПК-7. Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.	Выявление угроз безопасности информации в автоматизированных системах. Проведение анализа уязвимостей автоматизированных и информационных систем. Проведение анализа уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы Оценка информационных рисков Оценка последствий от реализации угроз безопасности информации в автоматизированной системе.	Определять подлежащие защите информационные ресурсы автоматизированных систем. Классифицировать и оценивать угрозы безопасности информации для объекта информатизации. Оценивать информационные риски в автоматизированных системах. Анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах.	Принципы построения информационных систем; принципы организации информационных систем в соответствии с требованиями по защите информации; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах.
Профессиональные компетенции			
эксплуатационная деятельность:			
ПК-1. Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Восстановление после сбоев и отказов программного обеспечения автоматизированных систем. Обнаружение и устранение неисправностей в работе системы защиты информации автоматизированной системы. Установка обновлений программного обеспечения автоматизированной системы. Осуществление автономной наладки технических и программных	Использовать криптографические методы и средства защиты информации в автоматизированных системах. Определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы.	Программно-аппаратные средства обеспечения защиты информации автоматизированных систем. Принципы построения средств защиты информации от "утечки" по техническим каналам. Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах.

Код и наименование компетенции	Трудовые действия/ практический опыт	Необходимые умения	Необходимые знания
	средств системы защиты информации автоматизированной системы.		
ПК-2. Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Использование основных методов и подходов к организации процесса разработки программного обеспечения. Применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач в сфере электронного бизнеса. Применять основные методы интернет-программирования, разработки интернет-приложений. Использования основных методов компонентно-ориентированного программирования, Разработки приложения на основе компонентно-ориентированного программирования.	Применять программные средства обеспечения безопасности данных. Устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации. Составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные. Использовать основные технологии и методы интернет-программирования, Разрабатывать интернет-приложения.	Назначение, функции и структуру операционных систем; системы управления базами данных. Типовые средства, методы и протоколы идентификации, аутентификации и авторизации. Основные технологии и методы программирования, инструментарий программирования приложений; системы программирования для решения профессиональных задач.
ПК-3. Способность администрировать подсистемы информационной безопасности объекта защиты	Навыки администрирования подсистем информационной безопасности объекта. Анализ воздействия изменений конфигурации автоматизированной системы на ее защищенность. Обнаружение, идентификация и устранение инцидентов в процессе эксплуатации автоматизированной системы. Организации комплекса мер по информационной безопасности.	Применять средства и методы администрирования подсистем информационной безопасности объекта. Конфигурировать параметры системы защиты информации автоматизированных систем. Регистрировать, контролировать и анализировать события, связанные с защитой информации в автоматизированных системах. Определять источники и причины возникновения инцидентов и оценивать последствия выявленных инцидентов	Основы администрирования вычислительных сетей. Регламент информирования персонала автоматизированной системы о выявленных инцидентах. Регламент учета выявленных инцидентов. Регламент устранения инцидентов.

Код и наименование компетенции	Трудовые действия/ практический опыт	Необходимые умения	Необходимые знания
ПК-4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Принципы формирования политики информационной безопасности в автоматизированных системах. Навыками по организации комплекса мер по информационной безопасности.	Разрабатывать политики безопасности информации автоматизированных систем. Устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации.	Структура и содержание политики информационной безопасности. Основные направления реализации политики информационной безопасности. Основные элементы реализации комплексного подхода к обеспечению информационной безопасности на предприятии. Порядок разработки КСЗИ, управление. КСЗИ,
ПК-5. Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Проведение экспертизы состояния защищенности информации автоматизированных систем. Выработка рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы. Выработка рекомендаций для принятия решения о повторной аттестации автоматизированной системы или о проведении дополнительных аттестационных испытаний. Проведение приемочных испытаний системы защиты информации автоматизированной системы; организации и сопровождения аттестации объекта информатизации по требованиям безопасности информации;	Конфигурировать аттестованную информационную систему и системы защиты информации информационной системы. Применять методы организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;	Критерии оценки защищенности автоматизированной системы. Методы организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации.
ПК-6. Сособность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации.	Навыками организации и проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации. Расчет показателей эффективности защиты информации, обрабатываемой в автоматизированных системах. Входной контроль	Принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации. Осуществлять контроль обеспечения уровня защищенности в автоматизированных системах. Применять технические средства контроля эффективности мер защиты	Методики организации и проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации. Технические средства контроля эффективности мер защиты информации. Критерии оценки эффективности и надежности средств

Код и наименование компетенции	Трудовые действия/ практический опыт	Необходимые умения	Необходимые знания
	качества комплектующих изделий системы защиты информации автоматизированной системы	информации. Контролировать эффективность принятых мер по защите информации в автоматизированных системах. Выполнять проверку работоспособности и эффективности программных, программно-аппаратных и технических средств защиты информации.	защиты программного обеспечения автоматизированных систем.
проектно-технологическая деятельность:			
ПК-7. Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.	Навыками сбора и анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности. Навыками технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности.	Собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности. Проводить и анализировать результаты технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности	Структуру и состав исходных данных для проектирования подсистем и средств обеспечения информационной безопасности. Принципы построения и организации систем защиты информации. Методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и систем защиты автоматизированных систем. Методы проведения технико-экономического обоснования проектных решений.
ПК-8. Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов.	Внесение изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы. Подготовка документов, определяющих правила и процедуры контроля обеспеченности уровня защищенности информации, содержащейся в информационной системе. Подготовка документов, определяющих правила и процедуры выявления инцидентов, которые могут привести к сбоям или нарушению	Разработать и оформить рабочую техническую документацию. Анализировать исходные данные для проектирования подсистем и средств обеспечения информационной безопасности. Применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности.	Структуру и состав систем документационного обеспечения. Содержание эксплуатационной документации автоматизированной системы. Нормативную и методическую документацию. Требования к оформлению рабочей технической документации с учетом действующих нормативных и методических документов.

Код и наименование компетенции	Трудовые действия/ практический опыт	Необходимые умения	Необходимые знания
	функционирования информационной системы и возникновению угроз безопасности информации. Проведение проверки полноты описания в организационно-распорядительных документах на автоматизированную систему действий персонала по реализации организационных мер защиты информации.		
экспериментально-исследовательская деятельность:			
ПК-9. Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности .	Навыки подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов. Навыками составления обзоров по вопросам обеспечения информационной безопасности;	Собрать информацию по вопросам обеспечения информационной безопасности по профилю своей деятельности и провести ее анализ.	Методы поиска информации. Методы подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов. Национальные, межгосударственные и международные стандарты в области защиты информации; нормативные и методические материалы по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности. Основные нормативные правовые документы, международные и отечественные стандарты в сфере информационной безопасности и защиты информации. Нормативные и методические основы экономики защиты информации.
ПК-10. Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.	Навыки проведения анализа информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов. Анализ и устранение недостатков в функционировании системы защиты информации автоматизированной системы.	Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем. Формулировать требования к настраиваемым аппаратным и программным комплексам.	Отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем. Методики сертификационных испытаний технических средств защиты

Код и наименование компетенции	Трудовые действия/ практический опыт	Необходимые умения	Необходимые знания
	Реализовывать требования стандартов в области информационной безопасности. Проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности. работы с инструментальными средствами тестирования и эксплуатации аппаратных и программных средств вычислительных устройств, комплексов, систем и сетей.		информации от "утечки" по техническим каналам на соответствие требованиям по безопасности информации. Основные методики эксплуатации объектов и систем в области информационной безопасности.
ПК-11. Способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов.	Навыки проведения экспериментов по заданной методике, обработки результатов, оценки погрешности и достоверности их результатов. Применения технологий проведения экспериментальных исследований для решения экономических задач.	Применять методы планирования экспериментов. Методики проведения экспериментов. Методики обработки результатов экспериментов и методики оценки погрешности и достоверности результатов экспериментов. Использовать математический аппарат при решении профессиональных задач. Применять основные положения и методы социальных, гуманитарных и экономических наук при решении профессиональных задач. Разрабатывать инновационные методы, средств и технологий в области профессиональной деятельности (коммерческой, маркетинговой, рекламной, логистической и (или) товароведной).	Методы планирования экспериментов. Методики проведения экспериментов. Методики обработки результатов экспериментов, методики оценки погрешности и достоверности результатов экспериментов. Основы экономических знаний в различных сферах деятельности. Типовые методики и действующие нормативно-правовые базы. Методики расчёта экономических и социально-экономических показателей, характеризующие деятельность хозяйствующих субъектов.
ПК-12. Способность принимать участие в проведении экспериментальных исследований системы защиты информации.	Проведение экспериментальных исследований и предварительных испытаний системы защиты информации автоматизированной системы. Использования инструментов моделирования и статистической обработки экономической информации.	Применять методики и средства проведении экспериментально-исследовательских работ системы защиты информации Осуществлять выбор рациональных информационных систем и информационно-коммуникативных технологий решения для управления бизнесом. Оценивать соотношение планируемого результата и	Методики и средства проведении экспериментально-исследовательских работ системы защиты информации. Способы осуществления сбора, анализа и обработки данных, необходимых для решения профессиональных задач

Код и наименование компетенции	Трудовые действия/ практический опыт	Необходимые умения	Необходимые знания
		затрачиваемых ресурсов.	
организационно-управленческая деятельность:			
ПК-13. Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.	Обеспечение безопасности информации с учетом требования эффективного функционирования автоматизированной системы. Составление комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе. Обоснование и контроль результатов управленческих решений в области безопасности информации автоматизированных систем.	Разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем. Применять средства обеспечения отказоустойчивости автоматизированных систем. Использовать методы организации комплекса мер по обеспечению информационной безопасности; Управлять процессом реализации комплекса мер по обеспечению информационной безопасности.	Основные меры по защите информации в автоматизированных системах. Основные понятие и технологии кодирования информации. Назначение комплекса мер по обеспечению информационной безопасности, методы управления процессом их реализации;
ПК-14. Способность организовывать работу малого коллектива исполнителей в профессиональной деятельности.	Проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий с персоналом на макетах или в тестовой зоне. Проведение проверки готовности персонала к эксплуатации системы защиты информации автоматизированной системы. Информирование пользователей о правилах эксплуатации автоматизированной системы с учетом требований по защите информации организации работы малого коллектива исполнителей в профессиональной деятельности.	Осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации. Обучать персонал автоматизированной системы комплексу мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения защиты информации. Организовывать работы малого коллектива исполнителей в профессиональной деятельности. Методики организации работы малого коллектива исполнителей в профессиональной деятельности.	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности и защиты информации автоматизированных систем. Методы организации работы малого коллектива исполнителей в профессиональной деятельности
ПК-15. Способность организовывать технологический процесс защиты	Навыками организации и обеспечения режима секретности. Методами формирования	Применять нормативные документы по противодействию технической разведке.	Руководящие и методические документы уполномоченных федеральных органов

Код и наименование компетенции	Трудовые действия/ практический опыт	Необходимые умения	Необходимые знания
информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	требований по защите информации; использования методов организации технологического процесса защиты информации ограниченного доступа. Организации технологического процесса защиты информации ограниченного доступа.	Обнаруживать и устранять нарушения правил разграничения доступа. Реализовывать правила разграничения доступа персонала к объектам доступа. Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем. Применять нормативные правовые акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	исполнительной власти по защите информации. Нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации. Способы и средства защиты информации от утечки по техническим каналам; методы организации технологического процесса защиты информации ограниченного доступа. Методы организации технологического процесса защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю .
Дополнительные компетенции:			
ПКВ-1 способность развивать (организовывать) предпринимательство в различных сферах деятельности	Навыки сбора и анализа исходных данных для развития предпринимательской деятельноси; навыки технико-экономического анализа и обоснования проектных решений; навыки применения современных систем внутреннего документооборота организации для формирования информационного обеспечения участников организационных проектов;	Применять нормативные документы для реализации предпринимательской деятельности; развивать (организовывать) предпринимательство в различных сферах деятельности, анализировать информационные потоки в организации и разрабатывать предложения по повышению эффективности документооборота при ведении баз данных по различным показателям;	- основные направления реализации предпринимательской деятельности; - основы реализации предпринимательства в различных сферах деятельности; - роль информации в общеорганизационном управлении и её связь со стратегическими задачами организации для обеспечения участников организационных проектов; - нормативную базу, российские и международные законодательные акты.
Профессионально-специализированные компетенции:			

Код и наименование компетенции	Трудовые действия/ практический опыт	Необходимые умения	Необходимые знания
ПСК-1. Способность разработать комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение и последующее	разработки комплекса мер по обеспечению информационной безопасности объекта в области технической защиты информации.	разработать комплекс мер по обеспечению информационной безопасности объекта в области технической защиты информации;	методы и средства контроля эффективности технической защиты информации;
ПСК-2. Способность организовать контроль защищенности объекта в соответствии с нормативными документами.	пользования нормативных документов по защите информации.	пользоваться нормативными документами по защите информации;	основные элементы контроля защищенности объекта в соответствии с нормативными документами;

1.4. Место ГИА в структуре образовательной программы, ее формы и объем

В соответствии с образовательной программой по направлению подготовки 10.03.01 «Информационная безопасность» в процедуру ГИА входит:

- защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты,
- подготовка к сдаче и сдача государственного экзамена.

№ п/п	*Форма ГИА*	*Объём ГИА*	*Формируемые компетенции*		
		з/ед.	*ОК*	*ОПК*	*ПК*
1	Государственный экзамен	3	-	ОПК-4 ОПК-6	ПК-1 ПК-3 ПСК-1 ПСК-2
2	Защита выпускной квалификационной работы	6	ОК-1 ОК-2 ОК-3 ОК-4 ОК-5 ОК-6 ОК-7 ОК-8 ОК-9	ОПК-1 ОПК-2 ОПК-3 ОПК-4 ОПК-5 ОПК-6 ОПК-7	ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 ПК-6 ПК-7 ПК-8 ПК-9 ПК-10 ПК-11 ПК-12 ПК-13 ПК-14 ПК-15 ПКВ-1 ПСК-1 ПСК-2
Всего:		**9**			

2. ПРОГРАММА ГОСУДАРСТВЕННОГО ЭКЗАМЕНА

2.1. Общие положения

Государственный экзамен проводится по следующим дисциплинам образовательной программы, результаты освоения которых имеют определяющее значение для профессиональной деятельности выпускников:

1. Защита и обработка конфиденциальных документов.
2. Информационные системы и технологии.
3. Криптографические методы защиты информации.
4. Нормативная база, российские и международные стандарты по информационной безопасности.
5. Основы научных исследований и дипломное проектирование.
6. Проектирование информационных систем.
7. Сети и системы передачи информации.
8. Техническая защита информации.

Государственный экзамен проводится письменно. Время проведения – 1,5 астрономических часа.

Перед государственным экзаменом проводится консультирование обучающихся по вопросам, включенным в программу государственного экзамена (предэкзаменационная консультация).

Результаты государственного аттестационного испытания объявляются в день его проведения либо на следующий рабочий день после дня его проведения.

По результатам государственного аттестационного испытания в форме государственного экзамена обучающийся имеет право на апелляцию.

2.2. Содержание государственного экзамена и его соотнесение с совокупным ожидаемым результатом освоения основной образовательной программы

На государственном экзамене обучающиеся получают экзаменационный билет (Приложение 1), в котором предлагается выполнить 20 тестовых заданий и решить практическое задание (задачу). Экзаменационный билет включает задания, которые отражают уровень сформированности компетенций обучающегося.

Задания, включаемые в билеты государственного экзамена, соответствуют рабочим учебным программам дисциплин учебного плана.

При ответе на вопросы/задания экзаменационного билета студент должен продемонстрировать совокупное владение следующими компетенциями или их элементами:

Вид профессиональной деятельности	*Код компетенции*	*Тестовые задания*	*Практическое задание (задача)*	*Наименование дисциплин*
	ОПК-4	+	+	Проектирование информационных систем. Информационные системы и технологии. Сети и системы передачи информации. Основы научных исследований и дипломное проектирование
	ОПК-6	+		Основы научных исследований и дипломное проектирование
	ПСК-1	+	+	Техническая защита информации
	ПСК-2	+		Нормативная база, российские и международные стандарты по информационной безопасности
Эксплуатационная деятельность	ПК-1	+	+	Защита и обработка конфиденциальных документов Криптографические методы защиты информации.
	ПК-3	+		Защита и обработка конфиденциальных документов.

2.3. Фонд оценочных средств для проведения государственной итоговой аттестации в форме государственного экзамена

2.3.1. Типовые контрольные задания к государственному экзамену, необходимые для оценки результатов освоения образовательной программы

Примерные тестовые задания по компетенциям, включенным в государственный экзамен:

- способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4):

1. Под доступностью информации принято понимать:

A. возможность за приемлемое время получить требуемую информационную услугу

B. актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения

C. защита от несанкционированного доступа к информации

D. возможность коллективно использовать информацию, обеспечивая при этом ее защиту и защиту ресурсов информационной системы

2. Под целостностью информации принято понимать:

A. возможность за приемлемое время получить требуемую информационную услугу

B. актуальность и непротиворечивость, защищенность от разрушения и несанкционированного изменения

C. защита от несанкционированного доступа к информации

D. возможность коллективно использовать информацию, обеспечивая при этом ее защиту и защиту ресурсов информационной системы

3. Под конфиденциальностью информации принято понимать:

A. возможность за приемлемое время получить требуемую информационную услугу

B. актуальность и непротиворечивость, защищенность от разрушения и несанкционированного изменения

C. защита от несанкционированного доступа к информации

D. возможность коллективно использовать информацию, обеспечивая при этом ее защиту и защиту ресурсов информационной системы

4. Потоки конфиденциальной информации делятся на

A. прямые и обратные

B. постоянные и временные

C. входные, выходные и внутренние

5. Информационные ресурсы – это:

A. совокупность данных любой природы;

B. файлы данных;

C. носители данных;

D. пакеты прикладных программ

6. Что такое автоматизированное рабочее место?

A. совокупность информационно-програмно-технических ресурсов, обеспечивающих конечному пользователю обработку данных и автоматизацию управленческих функций в конкретной предметной области

B. совокупность внутренних и внешних потоков прямой и обратной связи экономического объекта, методов, средств, специалистов, участвующих в процессе обработки информации и выработки управленческих решений

C. среди перечисленных правильных ответов нет

7. Современные операционные системы поддерживают следующие виды пользовательских интерфейсов:

A. речевые;

B. графические;

C. текстовые, речевые.

D. текстовые, речевые, графические

8. Основные принципы новой (компьютерной) информационной технологии:

A. интерактивный (диалоговый) режим работы с компьютером;

B. интегрированность (стыковка, взаимосвязь) с другими программными продуктами;

C. трудность процесса изменения, как данных, так и постановок задач;

D. применение только локальных аппаратных и программных средств обработки информации.

9. Выделите определения понятия «Информационная система»:

A. процесс, использующий совокупность средств и методов сбора, обработки и передачи данных (первичной информации) для получения информации нового качества о состоянии объекта, процесса или явления (информационного продукта);

B. совокупность четко определенных и целенаправленных действий персонала по переработке информации на компьютере;

C. человеко - компьютерная система для поддержки принятия решений и производства информационных продуктов, использующая компьютерную информационную технологию;

D. взаимосвязанная совокупность средств, методов и персонала, используемых для хранения, обработки и выдачи информации в интересах достижения поставленной цели

10. Технология обновления информационной базы справочно-поисковых систем подразумевает обновление информационного банка пользователя:

A. без его полной замены

B. путем полной замены

C. путем ответа на конкретизированные тематические запросы пользователя

D. верного ответа нет

11. Информационная технология, как и любая другая, должна отвечать следующим требованиям:

A. включать весь набор элементов, необходимых для достижения поставленной цели;

B. иметь регулярный характер. Этапы, действия, операции технологического процесса могут быть стандартизированы и унифицированы, что позволит более эффективно осуществлять целенаправленное управление информационными процессами;

C. обеспечивать необходимость ручного ввода и обработки информации на этапах технологии;

D. обеспечивать необходимость выполнения этапов (фаз), операций, действий процесса обработки информации только одним элементом информационной системы.

12. Информационная технология – это:

A. совокупность методов, производственных процессов и программно-технических средств для обработки данных;

B. технология общения с компьютером;

C. технология обработки данных на ЭВМ.

13. Микропроцессор:

A. это центральный блок ПК, предназначенный для управления работой всех блоков машины и для выполнения арифметических и логических операций над информацией;

B. это основная интерфейсная система компьютера, обеспечивающая сопряжение и связь всех его устройств между собой;

C. содержит провода и схемы сопряжения для передачи управляющих сигналов и импульсов во все блоки машины.

14. Информационная технология, как и любая другая, должна отвечать следующим требованиям:

A. включать весь набор элементов, необходимых для достижения поставленной цели;

B. иметь регулярный характер. Этапы, действия, операции технологического процесса могут быть стандартизированы и унифицированы, что позволит более эффективно осуществлять целенаправленное управление информационными процессами;

C. обеспечивать необходимость ручного ввода и обработки информации на этапах технологии;

D. обеспечивать необходимость выполнения этапов (фаз), операций, действий процесса обработки информации только одним элементом информационной системы.

15. Выделите характеристику 4-го этапа развития информационных технологий (с начала 90-х гг.):

A. этап характеризуется проблемой обработки больших объемов данных в условиях ограниченных возможностей аппаратных средств;

B. этап связывается с распространением ЭВМ серии IBM/360. Проблема этого этапа — отставание программного обеспечения от уровня развития аппаратных средств;

16. Под информационной безопасностью понимается (выбрать неверное высказывание):

A. защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений;

B. состояние защищенности информационной среды общества, обеспечивающее

ее формирование, использование и развитие в интересах граждан, организаций и государства;

C. в создание в организации комплекса административных мер, позволяющих разрешить или запретить доступ сотрудников к определенной информации и средствам ее обработки, выработать правила работы с информацией определить систему наказаний за их несоблюдение.

17. Процесс создания системы защиты информации в информационных системах подразумевает обязательное прохождение этапов:

A. описания информационных, технических и программных средств, обслуживающего персонала и пользователей;

B. выявление угроз, определение политики безопасности, создание механизмов поддержки безопасности и оценки защищенности системы;

C. выявления доступности, целостности и конфиденциальности.

18. Основным видом криптографического преобразования информации является шифрование, которое заключается в

A. скрытии смысла хранимой или передаваемой информации и самого факта хранения или передачи закрытой информации;

B. проведении обратимых математических, логических, комбинаторных и других преобразованиях искомой информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов;

C. замене смысловых конструкций исходной информации (слов, предложений) кодами.

19. Какое из следующих определений CASE-технологии является неверным?

A. совокупность методологий анализа, проектирования и сопровождения сложных информационных систем, поддерживаемая комплексом взаимосвязанных средств автоматизации

B. технология имитационного моделирования

C. метод отображения свойств системы через формализованное описание компонентов системы и связей между ними

D. инструментарий, позволяющий автоматизировать процесс проектирования экономической информационной системы

20. Какие существуют модели жизненного цикла информационных систем:

A. реляционная, сетевая, иерархическая

B. фреймовая, экспертная, комбинированная

C. каскадная, поэтапная, спиральная

D. системы управления базами данных

21. Впервые комплексный подход к защите информации применил

A. знаменитый режиссер Альфред Хичкок на съемках своих фильмов

B. известный изобретатель Альфред Нобель при производстве взрывчатых веществ

C. крупный промышленник Альфред Круп на своих фабриках

D. учёный и путешественник Альфред Брем при работе над научно-популярной книгой «Жизнь животных»

22. Фридрих Касиски опубликовал метод, впоследствии названный его именем, позволявший быстро и эффективно вскрывать практически любые шифры своего времени, в:

A. 1863 году

B. 1800 году

C. 1945 году

23. Знаменитая шифровальная машина Энигма была придумана в

A. Нидерландах

B. Германии

C. США

D. СССР

24. Самый известный криптоаналитик в России начала XX в.

A. И.А. Зыбин
B. Г.И. Бокий
C. В.Л. Бурцев
D. В. И. Ленин

25. Шифрование заключается в

A. проведении обратимых математических, логических, комбинаторных и других преобразованиях искомой информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов

B. скрытии смысла хранимой или передаваемой информации и самого факта хранения или передачи закрытой информации

C. замене смысловых конструкций исходной информации (слов, предложений) кодами

D. процессе преобразования закрытой информации без знания ключа и при отсутствии сведений об этом алгоритме

26. Стеганография заключается в

A. скрытии смысла хранимой или передаваемой информации и самого факта хранения или передачи закрытой информации

B. проведении обратимых математических, логических, комбинаторных и других преобразованиях искомой информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов

C. замене смысловых конструкций исходной информации (слов, предложений) кодами

D. процессе преобразования закрытой информации без знания ключа и при отсутствии сведений об этом алгоритме

27. Кодирование заключается в

A. замене смысловых конструкций исходной информации (слов, предложений) кодами

B. скрытии смысла хранимой или передаваемой информации и самого факта хранения или передачи закрытой информации

C. проведении обратимых математических, логических, комбинаторных и других преобразованиях искомой информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов

D. процессе преобразования закрытой информации без знания ключа и при отсутствии сведений об этом алгоритме

28. Криптостойкость обеспечивается

A. секретностью ключа
B. потенциальной стоимостью информации
C. секретностью алгоритма шифрования
D. временем шифрования или расшифрования

- способность применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности (ОПК-6):

29. Максимальная продолжительность работы за компьютером не должна превышать:

A. 6 часов;
B. 10 часов;
C. 20 часов.

30. Продолжительность непрерывной работы за компьютером (ЭВМ) не должна превышать норму в……., без учета регламентируемого времени перерыва

A. 1 час;

B. 3 часа;

C. 8 часов.

31. Площадь рабочего места каждого сотрудника должно быть не менее

A. 5 $м^2$;

B. 15 $м^2$;

C. 2 $м^2$.

32. В случае, если офискомпании, где будет происходить работа и обслуживанием информационной системы, составляет 30 м2, норма освещения для такой площади согласно СНиП для офисного помещения, общего назначения, составляет:

A. 400 Лк;

B. 800 Лк;

C. 1200 Лк.

33. Какой производственный фактор называют вредным?

A. фактор, негативное воздействие которого на человека приводит к ухудшению самочувствия;

B. фактор, негативное воздействие которого на человека приводит к травме;

C. фактор, негативное воздействие которого на человека приводит к заболеванию;

D. фактор, негативное воздействие которого на человека приводит к летальному исходу;

E. нет правильного ответа.

34. Как классифицируют опасности по вероятности воздействия на человека и среду обитания?

A. естественные, техногенные и антропогенные;

B. реальные и нереальные;

C. потенциальные, реальные и реализованные;

D. мотивированные и немотивированные;

E. нет правильного ответа.

35. Что такое «потенциальная опасность»?

A. опасность, которая всегда связана с конкретной угрозой воздействия на объект защиты, с пространством и временем;

B. опасность, представляющая угрозу общего характера, не связанная с пространством и временем;

C. факт воздействия реальной опасности на человека и среду обитания;

D. опасность, созданная элементами техносферы;

E. нет правильного ответа.

36. Что такое «безопасность»?

A. опасность, которая представляет угрозу общего характера, не связанная с пространством и временем воздействия;

B. состояние объекта защиты, при котором воздействие на него всех потоков вещества, энергии и информации не превышает максимально допустимых значений;

C. полное отсутствие опасностей;

D. количественная характеристика опасности;

E. нет правильного ответа.

37. Диаграммы потоков данных DFD рассматривает систему как

A. совокупность предметов

B. взаимосвязанные работы

C. основные бизнес-процессы

38. DFD описывает:

A. функции обработки информации, документы, объекты, сотрудников или отделы, которые участвуют в обработке информации, внешние ссылки и таблицы для хранения документов

B. основной поток событий, который приводит к требуемому результату наиболее коротким путем

C. входы/выходы, механизмы, управление и вызовы

39. Диаграммы потоков данных (Data flow diagramming, DFD) выполняются в программе

A. BPwin

B. Microsoft Visio

C. Adobe PhotoShop

40. Выявляет основные бизнес-процессы как последовательности транзакций, которые должны выполняться целиком, когда выполнение обособленного подмножества действий не имеет значения без выполнения всей последовательности - это

A. UML-диаграмма прецедентов использования

B. UML-диаграмма классов объектов

C. UML-диаграмма состояний

41. Диаграмма отображает динамику состояний объектов одного класса и связанных с ними событий - это

A. UML-диаграмма состояний

B. UML-диаграмма прецедентов использования

C. UML-диаграмма классов объектов

42. Диаграмма отображает динамическое взаимодействие объектов в рамках одного прецедента использования - это

A. UML-диаграмма взаимодействия объектов

B. UML-диаграмма прецедентов использования

C. UML-диаграмма состояний

43. Диаграмма, которая отображает потоки работ во взаимосвязанных прецедентах использования (могут декомпозироваться на более детальные диаграммы) - это

A. UML-диаграмма деятельностей

B. UML-диаграмма взаимодействия объектов

C. UML-диаграмма прецедентов использования

44. К источникам случайных воздействий можно отнести:

A. неисправные технические средства сбора, обработки, передачи и хранения информации

B. ошибки персонала

C. стихийные силы

D. программы, содержащие вирусы

E. действие создаваемых злоумышленником полей и сигналов

- способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1):

45. Какое сетевое устройство воспроизводит сигнал данных без сегментации сети?

A. маршрутизатор;

B. концентратор;

C. модем;

D. коммутатор.

46. Что характеризует физическую топологию локальной сети (LAN)?

A. указывает схему адресации, которая используется в LAN;

B. определяет, используется ли в LAN широковещательная рассылка или эстафетная передача;

C. указывает способ подключения к LAN узлов и сетевых устройств;

D. определяет порядок осуществления доступа узлов к сети.

47. Какой протокол действует на прикладном уровне модели TCP/IP?

A. IP;

B. TCP;
C. HTTP;
D. ICMP.

48. Какая организация по стандартам публикует действующие стандарты Ethernet?
A. EIA/TIA;
B. IEEE;
C. ANSI;
D. CCITT.

49. Сеть, какого типа охватывает одно здание или комплекс зданий и предоставляет сервисы и приложения пользователям в общей организационной структуре?
A. персональная сеть (PAN);
B. глобальная сеть (WAN);
C. локальная сеть (LAN);
D. муниципальная сеть (MAN).

50. Основные способы разделения субъектов к совместно используемым объектам:
A. Концептуальное - разделение объектов на уровне структуры ИС
B. Физическое - субъекты обращаются к физически различным объектам.
C. Временное - субъекты с различными правами доступа к объекту получают его в различные промежутки времени.
D. Логическое - субъекты получают доступ к совместно используемому объекту в рамках единой операционной среды, но под контролем средств разграничения доступа
E. Криптографическое - все объекты хранятся в зашифрованном виде

51. В качестве биометрических признаков, которые могут быть использованы при идентификации потенциального пользователя, можно выделить следующие:
узор радужной оболочки и сетчатки глаз;
A. отпечатки пальцев;
B. геометрическая форма руки;
C. форма и размеры лица;
D. форма и размеры носа и ушей;
E. особенности голоса;
F. особенности прически;
G. биомеханические характеристики рукописной подписи;
H. биомеханические характеристики "клавиатурного почерка".

52. Система разграничения доступа к информации должна содержать следующие функциональные блоки:
A. блок идентификации и аутентификации субъектов доступа;
B. диспетчер доступа;
C. диспетчер оперативной памяти;
D. диспетчер дисковых устройств;
E. блок криптографического преобразования информации при ее хранении и передаче;
F. блок очистки памяти.

53. Для аппаратной поддержки защиты и изоляции ядра в архитектуре ЭВМ должны быть предусмотрены:
A. многоуровневый режим выполнения команд;
B. использование ключей защиты и сегментирование памяти;
C. реализация механизма виртуальной памяти с разделением адресных пространств;
D. аппаратная реализация части функций ОС;
E. аппаратная реализация устройств доступа;

54. Какие защитные механизмы могут реализовать аппаратно-программные комплексы защиты?

A. идентификация и аутентификация пользователей;
B. авторизация пользователей;
C. разграничение доступа к файлам, каталогам, дискам;
D. контроль целостности программных средств и информации;
E. возможность создания функционально замкнутой среды пользователя;

55. Какие защитные механизмы могут реализовать аппаратно-программные комплексы защиты?

A. защита процесса загрузки ОС;
B. блокировка ПЭВМ на время отсутствия пользователя;
C. криптографическое преобразование информации;
D. регистрация событий;
E. очистка памяти.
F. очистка жесткого диска.

56. Основные компоненты системы защиты программных продуктов от несанкционированного копирования:

A. модуль проверки ключевой информации
B. модуль защиты от изучения алгоритма работы системы защиты;
C. модуль согласования с работой функций защищаемой программы в случае ее санкционированного использования;
D. модуль шифрования входной информации

57. Методы противодействия дизассемблированию:

A. шифрование;
B. архивация:
C. использование самогенерирующих кодов;
D. «обман» дизассемблера.
E. «обман» пользователя.

58. Для противодействия трассировке программы в ее состав вводятся следующие механизмы:

A. изменение среды функционирования;
B. модификация кодов программы;
C. «случайные» переходы.
D. «лишние» операторы.

59. Классификация. компьютерных вирусов по режиму функционирования:

A. резидентные вирусы
B. транзитные вирусы
C. файловые вирусы - вирусы, заражающие файлы с программами;
D. загрузочные (бутовые) вирусы - вирусы, заражающие программы, хранящиеся в системных областях дисков.

60. Классификация. компьютерных вирусов по объекту внедрения:

A. резидентные вирусы
B. транзитные вирусы
C. файловые вирусы - вирусы, заражающие файлы с программами;
D. загрузочные (бутовые) вирусы - вирусы, заражающие программы, хранящиеся в системных областях дисков.

61. Классификация компьютерных вирусов по степени и способу маскировки:

A. stealth-вирусы;
B. вирусы-мутанты (MtE-вирусы) - вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса.
C. транзитные вирусы
D. файловые вирусы - вирусы, заражающие файлы с программами;

- способность администрировать подсистемы информационной безопасности

объекта защиты (ПК-3):

62. Единая политика безопасности по всей сети – это особенность

A. корпоративных распределенных компьютерных сетей

B. любых компьютерных сетей

C. общедоступных распределенных компьютерных сетей

D. коммерческих распределенных компьютерных сетей

63. С увеличением интеграции узлов и компонентов в устройстве обработки информации

A. усложняется проведение специальной проверки данного устройства на наличие в нем модулей, выполняющих несанкционированные, с точки зрения пользователя, действия

B. упрощается проведение специальной проверки данного устройства на наличие в нем модулей, выполняющих несанкционированные, с точки зрения пользователя, действия

C. требуется обязательное проведение специализированной проверки данного устройства на наличие модулей, выполняющих несанкционированные, с точки зрения пользователя, действия

D. перестает требоваться проведение специальной проверки данного устройства на наличие модулей, выполняющих несанкционированные, с точки зрения пользователя, действия.

64. Увеличение производительности вычислительной системы и емкости каналов связи позволяет злоумышленнику в более короткие сроки произвести

A. вскрытие паролей и ключей доступа

B. организовать интенсивное воздействие на узел информационной сети

C. физическое хищение любых носителей информации

D. сбой в работе всей информационной системы

65. Автоматизация в виде скриптов, макросов, приложений VBA, технологии COM

A. может нанести серьезный ущерб системе защиты информации в целом

B. не может нанести серьезный ущерб системе защиты информации в целом

C. не сказывается на системе защиты информации в целом, т. к. влияет только на деятельности пользователей и обслуживающего персонала

D. упрощает работу системы защиты информации в целом за счет минимизации деятельности пользователей и обслуживающего персонала

66. Идентификация –

A. процесс распознавания элемента системы, обычно с помощью заранее определенной априорной информации; каждый субъект или объект должен быть однозначно идентифицируем.

B. проверка идентификации пользователя, процесса, устройства или другого компонента системы; а также проверка целостности данных при их хранении или передаче для предотвращения несанкционированной модификации.

C. предоставление субъекту прав на доступ к объекту.

D. ограничение возможностей использования ресурсов системы программами, процессами или другими системами (для сети) в соответствии с политикой безопасности.

67. Аутентификация –

A. процесс распознавания элемента системы, обычно с помощью заранее определенной априорной информации; каждый субъект или объект должен быть однозначно идентифицируем.

B. проверка идентификации пользователя, процесса, устройства или другого компонента системы; а также проверка целостности данных при их хранении или передаче для предотвращения несанкционированной модификации.

C. предоставление субъекту прав на доступ к объекту.

D. ограничение возможностей использования ресурсов системы программами, процессами или другими системами (для сети) в соответствии с политикой безопасности.

68. Авторизация –

A. процесс распознавания элемента системы, обычно с помощью заранее определенной априорной информации; каждый субъект или объект должен быть однозначно идентифицируем.

B. проверка идентификации пользователя, процесса, устройства или другого компонента системы; а также проверка целостности данных при их хранении или передаче для предотвращения несанкционированной модификации.

C. предоставление субъекту прав на доступ к объекту.

D. ограничение возможностей использования ресурсов системы программами, процессами или другими системами (для сети) в соответствии с политикой безопасности.

69. Политика безопасности:

A. фиксирует правила разграничения доступа

B. отражает подход организации к защите своих информационных активов

C. описывает способы защиты руководства организации

70. Что можно отнести к обязанностям начальника службы безопасности

A. осуществление непосредственного руководства деятельностью сотрудников СБ

B. организация всей системы мер безопасности, осуществление взаимодействия ее составляющих элементов

C. планирование процесса обеспечения безопасности

D. разработка руководящих документов и инструкций по вопросам безопасности

E. все вышеперечисленное

71. Какое из ниже перечисленных направлений не относятся к структуре СЗИ:

A. комплексная защита информации

B. мониторинг телефонных разговоров с санкции ФСБ

C. эксплуатация абонентского пункта специальной связи

D. администрирование ЛВС

E. администрирование безопасности БД

- способность разработать комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение и последующее сопровождение (ПСК-1):

72. Под утечкой понимают

A. неконтролируемое распространение защищаемой информации путем ее разглашения, несанкционированного доступа к ней и получения разведками

B. доведение защищаемой информации до неконтролируемого количества получателей информации

C. получение защищаемой информации заинтересованным субъектом с нарушением правил доступа к ней.

D. воздействие с нарушением правил ее изменения (например, намеренное внедрение в защищаемые информационные ресурсы вредоносного программного кода).

E. воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств, природных явлений, иных нецеленаправленных воздействий

73. Разглашение — это

A. неконтролируемое распространение защищаемой информации путем ее разглашения, несанкционированного доступа к ней и получения разведками

B. доведение защищаемой информации до неконтролируемого количества получателей информации

C. получение защищаемой информации заинтересованным субъектом с нарушением правил доступа к ней.

D. воздействие с нарушением правил ее изменения (например, намеренное внедрение в защищаемые информационные ресурсы вредоносного программного кода).

E. воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств, природных явлений, иных нецеленаправленных воздействий

74. Целями системы защиты информации предприятия являются:

A. приемлемость защиты для пользователей

B. определение объектов защиты

C. предотвращение утечки, хищения, утраты, искажения, подделки информации

75. Для грамотного построения и эксплуатации системы защиты необходимо соблюсти следующие принципы ее применения:

A. сохранение, конфиденциальности документированной информации в соответствии с законодательством

B. постоянный контроль за наиболее важной информацией

C. независимость системы управления для пользователей

76. Алгоритм создания системы защиты конфиденциальной информации таков

A. определение объектов защиты

B. определение объектов защиты, сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах

C. независимость системы управления для пользователей

77. Какая концепция предполагает возможность использования службой безопасности всего комплекса легитимных методов профилактики и отражения потенциальных угроз:

A. стратегия адекватного ответа

B. стратегия пассивной защиты

C. упреждающего противодействия

78. Задача проведения анализа уязвимости информационной системы:

A. рассмотрение всех возможных угроз и оценка размеров возможного ущерба

B. определение всех возможных слабых мест информационной системы

C. регламентация деятельности кредитной организации

79. Служба защиты информации (СЗИ) – это:

A. государственное учреждение по защите информации

B. специализированная организация

C. это самостоятельное структурное подразделение в рамках деятельности организации, тесно связана со службами охраны и объектового режима, составляет основу всей системы обеспечения информационной безопасности

80. В число целей политики безопасности верхнего уровня входит:

A. решение сформировать или пересмотреть комплексную программу безопасности

B. обеспечение базы для соблюдения законов и правил

C. обеспечение конфиденциальности почтовых сообщений

- способность организовать контроль защищенности объекта в соответствии с нормативными документами (ПСК-2):

81. Согласно Закону «Об информации, информатизации и защите информации» риск, связанный с использованием информации, полученной из несертифицированной системы, лежит на

A. владельце этой системы и средств;

B. собственнике документов;

C. потребителе информации.

82. К охраняемым объектам информационной сферы относят:

A. информационные ресурсы, систему их формирования, распространения и использования, информационную инфраструктуру

B. мировые информационные ресурсы

C. персональные данные, коммерческую тайну, промышленные секреты и государственную тайну

83. Любое решение на передачу персональных данных за границу в страну с другим подходом к защите данных основывается на

A. взаимном договоре соответствующих органов защиты информации странах-партнеров

B. доверии к реципиенту и к правовым положениям о защите данных, существующим в стране-импортере

C. договоре с третьей стороной, которая будет выступать независимы контролером положений о защите данных в этих двух странах

D. взаимном изменении законодательства стран-партнеров

84. Перечень издаваемых конфиденциальных документов

A. стандартизирован для всех предприятий определенной сферы деятельности

B. разрабатывается для каждого предприятия индивидуально

C. общепринят для всех предприятий определенной формы собственности

85. Система электронного документооборота должна поддерживать

A. весь жизненный цикл документов, включая подготовку, согласование и визирование их проектов, публикацию документа, организацию архивного хранения документов с доступом к электронным архивам

B. работу с электронным архивом типовых документов, базу данных сотрудников, регистрацию проектов, и организацию архивного хранения документов

C. подготовку как электронных, так и бумажных документов

86. Юридическая сила документа –

A. это свойство официального документа, сообщаемое ему действующим законодательством, компетенцией издавшего его органа и установленным порядком оформления

B. в правильном порядком оформления и наличие подписи ответственного лица

C. реквизит, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации и позволяющий идентифицировать владельца, а также установить отсутствие искажения информации

87. Документооборот (как предмет защиты) – это

A. обмен документами между двумя организациями

B. движение документов между двумя пунктами документооборота

C. упорядоченная совокупность или сеть каналов объективного, санкционированного распространения конфиденциальной информации в процессе управленческой и производственной деятельности пользователей или потребителей этой информации

88. Информация, полученная без использования неправомерных средств, при проведении собственных исследований, по собственной инициативе, путем систематических наблюдений или сбора сведений

A. может быть отнесена к коммерческой тайне по усмотрению получателя информации

B. не должна относиться к коммерческой тайне

C. обязательно должна являться общедоступной

89. Четко определена Федеральным законом обязательность составления

A. бухгалтерская документация

B. управленческая документация

C. научно-техническая документация

90. При осуществлении конфиденциального документооборота Доступ – это

A. получение разрешения руководителя на выдачу тому или иному сотруднику конкретных сведений с учетом его служебных обязанностей

B. установление правил, определяющих порядок доступа

C. процесс обеспечения достижения оптимального уровня обеспечения доступа

91. Универсальным носителем информации считается

A. человек
B. магнитные диски
C. оптические диски

92. Несанкционированный доступ —

A. неконтролируемое распространение защищаемой информации путем ее разглашения, несанкционированного доступа к ней и получения разведками

B. доведение защищаемой информации до неконтролируемого количества получателей информации

C. получение защищаемой информации заинтересованным субъектом с нарушением правил доступа к ней.

D. воздействие с нарушением правил ее изменения (например, намеренное внедрение в защищаемые информационные ресурсы вредоносного программного кода).

E. воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств, природных явлений, иных нецеленаправленных воздействий

93. Несанкционированное воздействие на защищаемую информацию —

A. неконтролируемое распространение защищаемой информации путем ее разглашения, несанкционированного доступа к ней и получения разведками

B. доведение защищаемой информации до неконтролируемого количества получателей информации

C. получение защищаемой информации заинтересованным субъектом с нарушением правил доступа к ней.

D. воздействие с нарушением правил ее изменения (например, намеренное внедрение в защищаемые информационные ресурсы вредоносного программного кода).

E. воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств, природных явлений, иных нецеленаправленных воздействий

94. Под непреднамеренным воздействием на защищаемую информацию понимают

A. неконтролируемое распространение защищаемой информации путем ее разглашения, несанкционированного доступа к ней и получения разведками

B. доведение защищаемой информации до неконтролируемого количества получателей информации

C. получение защищаемой информации заинтересованным субъектом с нарушением правил доступа к ней.

D. воздействие с нарушением правил ее изменения (например, намеренное внедрение в защищаемые информационные ресурсы вредоносного программного кода).

E. воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств, природных явлений, иных нецеленаправленных воздействий

95. К умышленным угрозам относятся:

A. несанкционированные действия обслуживающего персонала ИС (например, ослабление политики безопасности администратором, отвечающим за безопасность ИС);

B. случайные сбои в работе аппаратных средств ИС, линий связи, энергоснабжения;

C. ошибки пользователей ИС;

D. воздействие на аппаратные средства ИС физических полей других электронных устройств (при несоблюдении условий их электромагнитной совместимости)

E. несанкционированный доступ к ресурсам ИС со стороны пользователей ИС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями.

96. К непреднамеренным угрозам относятся:

A. ошибки в разработке программных средств ИС;

B. воздействие на аппаратные средства ИС физических полей других электронных устройств (при несоблюдении условий их электромагнитной совместимости)

C. несанкционированные действия обслуживающего персонала ИС (например, ослабление политики безопасности администратором, отвечающим за безопасность ИС);

D. несанкционированный доступ к ресурсам ИС со стороны пользователей ИС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями.

Типовые практические задания (задачи) к государственному экзамену (ОПК-4, ПК-1, ПСК-1):

Практическое задание 1.

Решить задачи:

1. *Получено шифрованное сообщение РДАИАНМН. Стало известно, что при шифровании применялся метод перестановки с фиксированным периодом d=8 с ключом 64275813 Получить исходный текст.*

2. *В компании введено в эксплуатацию новое офисное здание, в котором предусмотрено отдельное помещение (комната) для проведения совещаний руководства.*

Конструкция здания	Каркасное +металл, пластик
Этаж	8
Площадь помещения, $м^2$	50
Наличие окон	3 окна
Оборудование	кондиционер
Телефонная связь	Телефон внутренний
Компьютеры	Компьютер секретаря в сети Ethternet

Задание:

1. Провести предварительный анализ и определить возможные технические каналы утечки информации для заданного помещения. Оценить их по следующим направлениям:
   - с точки зрения возможности доступа,
   - с точки зрения вида информации и возможного ущерба от её утечки.
2. Предложить основные мероприятия по инженерно-технической защите информации для заданного помещения:
   - на постоянной основе (стационарно в помещении или в здании);
   - проводимые во время проведения совещаний руководства в данном помещении.

Практическое задание 2.

Решить задачи:

1. *Расшифруйте сообщение, зашифрованное методом перестановки по таблице 4х4 (символ подчеркивания заменяет пробел).*
Ключ указывает порядок считывания столбцов при шифровании
Ответ запишите прописными русскими буквами; в качестве пробела используйте символ подчеркивания Сообщение: РНПЛНЕРЙХЕ_ОАИАЕ Ключ: 2413

2. *Внесите данные в таблицы в соответствие с функциями указанных протоколов, перечислите функции протоколов.*

TCP	• Электронная почта.	UDP

	• Обнаружение ошибок. • Надежная доставка данных • Снижение накладных расходов • WEB-браузер • NFS • Simple File Transfer • Без привязки к соединениям	

Практическое задание 3.

Решить задачи:

1. *Определите ключ в системе шифрования, использующей перестановку с фиксированным периодом d=5 по паре открытых и зашифрованных сообщений: ОДНА_БУКВА – _НОАДАКБВУ*
Ответ запишите в виде последовательности цифр без пробелов

2. *Соотнесите уровни модели OSI с уровнями модели TCP/IP*

Модель OSI	Модель TCP/IP
Транспортный Сетевой Представления Сеансовый Физический Канальный Уровень приложений	Уровень приложений Транспортный
	Internet Сетевой доступ

Для описания, каких процессов, используются данные модели OSI и TCP/IP?

Из приведенной ниже последовательности названий стандартных стеков коммуникационных протоколов выделите названия, которые относятся к одному и тому же стеку: TCP/IP, Microsoft, IPX/SPX, Novell, Internet, DoD, NetBIOS/SMB, DECnet.

Практическое задание 4.

Решить задачи:

1. *Определите ключ в системе шифрования, использующей перестановку с фиксированным периодом d=5 по паре открытых и зашифрованных сообщений: ШИФРОВАНИЕ – ОИРШФЕАИВН Ответ запишите в виде последовательности цифр без пробелов.*

2. *Исходные данные:*
В компании введено в эксплуатацию новое офисное здание, в котором предусмотрено отдельное помещение (комната) для проведения совещаний руководства.

Конструкция здания	Бетон (монолит)
Этаж	6
Площадь помещения, м^2	30
Наличие окон	3 окна
Оборудование	кондиционер
Телефонная связь	Телефон гор.тел.сети
Компьютеры	Компьютер секретаря в сети Ethternet

Задание:

1. Провести предварительный анализ и определить возможные технические каналы утечки информации для заданного помещения. Оценить их по следующим направлениям:
   - с точки зрения возможности доступа,
   - с точки зрения вида информации и возможного ущерба от её утечки.
2. Предложить основные мероприятия по инженерно-технической защите информации для заданного помещения:
   - На постоянной основе (стационарно в помещении или в здании);
   - Проводимые во время проведения совещаний руководства в данном помещении.

Практическое задание 5.

Решить задачи:

1. *Определить, чему равен результат выполнения побитовой операции «сумма по модулю 2» для десятичных чисел 250 и 191? Ответ представить в двоичной системе счисления.*

2. *Исходные данные:*

В компании введено в эксплуатацию новое офисное здание, в котором предусмотрено отдельное помещение (комната) для проведения совещаний руководства.

Конструкция здания	Каркасное +кирпич
Этаж	7
Площадь помещения, м^2	40
Наличие окон	нет
Оборудование	Встроенный кондиционер
Телефонная связь	Телефон гор.тел.сети
Компьютеры	Компьютер секретаря

Задание:

1. Провести предварительный анализ и определить возможные технические каналы утечки информации для заданного помещения. Оценить их по следующим направлениям:
   - с точки зрения возможности доступа,
   - с точки зрения вида информации и возможного ущерба от её утечки.
2. Предложить основные мероприятия по инженерно-технической защите информации для заданного помещения:
   - На постоянной основе (стационарно в помещении или в здании);
   - Проводимые во время проведения совещаний руководства в данном помещении.

Практическое задание 6.

1. *Определить результат выполнения побитовой операции «сумма по модулю 2» для шестнадцатеричных чисел 9E и 0A3?*

2. *Исходные данные:*

В компании введено в эксплуатацию новое офисное здание, в котором предусмотрено отдельное помещение (комната) для проведения совещаний руководства.

Конструкция здания	Бетон (монолит)
Этаж	3
Площадь помещения, м^2	40
Наличие окон	3 окна
Оборудование	кондиционер
Телефонная связь	Телефон внутренний
Компьютеры	Компьютер секретаря

Задание:

1. Провести предварительный анализ и определить возможные технические каналы утечки информации для заданного помещения. Оценить их по следующим направлениям:
   - с точки зрения возможности доступа,
   - с точки зрения вида информации и возможного ущерба от её утечки.
2. Предложить основные мероприятия по инженерно-технической защите информации для заданного помещения:
   - На постоянной основе (стационарно в помещении или в здании);
   - Проводимые во время проведения совещаний руководства в данном помещении.

Практическое задание 7.

Решить задачи:

1. *Таблица замен для пропорциональных шифров имеет вид:*

Символ	Варианты замены					Символ	Варианты замены					
А	760	128	350	201		С	800	767	105			
Б	101					Т	759	135	214			
В	210	106				У	544					
Г	351					Ф	560					
Д	129					Х	768					
Е	761	130	802	352		Ц	545					
Ж	102					Ч	215					
З	753					Ш	103					
И	762	211	131			Щ	752					
К	754	764				Ъ	561					
Л	132	354				Ы	136					
М	755	742				Ь	562					
Н	763	756	212			Э	750					
О	757	213	765	133	353	Ю	570					
П	743	766				Я	216	104				
Р	134	532				Пробел	751	769	758	801	849	035...

Определить, какое сообщение зашифровано последовательностью:
2118001357652152127627548011317635601331347427605452111 31?

2. *Исходные данные:*

В компании введено в эксплуатацию новое офисное здание, в котором предусмотрено отдельное помещение (комната) для проведения совещаний руководства.

Конструкция здания	Кирпичное
Этаж	2
Площадь помещения, м^2	30
Наличие окон	2 окна
Оборудование	кондиционер
Телефонная связь	Телефон гор.тел.сети
Компьютеры	Компьютер секретаря в сети Ethternet

Задание:

1. Провести предварительный анализ и определить возможные технические каналы утечки информации для заданного помещения. Оценить их по следующим направлениям:
   - с точки зрения возможности доступа,
   - с точки зрения вида информации и возможного ущерба от её утечки.
2. Предложить основные мероприятия по инженерно-технической защите информации для заданного помещения:
   - На постоянной основе (стационарно в помещении или в здании);
   - Проводимые во время проведения совещаний руководства в данном помещении.

Практическое задание 8.

Решить задачи:

1. *Таблица замен для пропорциональных шифров имеет вид:*

Символ	Варианты замены					Символ	Варианты замены					
А	760	128	350	201		С	800	767	105			
Б	101					Т	759	135	214			
В	210	106				У	544					
Г	351					Ф	560					
Д	129					Х	768					
Е	761	130	802	352		Ц	545					
Ж	102					Ч	215					
З	753					Ш	103					
И	762	211	131			Щ	752					
К	754	764				Ъ	561					
Л	132	354				Ы	136					
М	755	742				Ь	562					
Н	763	756	212			Э	750					
О	757	213	765	133	353	Ю	570					
П	743	766				Я	216	104				
Р	134	532				Пробел	751	769	758	801	849	035...

Определить, какое сообщение зашифровано последовательностью
3532147641341367591367628497541282123503540357671062167532 11?

2. *Исходные данные:*

В компании введено в эксплуатацию новое офисное здание, в котором предусмотрено отдельное помещение (комната) для проведения совещаний руководства.

Конструкция здания	панельное
Этаж	1
Площадь помещения, $м^2$	25
Наличие окон	2 окна
Оборудование	кондиционер
Телефонная связь	Телефон внутренний
Компьютеры	Компьютер секретаря

Задание:

1. Провести предварительный анализ и определить возможные технические каналы утечки информации для заданного помещения. Оценить их по следующим направлениям:
   - с точки зрения возможности доступа,
   - с точки зрения вида информации и возможного ущерба от её утечки.
2. Предложить основные мероприятия по инженерно-технической защите информации для заданного помещения:
   - На постоянной основе (стационарно в помещении или в здании);
   - Проводимые во время проведения совещаний руководства в данном помещении.

Практическое задание 9.

Решить задачи:

1. *Документооборот фирмы составляет примерно 10 тысяч документов в год, нормированное количество листов каждого дела не более 250. Средний объем хранимых документов, включая копии, - 5 листов. В фирме работает 50 человек, а текучесть кадров - 20% в год. Рассчитать наполняемость и требуемую площадь для хранения документов этой фирмы.*

2. *Определить законодательно-нормативную базу, определяющую обращение с информацией на всех видах носителей, для предприятия, указанного в варианте задания. Отдельно выделить законодательно-нормативную базу, касающуюся защиты персональных данных.*

В ответе документы сгруппировать по следующим уровням:

- федеральный;
- региональный и местный;
- нормативная база предприятия (организации).

Варианты:

Предприятие по выпуску комплектующих изделий и узлов для автомобилей.

Примечание: на предприятии применяется система электронного документооборота с применением электронной цифровой подписи.

Практическое задание 10.

Решить задачи:

1. *Определить результат шифрования, если известно:*

Первый байт фрагмента текста в шестнадцатеричном виде имеет вид А5. На него накладывается по модулю два 4-х битовая гамма 0111 (в двоичном виде).

2. *Определить законодательно-нормативную базу, определяющую обращение с информацией на всех видах носителей, для предприятия, указанного в варианте задания.*

Отдельно выделить законодательно-нормативную базу, касающуюся защиты интеллектуальной собственности.

В ответе документы сгруппировать по следующим уровням:

- федеральный;
- региональный и местный;
- нормативная база предприятия (организации).

Варианты:

Завод по производству минеральных удобрений.

Примечание: на предприятии применяется система электронного документооборота с применением электронной цифровой подписи.

Практическое задание 11.

Решить задачи:

1. *Первый байт фрагмента текста, зашифрованного методом гаммирования (по модулю 2), в шестнадцатеричном виде имеет вид 9А. До шифрования текст имел первый байт, равный 74 (в шестнадцатеричном виде). Определить, какой ключ использовался при шифровании.*

2. *Определить законодательно-нормативную базу, определяющую обращение с информацией на всех видах носителей, для предприятия, указанного в варианте задания. Отдельно выделить законодательно-нормативную базу, касающуюся защиты персональных данных.*

В ответе документы сгруппировать по следующим уровням:

- федеральный;
- региональный и местный;
- нормативная база предприятия (организации).

Варианты:

Предприятие по выпуску мороженого и кондитерских изделий.

Примечание: на предприятии применяется система электронного документооборота с применением электронной цифровой подписи.

2.3.2. Описание критериев оценки результатов сдачи государственного экзамена, оценивания компетенций, а также шкал оценивания

При оценивании результатов сдачи государственного экзамена используются критерии оценивания ответов практических заданий, оценивания компетенций.

Шкала оценки уровня освоения компетенций

Качественная оценка может быть выражена: в процентном отношении качества уровня освоения компетенций, которая соответствует баллам, и переводится в уровневую шкалу и оценки «отлично» / 5, «хорошо» / 4, «удовлетворительно» / 3, «неудовлетворительно» / 2.

Шкалы оценки уровня сформированности компетенций		**Уровневая шкала оценки за государственный экзамен**	
Уровневая шкала оценки компетенций	*100 балльная шкала, %*	*100 балльная шкала, %*	*5-балльная шкала, дифференцированная оценка/балл*
допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2
пороговый	61-85,9	70-85,9	«хорошо» / 4
		61-69,9	«удовлетворительно» / 3

повышенный	86-100	86-100	«отлично» / 5

Для интегральной оценки освоения студентами компетенций применяется единый подход согласно балльно-рейтинговой системы по 100-балльной шкале, действующей в университете.

Итоговая оценка результатов государственного экзамена определяется как результат итогов выполнения заданий экзаменационного билета. Форма оценочного листа результатов государственного экзамена представлена в Приложении 2.

Результирующая оценка государственного экзамена получается путем суммирования оценок, полученных на отдельных этапах экзамена. В основу оценивания уровня подготовки выпускника на государственном экзамене положен квалиметрический метод с учетом весомости ответов на вопросы, при этом вес оценки за решение тестовых заданий – 0,7 баллов, за выполнение практического задания – 0,3 баллов.

$$O_{результ} = 0{,}7 \cdot O_{тест} + 0{,}3 \cdot O_{практика},$$

где Орезульт – результирующая оценка по государственному экзамену в баллах; Отест – балльная оценка за тестовые задания; Опрактика – балльная оценка выполнения практического задания государственного экзамена.

По завершении экзамена члены ГЭК на закрытом заседании обсуждают характер ответов каждого обучающегося, анализируют проставленные каждым членом комиссии оценки, и проставляют итоговую согласованную оценку по государственному экзамену.

Решение о соответствии компетенций, сформированных у обучающегося, требованиям ФГОС ВО, принимается членами ГЭК персонально на основании балльной оценки каждого вопроса.

Оценка «отлично», соответствующая повышенному уровню сформированности компетенций, выставляется обучающемуся, если он усвоил методологические основы (свободно владеет понятиями, определениями, терминами), показал систематизированные и полные знания учебного материала, умеет анализировать и выявлять его взаимосвязь с другими областями знаний, исчерпывающе, последовательно, четко и логически его излагает, умеет тесно увязывать теорию с практикой, правильно обосновывает принятие решения и имеет оценку за выполнение заданий не ниже 86 баллов, владеет разносторонними навыками и приемами выполнения практических заданий, способен к самостоятельному анализу и оценке проблемных ситуаций. Содержание ответов свидетельствует об уверенных знаниях, об умении самостоятельно решать профессиональные задачи, соответствующие будущей квалификации.

Оценка «хорошо», соответствующая пороговому уровню сформированности компетенций, выставляется обучающемуся, если он твердо знает учебный материал, грамотно и по существу его излагает, не допуская существенных неточностей, владеет понятиями, терминами, методами исследования, умеет установить взаимосвязь изученной дисциплины с другими областями знаний, владеет необходимыми навыками и приемами решения практических и ситуационных задач, применяет теоретические знания на практике и получившему при выполнении заданий государственного экзамена оценку 70-85,9 баллов. Содержание ответов свидетельствует о достаточных знаниях и об умении решать профессиональные задачи, соответствующие будущей квалификации, однако обучающимся допущены незначительные неточности при изложении материала, не искажающие содержание ответа по существу вопроса.

Оценка «удовлетворительно», соответствующая пороговому уровню сформированности компетенций, выставляется обучающемуся, если он имеет знание основного материала, но при его изложении, нарушает логическую последовательность, справляется с заданиями на пороговом уровне и имеет оценку за выполнение заданий 61-69,9 баллов.

Оценка «неудовлетворительно», соответствующая допороговому уровню сформированности компетенций (ниже 61 балла), выставляется обучающемуся в случае,

если сформированность компетенций, выносимых на государственный экзамен, не соответствует требованиям ФГОС.

2.4. Рекомендации обучающимся по подготовке к государственному экзамену

Подготовка к государственному экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач.

Самостоятельная подготовка к государственному экзамену включает в себя как повторение на более высоком уровне полученных в процессе профессиональной подготовки блоков и разделов образовательной программы, вынесенных на экзамен, так и углубление, закрепление и самопроверку приобретенных и имеющихся знаний. Особое внимание следует уделять интеграции знаний из разных дисциплин, то есть собственно междисциплинарности конструируемого ответа. Междисциплинарность при ответе на вопрос, поставленный в экзаменационном билете, означает, что выпускник должен продемонстрировать свои знания в совокупности дисциплин, что позволит вынести заключение об уровне его подготовленности к самостоятельной практической деятельности.

Перед сдачей государственного экзамена для студентов организуется консультация ведущих преподавателей дисциплин, включенных в государственный экзамен, на которой преподаватели напоминают обучающимся наиболее сложные вопросы дисциплин, вынесенные на государственный экзамен, решают типовые задачи, отвечают на вопросы студентов.

Формулировка вопросов экзаменационного билета совпадает с формулировкой перечня рекомендованных для подготовки вопросов государственного экзамена, доведенного до сведения студентов за 6 месяцев до ГИА. Пример экзаменационного билета представлен в Приложении к настоящей программе.

Каждая дисциплина для подготовки к госэкзамену сопровождается указанием на литературу. Изучение проблемы, поставленной в задании, целесообразно начать с основной литературы по учебной дисциплине.

2.5.Перечень рекомендуемой литературы для подготовки к государственному экзамену

1. Басовский, Л. Е. Экономика отрасли [Электронный ресурс] : учеб. пособие для вузов по направлениям подгот. 38.03.02 "Менеджмент", 44.03.04 "Проф. обучение" (квалификация (степень) "бакалавр") / Л. Е. Басовский. - Документ Bookread2. - М. : Инфра-М, 2017. - 145 с. : ил. - Библиогр.: с. 143. - (Высшее образование). - Режим доступа: http://znanium.com/bookread2.php?book=774017
2. Бороненкова, С. А. Комплексный экономический анализ в управлении предприятием [Электронный ресурс] : учеб. пособие для бакалавров и магистров по направлению подгот. "Экономика" / С. А. Бороненкова, М. В. Мельник. - Документ Bookread2. - М. : Форум, 2016. - 351 с. - Библиогр.: с. 338-340. - Прил.. - Режим доступа: http://znanium.com/bookread2.php?book=519274
3. Волков, О. И. Экономика предприятия [Электронный ресурс] : учеб. пособие для вузов по экон. специальностям и направлениям / О. И. Волков, В. К. Скляренко. - 2-е изд. - Документ Bookread2. - М. : ИНФРА-М, 2016. - 263 с. : ил. - Режим доступа: http://http://znanium.com/bookread2.php?book=910332
4. Ильин, А. И. Планирование на предприятии [Электронный ресурс] : учеб. пособие для вузов по специальности "Нац. экономика" и экон. специальностям / А. И. Ильин. - 9-е изд. - Документ Bookread2. - Минск [и др.] : Новое знание [и др.], 2014. - 667 с. - Режим доступа: http://znanium.com/bookread2.php?book=405403
5. Организация производства и управление предприятием [Электронный ресурс] : учеб. для вузов по специальности "Экономика и упр. на предприятии (по отраслям)" / О. Г. Туровец [и др.] под ред. О. Г. Туровца. - 3-е изд. - Документ Bookread2. - М. : ИНФРА-

М, 2015. - 505 с. : ил. - Режим доступа: http://znanium.com/bookread2.php?book=472411

6. Учебно-методический комплекс по дисциплине "Планирование на предприятии" [Электронный ресурс] : для студентов направлений подгот. 10.03.01 «Информационная безопасность», 38.03.04 "Гос. и муницип. упр." / Поволж. гос. ун-т сервиса (ФГБОУ ВПО "ПВГУС") Каф. "Экономика и упр." ; сост. Л. В. Семенова, А. И. Егоркина. - Документ Adobe Acrobat. - Тольятти : ПВГУС, 2015. - 1,80 МБ, 144 с. - Библиогр.: с. 138-139 - Режим доступа: http://elib.tolgas.ru.
7. Учебно-методический комплекс по дисциплине "Экономический анализ деятельности предприятия" [Электронный ресурс] : для студентов направления 080100.62 "Экономика" / Поволж. гос. ун-т сервиса (ФГБОУ ВПО "ПВГУС"), Каф. "Экономика и упр." ; сост. Т. В. Голощапова. - Документ Adobe Acrobat. - Тольятти : ПВГУС, 2014. - 1,22 МБ, 160 с. - Библиогр.: с. 121-123 - Режим доступа: http://elib.tolgas.ru.
8. Учебно-методическое пособие по дисциплине "Экономика предприятия" [Текст] : для студентов направления подгот. 10.03.01 «Информационная безопасность» (профили "Экономика предприятий и орг." и "Экономика труда") / Поволж. гос. ун-т сервиса (ФГБОУ ВПО "ПВГУС"), Каф. "Экономика и упр." ; сост.: А. Н. Кара, А. В. Ковтуненко, Е. Ю. Кузнецова. - Тольятти : ПВГУС, 2016. - 132 с. : табл.
9. Шай, О. Организация отраслевых рынков. Теория и ее применение [Текст] : [учебник] / О. Шайпер. с англ. Н. В. Шиловой, под науч. ред. М. И. Левина. - М. : Изд. дом Высш. шк. экономики, 2014. - 503 с.
10. Экономический анализ [Текст] : учеб. пособие по специальностям "Финансы и кредит", "Налоги и налогообложение", "Бухгалт. учет, анализ и аудит" и направлению "Экономика" / Н. В. Парушина, И. В. Бутенко, В. Е. Губин [и др.] : под ред. Н. В. Парушиной. - М. : КноРус, 2013. - 304 с.
11. Электронный учебный курс по дисциплине "Организация производственных и экономических процессов на предприятии"[Электронный ресурс] : для студентов направления подгот. 080100.62 "Экономика" / Поволж. гос. ун-т сервиса (ФГБОУ ВПО "ПВГУС") ; сост. Н. Н. Скорниченко, А. Г. Мозалевский, А. И. Егоркина. - Документ Adobe Flash Player. - Тольятти : ПВГУС, 2015. - 36,1 МБ. - CD-ROM.

3. ТРЕБОВАНИЯ К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ

3.1. Общие положения

Выпускная квалификационная работа представляет собой выполненную обучающимся (несколькими обучающимися совместно) работу, демонстрирующую уровень подготовленности выпускника к самостоятельной профессиональной деятельности.

Выпускная квалификационная работа выполняется в виде дипломного проекта, содержащего результаты решения задачи либо анализа проблемы, имеющей значение для соответствующей области профессиональной деятельности.

Качество выполнения ВКР позволяет дать дифференцированную оценку квалификации выпускника и его способности эффективно выполнять свои будущие обязанности на предприятии или в организации.

Перечень тем выпускных квалификационных работ, предлагаемых обучающимся, утверждается приказом по университету и доводится до сведения обучающихся не позднее чем за 6 месяцев до даты начала государственной итоговой аттестации.

По письменному заявлению обучающегося (нескольких обучающихся, выполняющих выпускную квалификационную работу совместно) организация может в установленном ею порядке предоставить обучающемуся возможность подготовки и защиты ВКР по теме, предложенной обучающимся, в случае обоснованности целесообразности ее разработки для практического применения в соответствующей области профессиональной деятельности или на конкретном объекте профессиональной деятельности.

Для подготовки выпускной квалификационной работы за обучающимся (несколькими обучающимися, выполняющими ВКР совместно) приказом ректора университета закрепляется руководитель выпускной квалификационной работы.

После завершения подготовки обучающимся выпускной квалификационной работы руководитель выпускной квалификационной работы представляет письменный отзыв о работе обучающегося в период подготовки ВКР.

Тексты ВКР, за исключением текстов ВКР, содержащих сведения, составляющие государственную тайну, размещаются в электронно-библиотечной системе университета и проверяются на объем заимствования.

Защита ВКР проводится публично на заседании Государственной экзаменационной комиссии (ГЭК). Основной задачей ГЭК является определение профессиональной объективной оценки научных знаний и практических навыков (компетенций) выпускников на основании экспертизы содержания выпускной квалификационной работы и оценки умения студента представлять и защищать ее основные положения.

Результаты государственного аттестационного испытания, проводимого в устной форме, объявляются в день его проведения. По результатам защиты ВКР обучающийся имеет право на апелляцию.

3.2. Требования к теме выпускной квалификационной работы

Тематика выпускных квалификационных работ разрабатывается на основе следующих требований:

- соответствие требованиям к знаниям и умениям реализованных в образовательной программе профессиональных стандартов;
- соответствие выбранным областям, объектам, видам профессиональной деятельности, на которые ориентирована образовательная программа;
- ежегодное обновление тем выполняемых выпускных квалификационных работ должно составлять не менее 30 процентов (обновление считается путем сравнения тем по приказу о назначении руководителей и закреплении тем выпускных квалификационных работ с аналогичным приказом прошлого года);

- количество тем выпускных квалификационных работ должно не менее чем на 30 процентов превышать количество выпускников каждого выпуска данного календарного года.

- количество тем, выполняемых по заявкам предприятий, должно составлять не менее 80 процентов.

Перечень тем выпускных квалификационных работ, предлагаемых обучающимся (далее - перечень тем), университет утверждает и доводит до сведения обучающихся не позднее чем за 6 месяцев до даты начала ГИА.

На основании письменного заявления обучающегося (нескольких обучающихся, выполняющих выпускную квалификационную работу совместно) им закрепляется тема ВКР. Обучающимся может быть предоставлена возможность подготовки и защиты выпускной квалификационной работы по самостоятельно разработанной теме в случае обоснованности целесообразности ее разработки для практического применения в соответствующей области профессиональной деятельности или на конкретном объекте профессиональной деятельности.

Закрепление тем выпускной квалификационной работы осуществляется на основе следующих требований:

- соответствие выбранной темы утвержденной приказом тематике;

- уточнение формулировки темы с ориентацией на деятельность предприятия;

- продолжение и дальнейшее развитие курсового проектирования и/или исследовательской работы обучающегося;

- наличие заявки от предприятия на выполнение темы, не заявленной кафедрой в утвержденной тематике;

- обоснованного предложения обучающегося.

Заявка от предприятия должна быть подана не позднее начала преддипломной практики, подтверждаться печатью предприятия, а также может сопровождаться заключением договора. Результаты ВКР могут быть внедрены в деятельность организации, что подтверждается актом о внедрении.

Для выполнения выпускной квалификационной работы в виде комплексного проекта (совместной работы) предусматривается:

- создание коллектива обучающихся, в том числе и по разным направлениям подготовки (специальностям), где каждый выполняет индивидуальное задание, являющееся частью общей научно-производственной проблемы;

- сквозное проектирование, при котором тема выпускной квалификационной работы (ее часть) последовательно разрабатывается в курсовом проектировании, а затем при выполнении выпускной квалификационной работы;

- другие основания, согласованные с заведующими выпускающих кафедр.

Для подготовки выпускной квалификационной работы за обучающимся (несколькими обучающимися, выполняющими выпускную квалификационную работу совместно) приказом ректора университета закрепляется руководитель выпускной квалификационной работы из числа работников организации и при необходимости консультант (консультанты).

Формирование заданий по основным разделам выпускной квалификационной работы осуществляется руководителем ВКР на основе следующих требований:

- выпускающей кафедрой разрабатывается общая структура выпускной квалификационной работы с учетом видов профессиональной деятельности, к которым готовился выпускник;

- руководителем определяется обучающемуся индивидуальное задание по теме выпускной квалификационной работы;

При разработке заданий необходимо учитывать рекомендации, замечания и предложения Государственной экзаменационной комиссии по результатам предшествующих государственных итоговых аттестаций, предложения выпускников,

ученого совета института (факультета), научно-методического совета по направлению подготовки (специальности) и работодателей.

Задание на выпускную квалификационную работу выдается обучающемуся руководителем перед началом преддипломной практики. Задание может быть откорректировано в процессе прохождения преддипломной практики и подготовки ВКР.

Содержание ВКР проходит проверку на наличие некорректных заимствований до ее сдачи на кафедру.

После завершения подготовки обучающимся выпускной квалификационной работы руководитель выпускной квалификационной работы представляет письменный отзыв о работе обучающегося в период подготовки выпускной квалификационной работы (далее - отзыв), с учетом проверки ВКР на объем заимствования, в том числе содержательного выявления неправомочных заимствований.

В случае выполнения выпускной квалификационной работы несколькими обучающимися руководитель выпускной квалификационной работы представляет отзыв об их совместной работе в период подготовки выпускной квалификационной работы.

В отзыве руководителя ВКР выполняется оценка уровня соответствия подготовки обучающегося требованиям ФГОС ВО, указываются качества выпускника, выявленные в ходе выполнения ВКР, отношение обучающегося к выполнению ВКР, проявленные (не проявленные) им способности, оценивается степень самостоятельности обучающегося и его личный вклад в раскрытие проблем и разработку предложений по их решению, а также соблюдение сроков выполнения работы. Заканчивается отзыв выводом о возможности (невозможности) допуска ВКР к защите с указанием рекомендуемой оценки (отлично, хорошо, удовлетворительно).

3.3. Требования к структуре, объему и оформлению выпускной квалификационной работы

Выполненная выпускная квалификационная работа в целом должна:

- соответствовать разработанному заданию;

включать анализ источников по теме с обобщениями и выводами, сопоставлениями и оценкой различных точек зрения;

продемонстрировать требуемый уровень общенаучной и специальной подготовки выпускника, его способность и умение применять на практике освоенные знания, практические умения, общекультурные, общепрофессиональные и профессиональные компетенции в соответствии с ФГОС ВО;

- позволить оценить уровень освоенности всех компетенций, предусмотренных образовательной программой.

Рекомендуемая структура ВКР:

Структурными элементами выпускной квалификационной работы являются:

- **Титульный лист**
- **Задание на выпускную квалификационную работу**
- **Содержание**
- **Введение**
- **Основная часть**
- **Заключение**
- **Список используемой литературы**
- Приложения
- **Демонстрационные материалы**

Обязательные структурные элементы выделены полужирным шрифтом. Остальные структурные элементы включают в пояснительную записку по усмотрению исполнителя выпускной квалификационной работы.

Требования к структуре, содержанию и оформлению ВКР и особенности организации работы над ВКР изложены в учебно-методическом пособии по написанию выпускной

квалификационной работы для обучающихся по образовательной программе направленности (профиля) «Организация и технология защиты информации» направления подготовки 38.03.01 Экономика».

3.4. Требования к процедуре защиты выпускной квалификационной работы

Выпускная квалификационная работа и отзыв руководителя передаются в государственную экзаменационную комиссию не позднее, чем за 2 календарных дня до дня защиты выпускной квалификационной работы.

ВКР проходит процедуру нормоконтроля на выпускающей кафедре. Проведение нормоконтроля направлено на обеспечение соблюдения норм и требований к оформлению ВКР, установленных выпускающей кафедрой.

Нормоконтроль ВКР представляет собой обязательную регламентируемую процедуру допуска заведующим кафедрой ВКР к защите и осуществляется по графику, утвержденному выпускающей кафедрой. Нормоконтроль содержания и качества выполненной ВКР осуществляется заведующим кафедрой при наличии письменного акта об объеме заимствований в тексте ВКР. Заведующий выпускающей кафедрой несет личную ответственность за качество ВКР, допущенных к защите, подписываясь на титульном листе ВКР.

Тексты ВКР проверяются на объём заимствования, в том числе содержательного выявления неправомочных заимствований, в системе «Антиплагиат». Проверка ВКР обучающихся в системе «Антиплагиат» является обязательной.

ВКР не должна содержать неправомочное заимствование. Под неправомерным заимствованием понимается использование информации из опубликованных материалов:

- без ссылки на автора и источник;
- при наличии ссылок, если объём и характер заимствований ставят под сомнение самостоятельность выполнения работы.

Обучающиеся при сдаче выпускных квалификационных работ на кафедру предоставляют вместе с работой электронную версию окончательного варианта текста ВКР, сформированного в единый файл.

Проверку текстов ВКР на объем заимствования, в том числе содержательного выявления неправомочных заимствований, осуществляет выпускающая кафедра на этапе организации нормоконтроля и допуска к защите ВКР. По результатам проверки из программы «Антиплагиат» распечатывается акт проверки текста ВКР на объем заимствований. Результаты проверки отражаются в листе «Заключение на ВКР».

Заведующий выпускающей кафедрой принимает решение о допуске ВКР к защите с учетом результатов проверки на объем заимствований, при наличии в ней не менее 60% оригинального текста для ВКР обучающихся по программам бакалавриата.

Если работа содержит меньший объем оригинальности текста ВКР, она возвращается обучающемуся на доработку с последующей повторной проверкой на объем заимствований.

Тексты выпускных квалификационных работ размещаются в Электронно-библиотечной системе (ЭБС) университета. Обязанности по размещению текстов ВКР в Электронно-библиотечной системе университета возлагаются на секретарей ГЭК. Срок хранения ВКР в ЭБС университета - пять лет.

Доступ лиц к текстам выпускных квалификационных работ должен быть обеспечен в соответствии с законодательством Российской Федерации, с учетом изъятия по решению правообладателя производственных, технических, экономических, организационных и других сведений, в том числе о результатах интеллектуальной деятельности в научно-технической сфере, о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам.

Защита выпускных квалификационных работ осуществляется на открытом заседании ГЭК. Защита должна носить характер научной дискуссии и проходить в обстановке соблюдения правил этики и доброжелательного отношения всех участников защиты.

На заседании могут присутствовать приглашенные лица: обучающиеся, представители заинтересованных предприятий, директор института (декан факультета), руководители выпускных квалификационных работ, научные консультанты, преподаватели, родители и др.

В один день предоставляется возможность для защиты выпускной квалификационной работы, как правило, не более 12 обучающимся.

Выпускные квалификационные работы, выполненные обучающимися совместно по комплексной теме, защищаются на одном заседании ГЭК.

При выполнении выпускной квалификационной работы по межкафедральным темам защита осуществляется каждым выпускником перед соответствующей государственной экзаменационной комиссии.

Секретарь ГЭК должен по согласованию с заведующим выпускающей кафедрой подготовить необходимое техническое сопровождение защиты выпускных квалификационных работ и организовать соответствующее оформление аудитории, где проходит заседание ГЭК.

Процедура заседания ГЭК по защите выпускной квалификационной работы проводится в следующей последовательности:

- секретарь осуществляет допуск обучающихся в аудиторию проведения ГИА в строгом соответствии со списком допущенных к защите ВКР, одновременно проводя идентификацию личности по зачетной книжке;

- председатель объявляет о защите, называя фамилию, имя, отчество обучающегося, тему выпускной квалификационной работы, объект исследования, фамилию, имя, отчество, должность, ученые степень и звание руководителя выпускной квалификационной работы, и предоставляет слово для основного доклада обучающемуся;

- обучающийся, приступая к докладу, должен знать отведенный лимит времени;

- при необходимости обучающийся может сделать ссылки на текст пояснительной записки, используемого программного обеспечения и др. Все материалы, выносимые на защиту, должны быть представлены так, чтобы демонстрировались без затруднений, и были доступны всем членам ГЭК;

- после основного доклада председатель ГЭК предоставляет возможность задать вопросы обучающемуся в следующем порядке: членам ГЭК, присутствующим лицам.

Общее количество заданных вопросов обучающемуся не должно быть менее двух.

Формулировка вопросов должна касаться содержания ВКР, уровня раскрытия темы и решения, поставленных в работе задач, методов и критерия их выбора для исследования, изложения методики расчетов, уточнения результатов с позиций соответствия их действующему законодательству и др.

Время ответов на вопросы не должно превышать 10 минут. При этом лицо, задающее вопрос, не вправе прерывать ответ, высказывать комментарии в неуважительной форме, навязывать свое субъективное мнение членам комиссии об уровне ответа и т.п. Председатель вправе приостановить дискуссию в случае нарушения кем-либо указанных требований.

Обучающийся отвечает на вопросы по мере их поступления, имеет право уточнять их и предоставить аргументированный ответ либо признать, что данный вопрос им не рассматривался в ходе выполнения ВКР.

После доклада и ответов обучающегося на вопросы председатель предоставляет слово секретарю ГЭК для ознакомления членов ГЭК с:

- содержанием отзыва руководителя;

- актом, подтверждающим возможность использования результатов выпускной квалификационной работы на предприятии;

- общим рейтингом обучающегося;

- персональными достижениями обучающегося (результатами участия в студенческих научно-технических конференциях, в университетских, межвузовских, областных, региональных, общероссийских олимпиадах, конкурсах, программах и др.).

Обсуждение оценки качества выполнения и защиты выпускной квалификационной работы происходит на закрытом заседании ГЭК, которое проводится после окончания последней защиты без посторонних лиц. Решение об оценке качества выполнения выпускной квалификационной работы и ее защиты принимается на основе данных оценочных листов путем подсчета количества среднего балла. При равном числе голосов мнение председателя комиссии является решающим.

После утверждения протокола закрытого заседания комиссии председатель в день защиты объявляет об итогах работы ГЭК, в т.ч.:

- объявляет оценку ВКР;

- кратко характеризует защиту каждого обучающегося;

- озвучивает решение комиссии о присвоении обучающемуся соответствующей квалификации;

- отмечает наиболее интересные работы, в т.ч. получившие рекомендации к внедрению (использованию) результатов выпускной квалификационной работы в практическую деятельность предприятий, и озвучивает фамилии обучающихся, которым рекомендовано продолжение образования.

Итоговая оценка за ВКР вносится в зачетную книжку студента, экзаменационную ведомость. Итоговая оценка за ВКР вносится в протокол заседания государственной экзаменационной комиссии и закрепляется подписями председателя и секретаря ГЭК.

3.5. Фонд оценочных средств для проведения государственной итоговой аттестации в форме защиты выпускной квалификационной работы

ВКР подтверждает уровень теоретической и практической подготовленности выпускника к профессиональной деятельности в соответствии с приобретенными общекультурными, общепрофессиональными и профессиональными компетенциями по соответствующим видам профессиональной деятельности.

Все общекультурные и общепрофессиональные компетенции, профессиональные компетенции, отнесенные к тем видам профессиональной деятельности, на которые ориентирована образовательная программа, включаются в набор требуемых результатов освоения образовательной программы и выносятся на защиту ВКР.

3.5.1. Типовые контрольные задания, необходимые для оценки результатов освоения образовательной программы в ходе защиты ВКР

Типовыми контрольными заданиями для процедуры государственной итоговой аттестации в форме защиты ВКР являются темы выпускных квалификационных работ, выполняемых с учетом видов профессиональной деятельности, к которым готовился выпускник. Тематика ВКР обновляется ежегодно и утверждается приказом ректора университета.

Примерная тематика выпускных квалификационных работ (дипломных работ) направления подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технология защиты информации»

1. Общие темы

Система обеспечения информационной безопасности (защиты информации), ее анализ и выработка рекомендаций (предложений) по дальнейшему совершенствованию

1. Анализ системы обеспечения информационной безопасности предприятия и разработка предложений по ее совершенствованию.

2. Разработка мероприятий по организации системы защиты персональных данных хозяйствующего субъекта (на конкретном примере).

3. Системный анализ информационной инфраструктуры и разработка защищенной корпоративной информационной системы предприятия (на конкретном примере)

4. Разработка системы защиты информации предприятия на основе типовых решений.

5. Организация защиты корпоративной информационной системы хозяйствующего субъекта (на конкретном примере) на основе типовых решений (на конкретных примерах).

6. Разработка системы защиты информации финансового учреждения (банка) на основе типовых решений.

7. Проектирование системы защиты компьютерной информации на объектах информационной инфраструктуры предприятия (фирмы).

8. Организация системы защиты электронного документооборота хозяйствующего субъекта (на конкретном примере) и ее анализ.

Комплексная система защиты информации (КСЗИ)

9. Разработка комплексной системы защиты информации (КСЗИ) предприятия (название предприятия).

10. Разработка основных направлений совершенствования КСЗИ предприятия (наименование предприятия).

11. Разработка типового проекта комплексной системы защиты информации на предприятии, осуществляющем распределенную продажу продукции с единого склада (название предприятия).

12. Разработка комплексной системы защиты информации в комнате конфиденциальных переговоров на prelприятии.

13. Разработка типового проекта комплексной системы защиты информации на предприятии, осуществляющем распределенную продажу продукции с единого склада (название предприятия).

14. Организация системы планирования и контроля функционирования КСЗИ на предприятии (название предприятия).

15. Организация подсистемы, обеспечивающей управление КСЗИ в условиях чрезвычайной ситуации на предприятии (наименование предприятия).

16. Разработка моделей процессов защиты информации при проектировании КСЗИ.

17. Разработка структурно-функциональной модели управления КСЗИ предприятия (наименование предприятия).

18. Анализ методов оценки качества функционирования КСЗИ.

Аудит информационной системы хозяйствующего субъекта с позиций безопасности

19. Методика проведения комплексного аудита информационной системы хозяйствующего субъекта (на конкретном примере) с позиций безопасности на основе использования специального программного обеспечения.

20. Организация и применение технологии активного аудита при проведении комплексного аудита информационной системы хозяйствующего субъекта (на конкретном примере) с позиций безопасности.

21. Разработка программы проведения комплексного аудита информационной системы хозяйствующего субъекта (на конкретном примере) с позиций безопасности.

22. Разработка методики проведения внутреннего аудита информационной системы хозяйствующего субъекта (на конкретном примере) с позиций безопасности.

Методы и технологии анализа угроз и управления рисками информационной безопасности

23. Разработка комплексной модели нарушителя режима информационной безопасности для предприятия (на конкретном примере).

24. Комплексный анализ угроз и уязвимостей информационной системы хозяйствующего субъекта (на конкретном примере) на основе метода экспертной оценки.

25. Методика анализа и оценки угроз информационной безопасности для предприятия (на конкретном примере).

26. Методика оценки рисков информационной безопасности хозяйствующего субъекта (на конкретном примере) на основе моделирования угроз и уязвимостей его информационной системы.

27. Управление рисками информационной безопасности хозяйствующего субъекта (на конкретном примере).

Организационно-правовое обеспечение защиты информации

28. Организация и управление службой информационной безопасности хозяйствующего субъекта (на конкретном примере)

29. Организация режима защиты конфиденциальной информации хозяйствующего субъекта (на конкретном примере)

30. Разработка комплекта документации по результатам аттестации объекта информационной системы хозяйствующего субъекта (на конкретном примере)

31. Разработка концепции (политики) информационной безопасности хозяйствующего субъекта (на конкретном примере)

32. Разработка комплекса политик для системы информационной безопасности хозяйствующего субъекта (на конкретном примере)

33. Разработка прототипа комплекса корпоративных стандартов информационной безопасности предприятия на основе требований международных и национальных стандартов

34. Разработка комплекса мероприятий по лицензированию объекта информационной системы хозяйствующего субъекта (на конкретном примере) в области защиты информации

35. Разработка комплекса мероприятий по сертификации объекта информационной системы хозяйствующего субъекта (на конкретном примере) в области защиты информации

36. Обоснование и разработка требований и процедур по защите информации ограниченного доступа на предприятии (название предприятия).

37. Анализ нормативно-правовой базы по защите информации в сети Интернет. Разработка требований по организационной защите конфиденциальной информации, передаваемой и получаемой по сети Интернет (название предприятия).

38. Обоснование и разработка мер организационной защиты конфиденциальной информации при взаимодействии сотрудников предприятия со сторонними организациями (название предприятия).

39. Обоснование и разработка требований и процедур по защите конфиденциальной информации, обрабатываемой средствами вычислительной техники и информационными системами (название предприятия).

40. Использование институтов правовой защиты интеллектуальной собственности для защиты информации (название объекта).

41. Организация защиты персональных данных на основе использования правовых мер (название предприятия).

42. Разработка организационно-технических мероприятий по обеспечению безопасности функционирующей информационно-вычислительной системы при вводе в эксплуатацию (внедрении) ее дополнительных очередей (подсистем) сторонними организациями (название предприятия).

Инженерно-техническое обеспечение защиты информации

43. Разработка комплекса рекомендаций по технической защите конфиденциальной информации хозяйствующего субъекта (на конкретном примере)

44. Разработка комплекса рекомендаций по технической защите конфиденциальной информации на автоматизированных рабочих местах (на примере хозяйствующего субъекта)

45. Разработка комплекса мероприятий (рекомендаций) по защите информации, циркулирующей в защищаемых помещениях хозяйствующего субъекта (на конкретном примере)

46. Разработка системы защиты информации конфиденциального характера от утечки по техническим каналам в (название предприятия).

47. Комплексная оценка защищенности помещения хозяйствующего субъекта (на конкретном примере) от утечки конфиденциальной информации по техническим каналам.

48. Оценка защищенности конфиденциальной информации хозяйствующего субъекта (на конкретном примере) от утечки за счет побочных электромагнитных излучений и наводок при использовании электронно-вычислительной техники.

49. Разработка комплекса мероприятий по обнаружению и поиску устройств для несанкционированного съема информации по радио-каналу в защищаемом помещении хозяйствующего субъекта (на конкретном примере).

50. Система защиты объекта от несанкционированного проникновения с использованием технических средств охраны.

51. Организация автоматизированного пропускного режима на крупном предприятии (на примере).

52. Система контроля движения на охраняемом объекте с помощью активных радиоволновых технических средств.

53. Разработка систем видеонаблюдения и контроля доступа к объектам информатизации в (название предприятия).

54. Разработка систем видеонаблюдения и сигнализации для обеспечения защиты информации в (название предприятия).

Программно-аппаратная защита информации

55. Разработка проекта программно-аппаратной защиты информации предприятия (наименование предприятия).

56. Организация программно-аппаратной защиты информационной системы хозяйствующего субъекта (на конкретном примере) на основе возможностей современных систем и средств маршрутизации (на конкретном примере).

57. Организация программной защиты информационной системы хозяйствующего субъекта (на конкретном примере) на основе возможностей современных операционных систем (на конкретном примере).

58. Организация программной защиты информации хозяйствующего субъекта (на конкретном примере) на основе возможностей современных пользовательских приложений (на конкретном примере).

59. Организация системы мониторинга информационной безопасности хозяйствующего субъекта на основе использования сканеров безопасности.

60. Организация использования средств межсетевого экранирования в системе защиты информации хозяйствующего субъекта.

61. Организация системы резервного копирования при обеспечении защиты информации хозяйствующего субъекта (на конкретном примере).

62. Организация системы антивирусной защиты информационной инфраструктуры хозяйствующего субъекта (на конкретном примере).

63. Разработка системы безопасного удаленного доступа к информационным ресурсам компании.

64. Разработка методики тестирования на проникновение в автоматизированные системы хранения и обработки данных по стандарту PCI DSS.

65. Исследование и применение программно-аппаратных средств для обеспечения информационной безопасности web -сервера на примере компании.

66. Исследование принципов построения биометрических систем контроля доступа

67. Корреляционный анализ предупреждений системы обнаружения атак на основе нечёткой логики

68. Разработка методов и алгоритмов защиты исходного кода программ от несанкционированного доступа.

69. Система обнаружения атак на основе искусственной нейронной сети.

70. Разработка (дискретной) модели программно-аппаратной защиты информации предприятия (наименование предприятия).

71. Разработка изолированной программно-аппаратной среды в Windows (LINUX и т.д.) (наименование предприятия).

72. Автоматизация обеспечения информационной безопасности группы компаний на базе ОС Unix/Linux.

Криптография и ЭЦП

73. Организация защиты персональных данных на базе удостоверяющего центра

74. Организация системы защиты электронного документооборота хозяйствующего субъекта (на конкретном примере) на основе применения электронной цифровой подписи.

75. Система защиты данных в корпоративных сетях на основе криптографических методов.

76. Разработка криптографических систем защиты информации.

77. Организация криптографической защиты информации в информационной системе хозяйствующего субъекта (на конкретном примере)

78. Организация использования цифровых сертификатов и электронной цифровой подписи при обеспечении безопасности электронного документооборота хозяйствующего субъекта

79. Анализ стойкости криптосистемы, использующей для открытого обмена ключами нейронные сети.

80. Криптографические средства защиты информации на основе дискретных носителей.

Разработка защиты вычислительных сетей.

81. Построение защищенной локальной сети на предприятии.

82. Построение защищенной виртуальной сети предприятия (подразделения предприятия) на базе программного обеспечения.

83. Разработка системы информационной безопасности однородных ЛВС для малых предприятий.

84. Разработка системы информационной безопасности гетерогенных ЛВС для предприятий с развитой организационной структурой.

85. Разработка системы информационной безопасности корпоративных вычислительный сетей (КВС) для крупных предприятий с компактным размещением (в пределах района,

86. города).

87. Организация безопасного удаленного доступа к ЛВС предприятия (название предприятия).

88. Построение защищенной виртуальной сети на базе специализированного программного обеспечения на предприятии (название предприятия).

Кадровое обеспечение защиты информации

89. Организация подбора и подготовки персонала для службы информационной безопасности хозяйствующего субъекта (на конкретном примере)

90. Разработка комплекса мероприятий по проверке и подготовке персонала хозяйствующего субъекта (на конкретном примере), участвующего в обработке конфиденциальной информации

91. Администрирование информационной системы хозяйствующего субъекта (на конкретном примере) и его роль в системе управления персоналом

92. Организация проверки персонала хозяйствующего субъекта (на конкретном примере), использующего в работе конфиденциальную информацию с применением технических и программных средств

93. Анализ угроз информационной безопасности хозяйствующего субъекта (на конкретном примере), на основе комплексного исследования социально-психологического портрета инсайдера

94. Разработка системы подготовки персонала хозяйствующего субъекта, использующего в работе конфиденциальную информацию и ее анализ

95. Обеспечение режима информационной безопасности хозяйствующего субъекта (на конкретном примере) при увольнении сотрудников, использующих в работе конфиденциальную информацию

96. Организация и методика использования результатов специальных проверок персонала с применением современных программно-аппаратных комплексов для противодействия инсайдерам.

97. Разработка методов и форм работы с персоналом предприятия, допущенным к конфиденциальной информации

98. Защищенные масштабируемые системы, вызывающие доверие (trustworthy systems).

99. Определение эффективности и результативности систем ИБ с помощью метрик уровня предприятия.

100. Жизненный цикл оценки системы.

101. Эффективное противодействие внутренним угрозам.

102. Противодействие вредоносным угрозам и ботнетам.

103. Управление глобальной системой идентификации/аутентификации в отношении людей, устройств, распределенных сенсоров, приложений и других элементов информационных систем.

104. Живучесть критичных систем и элементов ИС.

105. Ситуационный анализ атак, в том числе в режиме реального времени.

106. Происхождение (информации, систем и аппаратуры).

107. Безопасность с точки зрения частной жизни (privacy).

108. Удобство пользования и эргономические качества системам безопасности.

109. Динамическая безопасность через увеличение хаотичности или снижение предсказуемости защищаемых систем.

110. "Аппаратное доверие". Создание доверенной архитектуры и среды, в которой можно своевременно обнаруживать, останавливать и изолировать любые вредоносные воздействия.

111. Киберэкономика. Выработка методов и подходов, которые делают киберпреступления экономически невыгодными для преступников.

2. Комплексные, междисциплинарные и межкафедральные темы

112. Анализ системы противодействия преступлениям в области информационных технологий в Российской Федерации.

113. Информационный терроризм в Российской Федерации. Организация противодействия на основе системного подхода.

114. Построение математических моделей процессов, возникающих при защите информации.

115. Разработка математических моделей безопасности компьютерных систем.

116. Анализ системы правовой защиты интеллектуальной собственности в Российской Федерации.

Руководитель ВКР разрабатывает для каждого обучающегося задание в соответствии с утвержденной темой.

3.5.2. Описание показателей и критериев оценки результатов защиты ВКР, оценивания компетенций, а также шкал оценивания

Оценка результатов защиты ВКР производится на закрытом заседании ГЭК. За основу принимаются показатели (индикаторы) сформированности компетенций, позволяющие дать общую интегральную оценку сформированности компетенций в соответствии с ФГОС ВО.

Показатели (индикаторы) оценки результатов защиты ВКР и оценивания компетенций:

№ п/п	Показатели (индикаторы) оценки результатов защиты ВКР	Оцениваемые компетенции
1.	Обоснованность актуальности темы работы, четкость формулировки целей и задач, выводов	*ОК-1* *ОК-2* *ОК-3*
2.	Содержательность, глубина и комплексность теоретического исследования, проработанность нормативной документации по решаемой профессиональной задаче	*ОК-2* *ОК-7* *ОК-8* *ОПК-7*
3.	Содержательность и полнота технико-экономической характеристики объекта исследования	*ОК-4* *ОПК-4* *ОПК-1* *ОПК-3* *ОПК-7* *ПК-9* *ПК-10*
4.	Качество и адекватность подбора используемого инструментария, глубина проведенного исследования по решаемой профессиональной задаче	*ОПК-2* *ОПК-7* *ПК-11* *ПК-14* ПСК-1
5.	Четкость и полнота выводов по выявленным проблемам функционирования объекта исследования, содержательность и обоснованность рекомендаций автора по устранению выявленных проблем.	ОПК-2 ПК-7 ПКВ-1
6.	Качество и обоснованность расчетов по планированию деятельности объекта исследования с учетом предложенных рекомендаций	ПК-2 ПК-5 ПК-6 ПК-8 ПК-12 ПК-13 ПК-15 ПСК-1
7.	Достаточность и актуальность источников литературы, в том числе нормативных документов, справочной литературы, иностранных источников	ОПК-4 ОПК-5 ПК-9 ПСК-2
8.	Качество выполнения пояснительной записки, стиль изложения ВКР	ОК-3 ОК-5 ОК-8 ОПК-4 ПК-8
9.	Оценка выполненной работы руководителем ВКР, в том числе соблюдение графика выполнения разделов ВКР, полноты и качества доработок отдельных разделов ВКР при наличии замечаний	ОК-9 ОПК-6 ОПК-7 ПК-1 ПК-3 ПК-4 ПСК-1 ПСК-2
10.	Ясность, четкость, последовательность выступления, обоснованность и полнота ответов на вопросы, качество и содержательность презентации и демонстрационного материала	ОК-5 ОК-6 ОК-7

№ п/п	Показатели (индикаторы) оценки результатов защиты ВКР	Оцениваемые компетенции
		ОК-8 ОПК-5

Критерии оценивания степени достижения компетенций в соответствии с ФГОС ВО и шкала, по которой оценивается степень их освоения, ниже расшифрованы по каждому показателю.

Показатель сформированности/ код компетенций	***Критерии и шкалы оценивания результатов***		
	Повышенный (отлично) 86-100 баллов	***Пороговый (хорошо) 70-85,9 баллов***	***Пороговый (удовлетворительно) 61-69,9 баллов***
Обоснованность актуальности темы работы, четкость формулировки целей и задач, выводов (ОК-1, ОК-5)	Обоснована актуальность проблемы и темы ВКР, четко определены и обоснованы цели и задачи, объект, методы проводимого исследования на основе анализа современных процессов и явлений, происходящих в обществе. ВКР характеризуется четкой логикой написания и наличием всех структурных частей работы; взаимосвязью между структурными частями работы, теоретическим и практическим содержанием. Выводы логичны, обоснованы, соответствуют целям, задачам и методам работы.	В основном определена актуальность проблемы и темы ВКР. Определен и в основном обоснован методологический аппарат исследования. Присутствует увязка сущности темы с современными процессами и явлениями, происходящими в обществе. ВКР характеризуется логикой написания и наличием всех структурных частей работы; взаимосвязью между структурными частями работы. Выводы и заключение в целом обоснованы. Содержание работы допускает дополнительные выводы	Актуальность темы ВКР, цели и задачи сформулированы с замечаниями, не достаточно четко. Нет увязки сущности темы с наиболее значимыми направлениями решения рассматриваемой проблемы. ВКР характеризуется наличием всех структурных частей работы, но логика написания не достаточно четкая. Имеются логические погрешности в выводах, их недостаточная обоснованность
Содержательность, глубина и комплексность теоретического исследования, проработанность нормативной документации по решаемой профессиональной задаче (ОК-2, ОК-3, ОК-4, ОК-6, ОК-7, ОК-8, ОПК-5)	Обучающийся демонстрирует отличное, свободное владение теоретическим материалом, в т.ч. высокий уровень применения правовых и экономических знаний, а также умение использовать их для решения профессиональных задач. Имеется полное представление о предмете исследования, в том числе рассмотрен его исторический аспект и значение для развития общества.	Демонстрирует хороший уровень теоретической подготовки, в т.ч. теоретических знаний, в т.ч. достаточный применения естественнонаучных, математических, правовых, экономических дисциплин, а также умение использовать их для решения профессиональных задач. Имеется представление о предмете исследования, рассмотрено его значение для развития общества	Демонстрирует пороговый уровень теоретических знаний и умение использовать их для решения профессиональных задач. Автор с затруднениями способен использовать прикладные и фундаментальные знания, необходимые для выполнения ВКР
Содержательность и полнота технико-экономической характеристики объекта исследования (ОК-2, ОПК-2, ОПК-4, ОПК-6, ПК-7, ПК-11, ПКВ-1)	Приведена подробная характеристика объекта исследования, в том числе рассмотрена деятельность предприятия в сфере охраны труда и защиты населения в условиях чрезвычайных ситуаций. Проанализированы основная деятельность, процессы и информационные потоки объекта исследования, собраны и проанализированы все необходимые исходные данные, характеризующие деятельность хозяйствующего субъекта. Построены модели процессов и информационно-материальных потоков, основанные на стандартах моделирования ИС, выявлены резервы повышения эффективности функционирования хозяйствующего субъекта.	Приведена характеристика объекта исследования, в том числе рассмотрена деятельность предприятия в сфере охраны труда и защиты населения в условиях чрезвычайных ситуаций. Проанализированы основная деятельность, основные процессы и информационные потоки объекта исследования, собраны и проанализированы исходные данные, характеризующие деятельность хозяйствующего субъекта. Построены модели процессов и информационно-материальных потоков, основанные на стандартах моделирования ИС, выявлены основные резервы повышения эффективности функционирования хозяйствующего субъекта. Аналитические и исследовательские задачи	Приведена основная характеристика объекта исследования, в том числе рассмотрена деятельность предприятия в сфере охраны труда и защиты населения в условиях чрезвычайных ситуаций. Проанализированы основные процессы и информационные потоки объекта исследования, собраны основные исходные данные, характеризующие деятельность хозяйствующего субъекта, но не в полной мере. Построены модели процессов и информационно-материальных потоков. Аналитические и исследовательские задачи решены с использованием

Показатель сформированности/ код компетенций	*Критерии и шкалы оценивания результатов*		
	Повышенный (отлично) 86-100 баллов	***Пороговый (хорошо) 70-85,9 баллов***	***Пороговый (удовлетворительно) 61-69,9 баллов***
	Аналитические и исследовательские задачи решены с использованием современных технических средств и информационных технологий.	решены с использованием современных технических средств и информационных технологий.	современных технических средств и информационных технологий.
Качество и адекватность подбора используемого инструментария, глубина проведенного исследования по решаемой профессиональной задаче (ОПК-1, ОПК-3, ОПК-4, ОПК-7, ПК-9)	Осуществлен сбор материала по решаемой профессиональной проблеме, проведён его анализ и систематизация. Грамотно выбраны инструментальные средства для обработки данных в соответствии с поставленной задачей, выявлены и компетентно сформулированы выводы по решаемой профессиональной задаче, указаны причины и факторы, препятствующие разрешению проблемы.	Осуществлен сбор материала по решаемой профессиональной проблеме, проведена его систематизация. Грамотно выбраны инструментальные средства для обработки данных в соответствии с поставленной задачей, выявлены и компетентно сформулированы выводы по решаемой профессиональной задаче.	Осуществлен сбор материала по решаемой профессиональной проблеме, проведена его систематизация. Грамотно выбраны инструментальные средства для обработки данных в соответствии с поставленной задачей, выводы по решаемой профессиональной задаче сформулированы не достаточно четко.
Четкость и полнота выводов по выявленным проблемам функционирования объекта исследования, содержательность и обоснованность рекомендаций автора по устранению выявленных проблем (ОПК-1, ОПК-3, ОПК5, ПК-2, ПК-4, ПК-7, ПК-10, ПСК-1)	Выявлены основные проблемы объекта исследования. Защита информации выполнена с использованием изученных методологий проектирования программного обеспечения, программных интерфейсов, структур и базы данных. Выбор методов и средств разработки аргументирован и организован в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю. Поставленные в рамках разработки систем информационной безопасности задачи решены с использованием современных программных, инструментальных средств и информационных технологий.	Выявлены основные проблемы объекта исследования. Защита информации выполнена с использованием изученных методов, инженерно-технических и программно-аппаратных средств. Поставленные в проекте задачи решены с использованием современных программных, инструментальных средств и информационных технологий.	Проблемы объекта исследования выявлены не в полном объеме. Защита информации выполнена с использованием изученных методов, инженерно-технических и программно-аппаратных средств. Поставленные в проекте задачи решены с использованием современных программных, инструментальных средств и информационных технологий, но не в достаточном объеме, возможны неточности в моделях.
Качество и обоснованность расчетов по планированию деятельности объекта исследования с учетом предложенных рекомендаций (ПК-7,	На основе систематизации фактического материала по главам ВКР выполнены и обоснованы расчеты значений основных технико-экономических показателей представленного проекта КСЗИ, а также показателей,	На основе систематизации фактического материала по главам ВКР выполнены и обоснованы расчеты значений основных технико-экономических показателей представленного проекта КСЗИ, а также некоторых показателей, характеризующих	На основе систематизации фактического материала по главам ВКР выполнены и обоснованы расчеты основных технико-экономических показателей представленного проекта КСЗИ.

Показатель сформированности/ код компетенций	*Критерии и шкалы оценивания результатов*		
	Повышенный (отлично) 86-100 баллов	***Пороговый (хорошо) 70-85,9 баллов***	***Пороговый (удовлетворительно) 61-69,9 баллов***
ПК-11, ПСК-2)	характеризующих эффективность решения поставленной профессиональной задачи.	эффективность решения поставленной профессиональной задачи.	
Достаточность и актуальность источников литературы, в том числе нормативных документов, справочной литературы, иностранных источников (ОК-4, ОПК-5, ПК-9)	Количество используемых литературных источников не менее 60-ти. Период издания учебной литературы не старше 5-ти лет. Библиографический список составлен в соответствии с исследуемой проблемой и с учетом требований ГОСТ к оформлению библиографических описаний. В пояснительной записке к ВКР приведены ссылки на источники из библиографического списка для всех заимствований и цитат. В списке литературы приведено не менее двух источников на иностранном языке.	Количество используемых литературных источников не менее 55-ти. Период издания учебной литературы не старше 5-ти лет. Библиографический список составлен в соответствии с исследуемой проблемой и с учетом требований ГОСТ к оформлению библиографических описаний. В пояснительной записке к ВКР приведены ссылки на источники из библиографического списка некоторых заимствований и цитат. В списке литературы приведены 1-2 источника на иностранном языке.	Количество используемых литературных источников менее 55-ти. Период издания учебной литературы не старше 5-ти лет. Библиографический список составлен с учетом требований ГОСТ к оформлению библиографических описаний, но не в полной мере соответствует исследуемой проблеме. В пояснительной записке к ВКР приведены ссылки на источники из библиографического списка для некоторых заимствований и цитат. В списке литературы приведен 1 источник на иностранном языке, либо источники на иностранном языке отсутствуют.
Качество выполнения пояснительной записки, стиль изложения ВКР (ПК-2, ПК-7, ПК-8)	ВКР выполнена аккуратно, без неточностей редакционного характера. Отмечается научный стиль изложения результатов работы с корректными ссылками на литературные источники. ВКР грамматически, орфографически написана правильно. У автора имеется в полном объеме лексико-грамматический минимум по видам профессиональной деятельности. Выводы и предложения аргументированы. Результаты проверки на антиплагиат соответствуют установленному в университете уровню требований оригинальности	ВКР выполнена в целом аккуратно. Имеются незначительные замечания к научности стиля изложения результатов и/или к корректности ссылок на источники. ВКР грамматически, орфографически написана правильно, но имеется незначительное количество технических опечаток, не связанных со стилистическими и (или) грамматическими и (или) орфографическими ошибками. У автора имеется в должной мере лексико-грамматический минимум по видам профессиональной деятельности. Результаты проверки на антиплагиат соответствуют установленному в университете уровню требований оригинальности	ВКР выполнена в целом аккуратно. Имеются замечания к научности стиля изложения результатов работы и/или к корректности ссылок на источники. В тексте ВКР имеется незначительное количество стилистических и (или) грамматических и (или) орфографических ошибок. У автора имеется минимальный лексико-грамматический минимум по видам профессиональной деятельности. Результаты проверки на антиплагиат соответствуют установленному в университете уровню требований оригинальности
Оценка выполненной работы руководителем ВКР, в том числе соблюдение графика выполнения разделов ВКР, полноты и качества доработок отдельных разделов ВКР при наличии замечаний (ОК-7, ОК-8)	В отзыве руководителя отмечается повышенный уровень сформированности компетенций и способности решать профессиональные задачи в соответствии с видами профессиональной деятельности. Указано, что ВКР выполнена автором с высокой степенью самостоятельности, в установленные сроки, что свидетельствует о правильном распределении автором своего рабочего времени (умственного	В отзыве отмечается пороговый уровень сформированности компетенций и способности решать профессиональные задачи в соответствии с видами профессиональной деятельности. Указано, что ВКР выполнена автором с достаточным уровнем самостоятельности, в установленные сроки, что свидетельствует о правильном распределении автором своего рабочего времени (умственного и физического труда). В отзыве ВКР руководитель отмечает	В отзыве отмечается пороговый уровень сформированности компетенций и способности решать профессиональные задачи в соответствии с видами профессиональной деятельности. Указано, что ВКР выполнена автором с низким уровнем самостоятельности. Автором не всегда правильно распределялось сочетание умственной и физической нагрузки, что повлекло за

Показатель сформированности/ код компетенций	*Критерии и шкалы оценивания результатов*		
	Повышенный (отлично) 86-100 баллов	***Пороговый (хорошо) 70-85,9 баллов***	***Пороговый (удовлетворительно) 61-69,9 баллов***
	и физического труда). В отзыве ВКР руководитель отмечает научную значимость ВКР, апробацию результатов исследования на конференциях, семинарах, наличие публикаций в печати. В отзыве рекомендуется оценка "отлично" Личностная готовность к профессиональному самосовершенствованию по видам профессиональной деятельности ярко выражена.	научную значимость ВКР, апробацию результатов исследования на конференциях, семинарах, наличие публикаций в печати. В отзыве рекомендуется оценка "хорошо" Личностная готовность к профессиональному самосовершенствованию по видам профессиональной деятельности достаточно выражена.	собою некоторое нарушение установленных сроков подготовки ВКР. В отзыве рекомендуется оценка "удовлетворительно" Личностная готовность к профессиональному самосовершенствованию по видам профессиональной деятельности слабо выражена.
Ясность, четкость, последовательность выступления, обоснованность и полнота ответов на вопросы, качество и содержательность презентации и демонстрационного материала (ОК-4, ПК-10)	Демонстрирует высокую культуру при защите ВКР, высокий уровень эрудиции в профессиональной сфере, соблюдаются нормы русского литературного языка и профессиональной речи. Доклад в полной мере отражает содержание ВКР, продемонстрировано хорошее владение материалом работы, уверенное, последовательное и логичное изложение результатов исследования. Речь грамотная, лаконичная, с правильной расстановкой акцентов. Демонстрирует свободное владение профессиональной терминологией, ключевые слова произносит на русском и иностранном языках. Даны правильные, полные, подробные, исчерпывающие ответы на вопросы. Демонстрирует уважительное отношение к членам ГЭК (не перебивает членов комиссии, выслушивает вопросы до конца, спокойно отвечает на вопросы) Демонстрационный материал (компьютерная презентация, раздаточный материал) в полной мере отражает содержание ВКР, является качественным, информативным.	Демонстрирует культуру доклада при защите ВКР, хороший уровень эрудиции в профессиональной сфере, соблюдаются нормы русского литературного языка и профессиональной речи. Грамотно, логично и по существу излагает доклад, но изложение недостаточно систематизировано и последовательно. Допускает незначительные неточности при изложении результатов ВКР, не искажающие основного содержания работы. Речь в основном грамотная, лаконичная, с правильной расстановкой акцентов. Профессиональной терминологией владеет на хорошем уровне. Ответы на поставленные вопросы даны не полностью и/или с небольшими погрешностями. Демонстрирует уважительное отношение к членам ГЭК (не перебивает членов комиссии, выслушивает вопросы до конца, спокойно отвечает на вопросы). Имеются незначительные замечания к демонстрационному материалу (компьютерной презентации, раздаточному материалу).	Имеются существенные замечания к качеству доклада по теме ВКР. Допущены значительные неточности при изложении материала, влияющие на суть понимания основного содержания ВКР, нарушена логичность изложения, материал не систематизирован. Речь в основном грамотная, но лексически бедная. Профессиональной терминологией владеет на минимально необходимом уровне. Ответы на поставленные вопросы являются неполными, с серьезными погрешностями Требует дополнительных наводящих вопросов. Имеются существенные замечания к качеству демонстрационного материала (компьютерной презентации, раздаточному материалу).
Итоговая обобщенная оценка сформированности всех компетенций	Большинство компетенций сформированы на повышенном уровне. Сформированность компетенций полностью соответствует требованиям компетентностной модели выпускника. Имеющихся знаний, умений, опыта в полной мере достаточно для решения стандартных и нестандартных профессиональных задач по видам профессиональной	Все компетенции сформированы на пороговом или повышенном уровнях. Сформированность компетенций в целом соответствует требованиям компетентностной модели выпускника, но есть недочеты. Имеющихся знаний, умений, опыта в целом достаточно для решения профессиональных задач, но требуется дополнительная практика по некоторым профессиональным	Все компетенции сформированы, но большинство на пороговом уровне. Сформированность компетенций соответствует минимальным требованиям компетентностной модели выпускника. Имеющихся знаний, умений, опыта в целом достаточно для решения профессиональных задач, но требуется дополнительная практика по

Показатель сформированности/ код компетенций	*Критерии и шкалы оценивания результатов*		
	Повышенный (отлично) 86-100 баллов	***Пороговый (хорошо) 70-85,9 баллов***	***Пороговый (удовлетворительно) 61-69,9 баллов***
	деятельности	задачам	большинству профессиональных задач

Шкала оценки уровня освоения компетенций

Качественная оценка может быть выражена: в процентном отношении качества уровня освоения компетенций, которая соответствует баллам, и переводится в уровневую шкалу и оценки «отлично» / 5, «хорошо» / 4, «удовлетворительно» / 3, «неудовлетворительно» / 2.

Шкалы оценки уровня сформированности компетенций		**Уровневая шкала оценки результатов защиты ВКР**	
Уровневая шкала оценки компетенций	*100 балльная шкала, %*	*100 балльная шкала, %*	*5-балльная шкала, дифференцированная оценка/балл*
допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2
пороговый	61-85,9	70-85,9	«хорошо» / 4
		61-69,9	«удовлетворительно» / 3
повышенный	86-100	86-100	«отлично» / 5

Для интегральной оценки освоения студентами компетенций применяется единый подход согласно балльно-рейтинговой системы по 100-балльной шкале, действующей в университете.

Все компетенции, оцениваемые в ходе защиты ВКР (как элементы определенных групп показателей), подлежат оцениванию членами государственной экзаменационной комиссии. Форма оценочного листа результатов защиты ВКР представлена в Приложениях 4, 5.

Члены ГЭК дают свои оценки уровня сформированности компетенций по установленным показателям, основываясь на качестве доклада, презентации и демонстрационного материала; аргументированности выводов и рекомендаций по результатам ВКР; ответах на вопросы членов ГЭК, отзыве руководителя.

По результатам этой процедуры ГЭК принимает итоговое решение об уровне сформированности компетенций выпускника (повышенный, пороговый, допороговый).

Оценка «отлично», соответствующая повышенному уровню сформированности компетенций, выставляется обучающемуся, если он готов самостоятельно решать стандартные и нестандартные профессиональные задачи по видам профессиональной деятельности. Имеет интегральную оценку уровня сформированности компетенций не ниже 86 баллов.

Оценка «хорошо», соответствующая пороговому уровню сформированности компетенций, выставляется обучающемуся, если он готов самостоятельно решать стандартные профессиональные задачи в соответствии с видами профессиональной деятельности. Имеет интегральную оценку уровня сформированности компетенций 70-85,9 баллов.

Оценка «удовлетворительно», соответствующая пороговому уровню сформированности компетенций, выставляется обучающемуся, если он способен решать определенные профессиональные задачи в соответствии с видами профессиональной деятельности. Имеет интегральную оценку уровня сформированности компетенций не ниже 61-69,9 баллов.

Оценка «неудовлетворительно», соответствующая допороговому уровню сформированности компетенций, выставляется обучающемуся в случае, если сформированность компетенций не соответствует требованиям ФГОС; выпускник не готов решать профессиональные задачи в соответствии с видами профессиональной деятельности.

4.УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

4.1. Перечень учебной литературы

Нормативно – правовые акты

1. Библиографическая запись. Библиографическое описание. Общие требования и правила составления [Электронный ресурс] : ГОСТ 7.1-2003 : межгос. стандарт / Межгос. совет по стандартизации, метрологии и сертификации. - Документ Microsoft Word. - М. : Изд-во стандартов, 2004. - 987 КБ, 71 с. - Введ. 2004-07-01 . - Режим доступа: Локальная сеть.

2. Конституция Российской Федерации [Электронный ресурс] : принята всенар. голосованием 12 дек. 1993 г. : (с учетом поправок от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ) // КонсультантПлюс. – Режим доступа: http://www.consultant.ru/.

3. Об образовании в Российской Федерации [Электронный ресурс] : федер. закон от 29.12.2012 № 273-ФЗ : (с изменениями 2018 года) // Консультант Плюс. - Режим доступа: http://www.consultant.ru/.

4. Федеральный государственный образовательный стандарт высшего образования. Уровень высшего образования. Бакалавриат. Направление подготовки 10.03.01 Информационная безопасность (уровень бакалавриата) [Электронный ресурс] : утв. приказом Минобрнауки РФ от 1 декабря 2016 г. // КонсультантПлюс. - Режим доступа: http://www.consultant.ru/document/Cons_doc_LAW_209323/

Основная литература

5. Космин, В.В. Основы научных исследований (общий курс) [Электронный ресурс] : учеб. пособие / В. В. Космин. - 3-е изд., перераб. и доп. - Документ Bookread2. - М. : Риор [и др.], 2017. - 226 с. - Режим доступа: http://znanium.com/bookread2.php?book=774413.

6. Новиков, Ю.Н. Подготовка и защита бакалаврской работы, магистерской диссертации, дипломного проекта [Электронный ресурс] : учеб. пособие / Ю. Н. Новиков. - Изд. 2-е, стер. - Документ Reader. - СПб. [и др.] : Лань, 2017. - 31 с. - Режим доступа: https://e.lanbook.com/reader/book/94211/#1.

Дополнительная литература

10. Елиферов, В. Г. Бизнес-процессы: регламентация и управление [Электронный ресурс] : учеб. пособие по прогр. МВА и др. прогр. подгот. упр. кадров / В. Г. Елиферов, В. В. РепинИн-т экономики и финансов "Синергия". - Документ Bookread2. - М. : ИНФРА-М, 2018. - 319 с. : ил. - Режим доступа: http://znanium.com/bookread2.php?book=942762

11. Заботина, Н. Н. Проектирование информационных систем [Электронный ресурс] : учеб. пособие для вузов по специальности 09.03.03 "Приклад. информатика (по обл.)" и др. экон. специальностям / Н. Н. Заботина. - Документ Bookread2. - М. : ИНФРА-М, 2016. - 331 с. : ил. - Режим доступа: http://znanium.com/bookread2.php?book=542810

12. Савицкая, Г. В. Экономический анализ [Электронный ресурс] : учеб. для вузов по экон. направлениям и специальностям / Г. В. Савицкая. - 14-е изд., перераб. и доп. - Документ Bookread2. - М. : ИНФРА-М, 2017. - 648 с. : ил. - Режим доступа: http://znanium.com/bookread2.php?book=652550

13. Тарасов, С. В. СУБД для программиста. Базы данных изнутри [Электронный ресурс] : [для программистов, студентов] / С. В. Тарасов. - Документ Bookread2. - М. : СОЛОН-Пресс, 2015. - 319 с. - Режим доступа: http://znanium.com/bookread2.php?book=858603

14. Тельнов, Ю. Ф. Инжиниринг предприятия и управление бизнес-процессами. Методология и технология [Текст] : учеб. пособие для студентов вузов магистратуры по

направлению подгот. "Приклад. информатика" / Ю. Ф. Тельнов, И. Г. Фёдоров. - М. : ЮНИТИ-ДАНА, 2015. - 207 с. : ил.

15. Шустова, Л. И. Базы данных [Электронный ресурс] : учеб. по направлению подгот. 09.03.03 "Приклад. информатика" (квалификация (степень) "бакалавр") / Л. И. Шустова, О. В. Тараканов. - Документ Bookread2. - М. : ИНФРА-М, 2017. - 303 с. - Режим доступа: http://znanium.com/bookread2.php?book=751611

7. Балдин, К. В. Информационные системы в экономике [Электронный ресурс] : учеб. для вузов в обл. приклад. информатики / К. В. Балдин, В. Б. Уткин. - 7-е изд. - Документ Bookread2. - М. : Дашков и К, 2017. - 395 с. : ил. - Режим доступа: http://znanium.com/bookread2.php?book=327836

8. Баранова, Е. К. Информационная безопасность и защита информации [Электронный ресурс] : учеб. пособие по направлению "Приклад. информатика" / Е. К. Баранова, А. В. Бабаш. - 3-е изд., перераб. и доп. - Документ Bookread2. - М. : РИОР [и др.], 2016. - 321 с. - Режим доступа: http://znanium.com/bookread2.php?book=495249

9. Варфоломеева, А. О. Информационные системы предприятия [Электронный ресурс] : учеб. пособие для вузов по направлению 09.03.03. "Приклад. информатика" и др. экон. специальностям / А. О. Варфоломеева, А. В. Коряковский, В. П. Романов. - 2-е изд., перераб. и доп. - Документ Bookread2. - М. : ИНФРА-М, 2019. - 330 с. - Режим доступа: http://znanium.com/bookread2.php?book=1002067

16. Жукова, М. Н. Управление информационной безопасностью [Электронный ресурс] : учеб. пособие по направлениям "Информ. безопасность", "Информатика и вычисл. техника", "Информ. системы" : в 3 ч. . Ч. 2 : Управление инцидентами информационной безопасности / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев ; Сиб. гос. аэрокосм. ун-т им. акад. М. Ф. Решетнева. - Документ HTML. - Красноярск : Сиб. гос. аэрокосм. ун-т, 2012. - 100 с. - Режим доступа: http://znanium.com/bookread.php?book=463061.

17. Ищейнов, В. Я. Защита конфиденциальной информации [Текст] : учеб. пособие для вузов по специальностям "Орг. и технология защиты информации", "Комплексная защита объектов информации" / В. Я. Ищейнов, М. В. Мецатунян. - М. : ФОРУМ, 2013. - 256 с. : ил. - (Высшее образование).

18. Кабашов, С. Ю. Делопроизводство и архивное дело в терминах и определениях [Электронный ресурс] : учеб. пособие для вузов по специальности "Документоведение и док. обеспечение упр." / С. Ю. Кабашов, И. Г. Асфандиярова. - Документ HTML. - М. : Флинта [и др.], 2009. - 8,47 КБ, 296 с. - Режим доступа: http://znanium.com/bookread.php?book=200418.

19. Конфиденциальное делопроизводство и защищенный электронный документооборот [Электронный ресурс] : учеб. для вузов по направлениям подгот. "Документоведение и архивоведение", "Менеджмент", "Информац. безопасность", "Документоведение и документ. обеспечение управления", "Менеджмент орг.", "Орг. и технология защиты информации" / Н. Н. Куняев, А. С. Дёмушкин, Т. В. Кондрашова [и др.] ; под общ. ред. Н. Н. Куняева. - Документ HTML. - М. : Логос, 2011. - 449 с. - (Новая Университетская Библиотека) - Режим доступа: http://znanium.com/bookread.php?book=468998.

20. Корнеев, И. К. Защита информации в офисе [Текст] : учебник / И. К. Корнеев, Е. А. Степанов ; Гос. ун-т упр. - М. : Проспект, 2008. - 333 с.

21. Кузнецов, И. Н. Делопроизводство [Текст] : учеб.-справ. пособие / И. Н. Кузнецов. - 5-е изд., перераб. и доп. - М. : Дашков и К, 2009. - 519 с.

22. Некраха, А. В. Организация конфиденциального делопроизводства и защита информации [Текст] : учеб. пособие для вузов по специальности "Орг. и технология защиты информ." / А. В. Некраха, Г. А. Шевцова ; Ин-т информ. наук и технологий безопасности, Рос. гос. гуманитар. ун-т. - М. : Акад. проект, 2007. - 220 с. - (Gaudeamus).

23. Непогода, А. В. Делопроизводство организации: подготовка, оформление и ведение документации : 75 образцов основных документов [Текст] / А. В. Непогода, П. А.

Семченко. - 3-е изд., стер. - М. : Омега-Л, 2009. - 478 с. : табл. - (Библиотека типовых документов).

24. Правовое обеспечение информационной безопасности [Текст] : учеб. для высш. проф. образования МВД России по специальности "Информ. безопасность телекоммуникац. систем" / [под общ. ред. В. А. Минаева [и др.]. - Изд. 2-е, расшир. и доп. - М. : Маросейка, 2008. - 368 с. - (Информатика и информационная безопасность).

4.2. Перечень информационных технологий, используемых при проведении государственной итоговой аттестации, включая перечень программного обеспечения и информационных справочных систем

4.2.1. Программное обеспечение

№ п/п	Программный продукт	Характеристика	Назначение при освоении дисциплины
1	Microsoft Office 2003/2007/2010	Microsoft Office – комплект рабочих приложений и программ: текстовый редактор Microsoft Word; Редактор электронных таблиц Microsoft Excel; Система управления базами данных Microsoft access; программа создания презентаций Microsoft Power Point; программа для работы с электронной почтой Microsoft Outlook; программа создания публикаций Microsoft Publisher; программа для разработки схем и моделей Microsoft Visio.	WORD – подготовка текстовых документов и раздаточного материала. EXCEL – создание и оформление электронных таблиц, построение графиков. PowerPoint - подготовка презентаций для выступлений с докладами и рефератами, проведения слайд-лекций и практик. Visio - создание и оформление проектных моделей.
2	Microsoft Visual Studio.NET	Среда программирования	Решение практических заданий
3	Delphi	Среда программирования	Решение практических заданий
4	Программа CPU-Z	Программа для тестирования и просмотра характеристик процессора, материнской платы, памяти, видеокарты	Решение практических заданий
5	Программа Cache Burst 32	Утилита для анализа и диагностики работы подсистемы кэш и памяти компьютера	Решение практических заданий
6	Программа System Information for Windows (SIW)	Программа для предоставления детальной информации о компьютере	Решение практических заданий
7	Программа HD Tune	Утилита для работы с жёстким диском и SSD	Решение практических заданий

4.4.2. Информационные справочные системы

1. КонсультантПлюс [Электронный ресурс] : некоммерческая интернет-версия «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/. – Загл. с экрана.
2. Лаборатория сетевой безопасности. Профессиональный блог [Электронный ресурс]. - Режим доступа: http://ypn.ru/146/securing-networking-information/. - Загл. с экрана.
3. Методы и средства защиты информации [Электронный ресурс]. - Режим доступа: http://scanner.narod.ru/link/Safe/miszi/miszi1.htm. - Загл. с экрана.
4. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс]. - Режим доступа: http://elibrary.ru/defaultx.asp. - Загл с экрана.
5. Образование и информатика. [Электронный ресурс]. - Режим доступа: http://www.infojournal.ru. - Загл. с экрана.
6. Положение о порядке организации и проведения работ по защите конфиденциальной информации при ее автоматизированной обработке [Электронный ресурс]. - Режим доступа: http://www.iso2700.ru/zakonodatelstvo/dokumenty-pravitelstva-moskvy-v-oblasti-informacionnoi-bezopasnosti/polozhenie-o-poryadke-organizacii-i-provedeniya-rabot-po-zaschite-konfidencialnoi-informacii-pri-ee-avtomatizirovannoi-obrabotke. – Загл. с экрана.
7. Технологические системы защиты и обработки конфиденциальных документов [Электронный ресурс]. - Режим доступа: http://studopedia.net/9_2263_tehnologicheskie-sistemi-zashchiti-i-obrabotki-konfidentsialnih-dokumentov.html. – Загл. с экрана.
8. Центр образования «Технологии обучения». [Электронный ресурс]. - Режим доступа: www.cor.home-edu.ru. – Загл. с экрана.
9. Экономическая и информационная безопасность. Служба защиты информации предприятия [Электронный ресурс]. - Режим доступа: http://www.abc-people.com/typework/economy/e-confl-8.htm. – Загл. с экрана.
10. Электронная библиотечная система Поволжского государственного университета сервиса [Электронный ресурс]. - Режим доступа: http://elib.tolgas.ru/. - Загл. с экрана.
11. Электронно-библиотечная система Znanium.com [Электронный ресурс]. - Режим доступа: http://znanium.com/. – Загл. с экрана.

5. НЕОБХОДИМАЯ МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА ПРОВЕДЕНИЯ ГИА

Для проведения государственного экзамена необходима аудитория, оборудованная столами, с возможностью проведения письменных работ.

В аудитории во время экзамена у каждого экзаменующегося должны быть две шариковые ручки с синими чернилами, непрограммируемый калькулятор.

Для проведения процедуры защиты выпускной квалификационной работы необходимо помещение, в котором оборудованы рабочие места для всех членов ГЭК, с возможностью выслушивать доклады, просматривать публичные презентации выступающих, вести записи и протоколы, имеются места для слушателей, желающих присутствовать на процедуре защиты ВКР. В состав необходимого оборудования помещения входит аппаратура для публичных презентаций результатов ВКР, содержащая экран, ноутбук, проектор.

О дополнительных требованиях к материально-технической базе, необходимой для представления своей ВКР, студент должен письменным заявлением известить кафедру не позднее, чем за неделю до проведения процедуры защиты.

6. ПОРЯДОК ПОДАЧИ И РАССМОТРЕНИЯ АПЕЛЛЯЦИЙ

По результатам государственных аттестационных испытаний обучающийся имеет право на апелляцию.

Обучающийся имеет право подать в апелляционную комиссию письменную апелляцию о нарушении, по его мнению, установленной процедуры проведения государственного аттестационного испытания и (или) несогласии с результатами государственного экзамена.

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

Для рассмотрения апелляции секретарь государственной экзаменационной комиссии направляет в апелляционную комиссию протокол заседания государственной экзаменационной комиссии, заключение председателя государственной экзаменационной комиссии о соблюдении процедурных вопросов при проведении государственного аттестационного испытания, а также письменные ответы обучающегося (при их наличии) (для рассмотрения апелляции по проведению государственного экзамена) либо выпускную квалификационную работу, отзыв и рецензию (рецензии) (для рассмотрения апелляции по проведению защиты выпускной квалификационной работы).

Апелляция не позднее 2 рабочих дней со дня ее подачи рассматривается на заседании апелляционной комиссии, на которое приглашаются председатель государственной экзаменационной комиссии и обучающийся, подавший апелляцию. Заседание апелляционной комиссии может проводиться в отсутствие обучающегося, подавшего апелляцию, в случае его неявки на заседание апелляционной комиссии.

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

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

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

- об удовлетворении апелляции, если изложенные в ней сведения о допущенных нарушениях процедуры проведения государственного аттестационного испытания обучающегося подтвердились, и повлияли на результат государственного аттестационного испытания.

В случае удовлетворении апелляции результат проведения государственного аттестационного испытания подлежит аннулированию, в связи, с чем протокол о рассмотрении апелляции не позднее следующего рабочего дня передается в государственную экзаменационную комиссию для реализации решения апелляционной комиссии.

Обучающемуся предоставляется возможность пройти государственное аттестационное испытание в сроки, установленные дополнительно.

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

- об отклонении апелляции и сохранении результата государственного экзамена;

- об удовлетворении апелляции и выставлении иного результата государственного экзамена.

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

Решение апелляционной комиссии является окончательным, и пересмотру не подлежит.

Повторное проведение государственного аттестационного испытания обучающегося, подавшего апелляцию, осуществляется в присутствии одного из членов апелляционной комиссии не позднее даты завершения обучения в университете в соответствии с требованиями ФГОС.

Апелляция на повторное проведение государственного аттестационного испытания не принимается.

7. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ГИА ДЛЯ ОБУЧАЮЩИХСЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Для обучающихся из числа инвалидов и лиц с ОВЗ (далее – инвалидов) ГИА проводится в университете с учетом особенностей их психофизического развития, их индивидуальных возможностей и состояния здоровья (далее - индивидуальные особенности).

При проведении ГИА обеспечивается соблюдение следующих общих требований:

- проведение государственной итоговой аттестации для инвалидов в одной аудитории совместно с обучающимися, не являющимися инвалидами, если это не создает трудностей для инвалидов и иных обучающихся при прохождении государственной итоговой аттестации;
- присутствие в аудитории ассистента (ассистентов), оказывающего обучающимся инвалидам необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочитать, и оформить задание, общаться с председателем и членами государственной экзаменационной комиссии);
- пользование необходимыми обучающимся инвалидам техническими средствами при прохождении государственной итоговой аттестации с учетом их индивидуальных особенностей;
- обеспечение возможности беспрепятственного доступа обучающихся инвалидов в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов, лифтов, при отсутствии лифтов аудитория должна располагаться на первом этаже, наличие специальных кресел и других приспособлений).

Все локальные нормативные акты по вопросам проведения государственной итоговой аттестации доводятся до сведения обучающихся инвалидов в доступной для них форме.

По письменному заявлению обучающегося инвалида продолжительность сдачи обучающимся инвалидом государственного аттестационного испытания может быть увеличена по отношению к установленной продолжительности его сдачи:

- продолжительность сдачи государственного экзамена, проводимого в письменной форме, - не более чем на 90 минут;
- продолжительность подготовки обучающегося к ответу на государственном экзамене, проводимом в устной форме, - не более чем на 20 минут;
- продолжительность выступления обучающегося при защите выпускной квалификационной работы - не более чем на 15 минут.

В зависимости от индивидуальных особенностей обучающихся с ограниченными возможностями здоровья в университете обеспечивается выполнение следующих требований при проведении государственного аттестационного испытания:

а) для слепых:

задания и иные материалы для сдачи государственного аттестационного испытания оформляются рельефно-точечным шрифтом Брайля или в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, либо зачитываются ассистентом;

письменные задания выполняются обучающимися на бумаге рельефно-точечным шрифтом Брайля или на компьютере со специализированным программным обеспечением для слепых, либо надиктовываются ассистенту;

при необходимости обучающимся предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным обеспечением для слепых;

б) для слабовидящих:

задания и иные материалы для сдачи государственного аттестационного испытания оформляются увеличенным шрифтом;

обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

в) для глухих и слабослышащих, с тяжелыми нарушениями речи:

обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающимся предоставляется звукоусиливающая аппаратура индивидуального пользования;

по их желанию государственные аттестационные испытания проводятся в письменной форме;

г) для лиц с нарушениями опорно-двигательного аппарата (тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

письменные задания выполняются обучающимися на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;

по их желанию государственные аттестационные испытания проводятся в устной форме.

Обучающийся инвалид не позднее чем за 3 месяца до начала проведения государственной итоговой аттестации подает письменное заявление о необходимости (отсутствии необходимости) создания для него специальных условий при проведении государственных аттестационных испытаний с указанием его индивидуальных особенностей. К заявлению прилагаются документы, подтверждающие наличие у обучающегося индивидуальных особенностей.

В заявлении обучающийся указывает на необходимость (отсутствие необходимости) присутствия ассистента на государственном аттестационном испытании, необходимость (отсутствие необходимости) увеличения продолжительности сдачи государственного аттестационного испытания по отношению к установленной продолжительности (для каждого государственного аттестационного испытания).

Приложение 1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СЕРВИСА»
(ФГБОУ ВО «ПВГУС»)

Институт экономики.
Кафедра «Прикладная информатика в экономике»
Направление 10.03.01 «Информационная безопасность» (направленность «Организация и технология защиты информации»)

УТВЕРЖДАЮ:
Заведующий кафедрой
_____ _____
(ФИО)
«_____»_____г.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №___
ГОСУДАРСТВЕННОГО ЭКЗАМЕНА

ЗАДАНИЕ 1. ТЕСТ

1. Под информационной безопасностью понимается (выбрать неверное высказывание):

A. защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений;

B. состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций и государства;

C. в создание в организации комплекса административных мер, позволяющих разрешить или запретить доступ сотрудников к определенной информации и средствам ее обработки, выработать правила работы с информацией определить систему наказаний за их несоблюдение.

2. Процесс создания системы защиты информации в информационных системах подразумевает обязательное прохождение этапов:

A. описания информационных, технических и программных средств, обслуживающего персонала и пользователей;

B. выявление угроз, определение политики безопасности, создание механизмов поддержки безопасности и оценки защищенности системы;

C. выявления доступности, целостности и конфиденциальности.

3. Основным видом криптографического преобразования информации является шифрование, которое заключается в

A. скрытии смысла хранимой или передаваемой информации и самого факта хранения или передачи закрытой информации;

B. проведении обратимых математических, логических, комбинаторных и других преобразованиях искомой информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов;

C. замене смысловых конструкций исходной информации (слов, предложений) кодами.

4. Максимальная продолжительность работы за компьютером не должна превышать:

A. 6 часов;

B. 10 часов;

C. 20 часов.

Экзаменационный билет №1 / Лист 2

5. Продолжительность непрерывной работы за компьютером (ЭВМ) не должна превышать норму в……., без учета регламентируемого времени перерыва

A. 1 час;

B. 3 часа;

C. 8 часов.

6. Что такое «безопасность»?

A. опасность, которая представляет угрозу общего характера, не связанная с пространством и временем воздействия;

B. состояние объекта защиты, при котором воздействие на него всех потоков вещества, энергии и информации не превышает максимально допустимых значений;

C. полное отсутствие опасностей;

D. количественная характеристика опасности;

E. нет правильного ответа.

7. Диаграмма, которая отображает потоки работ во взаимосвязанных прецедентах использования (могут декомпозироваться на более детальные диаграммы) - это

A. UML-диаграмма деятельностей

B. UML-диаграмма взаимодействия объектов

C. UML-диаграмма прецедентов использования

8. Сеть, какого типа охватывает одно здание или комплекс зданий и предоставляет сервисы и приложения пользователям в общей организационной структуре?

A. персональная сеть (PAN);

B. глобальная сеть (WAN);

C. локальная сеть (LAN);

D. муниципальная сеть (MAN).

9. Основные способы разделения субъектов к совместно используемым объектам:

A. Концептуальное - разделение объектов на уровне структуры ИС

B. Физическое - субъекты обращаются к физически различным объектам.

C. Временное - субъекты с различными правами доступа к объекту получают его в различные промежутки времени.

D. Логическое - субъекты получают доступ к совместно используемому объекту в рамках единой операционной среды, но под контролем средств разграничения доступа

E. Криптографическое - все объекты хранятся в зашифрованном виде

10. В качестве биометрических признаков, которые могут быть использованы при идентификации потенциального пользователя, можно выделить следующие:

узор радужной оболочки и сетчатки глаз;

A. отпечатки пальцев;

B. геометрическая форма руки;

C. форма и размеры лица;

D. форма и размеры носа и ушей;

E. особенности голоса;

F. особенности прически;

G. биомеханические характеристики рукописной подписи;

H. биомеханические характеристики "клавиатурного почерка".

11. Система разграничения доступа к информации должна содержать следующие функциональные блоки:

A. блок идентификации и аутентификации субъектов доступа;

B. диспетчер доступа;

C. диспетчер оперативной памяти;

D. диспетчер дисковых устройств;

E. блок криптографического преобразования информации при ее хранении и передаче;

F. блок очистки памяти.

12. Единая политика безопасности по всей сети – это особенность

A. корпоративных распределенных компьютерных сетей

B. любых компьютерных сетей

C. общедоступных распределенных компьютерных сетей

D. коммерческих распределенных компьютерных сетей

13. С увеличением интеграции узлов и компонентов в устройстве обработки информации

A. усложняется проведение специальной проверки данного устройства на наличие в нем модулей, выполняющих несанкционированные, с точки зрения пользователя, действия

B. упрощается проведение специальной проверки данного устройства на наличие в нем модулей, выполняющих несанкционированные, с точки зрения пользователя, действия

C. требуется обязательное проведение специализированной проверки данного устройства на наличие модулей, выполняющих несанкционированные, с точки зрения пользователя, действия

D. перестает требоваться проведение специальной проверки данного устройства на наличие модулей, выполняющих несанкционированные, с точки зрения пользователя, действия.

14. Увеличение производительности вычислительной системы и емкости каналов связи позволяет злоумышленнику в более короткие сроки произвести

A. вскрытие паролей и ключей доступа

B. организовать интенсивное воздействие на узел информационной сети

C. физическое хищение любых носителей информации

D. сбой в работе всей информационной системы

15. Целями системы защиты информации предприятия являются:

A. приемлемость защиты для пользователей

B. определение объектов защиты

C. предотвращение утечки, хищения, утраты, искажения, подделки информации

16. Для грамотного построения и эксплуатации системы защиты необходимо соблюсти следующие принципы ее применения:

D. сохранение, конфиденциальности документированной информации в соответствии с законодательством

E. постоянный контроль за наиболее важной информацией

F. независимость системы управления для пользователей

17. Алгоритм создания системы защиты конфиденциальной информации таков

A. определение объектов защиты

B. определение объектов защиты, сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах

C. независимость системы управления для пользователей

18. Какая концепция предполагает возможность использования службой безопасности всего комплекса легитимных методов профилактики и отражения потенциальных угроз:

A. стратегия адекватного ответа

B. стратегия пассивной защиты

C. упреждающего противодействия

19. Задача проведения анализа уязвимости информационной системы:

A. рассмотрение всех возможных угроз и оценка размеров возможного ущерба

B. определение всех возможных слабых мест информационной системы

C. регламентация деятельности кредитной организации

20. Информация, полученная без использования неправомерных средств, при проведении собственных исследований, по собственной инициативе, путем систематических наблюдений или сбора сведений

A. может быть отнесена к коммерческой тайне по усмотрению получателя информации

B. не должна относиться к коммерческой тайне

C. обязательно должна являться общедоступной

ЗАДАНИЕ 2. Решение задач:

1. *Определите ключ в системе шифрования, использующей перестановку с фиксированным периодом d=5 по паре открытых и зашифрованных сообщений: ШИФРОВАНИЕ – ОИРШФЕАИВН Ответ запишите в виде последовательности цифр без пробелов.*

2. *Исходные данные:*

В компании введено в эксплуатацию новое офисное здание, в котором предусмотрено отдельное помещение (комната) для проведения совещаний руководства.

Конструкция здания	Бетон (монолит)
Этаж	6
Площадь помещения, $м^2$	30
Наличие окон	3 окна
Оборудование	кондиционер
Телефонная связь	Телефон гор.тел.сети
Компьютеры	Компьютер секретаря в сети Ethternet

Задание:

1. Провести предварительный анализ и определить возможные технические каналы утечки информации для заданного помещения. Оценить их по следующим направлениям:
   - с точки зрения возможности доступа,
   - с точки зрения вида информации и возможного ущерба от её утечки.
2. Предложить основные мероприятия по инженерно-технической защите информации для заданного помещения:
   - На постоянной основе (стационарно в помещении или в здании);
   - Проводимые во время проведения совещаний руководства в данном помещении.

СОГЛАСОВАНО:

Руководитель образовательной программы

_____ _____

(подпись) (Ф.И.О.)

«___»_____г.

Приложение 2

СВОДНЫЙ ОЦЕНОЧНЫЙ ЛИСТ РЕЗУЛЬТАТОВ ГОСУДАРСТВЕННОГО ЭКЗАМЕНА

Группа_____ Направление _______
Номер группы *Код направления подготовки, и профиль*

	ФИО студента / Задания/ код компетенций										
1	Задание № 1 (тест)	ОПК-4 ОПК-6 ПК-1 ПК-3 ПСК-1 ПСК-2									
2	Задание № 2 (задача)	ОПК-4 ПК-1 ПСК-1									
	Результирующая оценка										
	Итоговая обобщенная оценка уровня сформированности компетенций (отлично, хорошо, удовлетворительно)										

Примечание: Каждое задание оценивается по 100-балльной шкале
86-100 баллов - повышенный уровень (отлично)
70-85,9 баллов - пороговый уровень (хорошо)
61-69,9 баллов - пороговый уровень (удовлетворительно)
Результирующая оценка государственного экзамена получается путем суммирования оценок полученных на отдельных этапах экзамена. При этом вес оценки за решение тестовых заданий – 0,7 баллов, за выполнение практического задания – 0,3 баллов.

Подпись члена ГЭК_____ _____
(ФИО)

дата _____

Приложение 3

СВОДНАЯ ВЕДОМОСТЬ
СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ,
ВЫНОСИМЫХ НА ГОСУДАРСТВЕННЫЙ ЭКЗАМЕН

Группа _____ **Направление**_____
Номер группы *Код направления подготовки, и профиль*

Присутствовали: Председатель: _____
Члены ГЭК:_____.
ФИО членов ГЭК

ФИО обучающегося	Уровень освоения компетенций, баллы						Итоговый уровень сформированности компетенций*
	ОПК-4	ОПК-6	ПК-1	ПК-3	ПСК-1	ПСК-2	

** Примечание:*
86-100 баллов - повышенный уровень (отлично), соответствует требованиям ФГОС ВО
70-85,9 баллов - пороговый уровень (хорошо), в основном соответствует требованиям ФГОС ВО
61-69,9 баллов - пороговый уровень (удовлетворительно), в основном соответствует требованиям ФГОС ВО

Председатель ГЭК_____ ФИО
(подпись)
Секретарь ГЭК _____ ФИО
(подпись)

Приложение 4

СВОДНЫЙ ОЦЕНОЧНЫЙ ЛИСТ РЕЗУЛЬТАТОВ ЗАЩИТЫ ВКР

Член ГЭК _____ Группа _____
ФИО члена ГЭК *Номер группы*

Направление _____
Код направления подготовки, и профиль

Показатель* /коды компетенций \ **ФИО студента**							
Обоснованность актуальности темы работы, четкость формулировки цели и задач, выводов	*ОК-1* *ОК-2* *ОК-3*						
Актуальность и полнота анализа информационных ресурсов организации, выявление областей для улучшения, обоснованность рекомендаций по решению выявленных проблем	*ОК-2* *ОК-7* *ОК-8* *ОПК-7*						
Содержательность, глубина и комплексность теоретического исследования	*ОК-4* *ОПК-4* *ОПК-1* *ОПК-3* *ОПК-7* *ПК-9* *ПК-10*						
Качество и адекватность подбора используемого инструментария, глубина и комплексность проведенного исследования по решаемым профессиональным задачам	*ОПК-2* *ОПК-7* *ПК-11* *ПК-14* ПСК-1						
Содержательность и полнота технико-экономического обоснования проектных решений	*ОПК-2* *ПК-7* *ПКВ-1*						
Разработка и описание проекта в соответствии со стадиями жизненного цикла	*ПК-2* *ПК-5* *ПК-6* *ПК-8* *ПК-12* *ПК-13* *ПК-15* ПСК-1						
Достаточность и актуальность источников литературы (в том числе нормативных документов, справочной литературы, иностранных источников), проработанность нормативной документации по решаемым профессиональным задачам	*ОПК-4* *ОПК-5* *ПК-9* ПСК-2						
Качество выполнения пояснительной записки, стиль изложения ВКР	ОК-3 ОК-5 ОК-8 ОПК-4 *ПК-8*						
Оценка выполненной работы руководителем ВКР, в том числе соблюдение графика выполнения разделов ВКР, полноты и качества доработок отдельных разделов ВКР при	*ОК-9* *ОПК-6* *ОПК-7* *ПК-1* *ПК-3*						

наличии замечаний	*ПК-4* ПСК-1 ПСК-2						
Ясность, четкость, последовательность выступления, обоснованность и полнота ответов на вопросы, качество и содержательность презентации и демонстрационного материала	*ОК-5* *ОК-6* *ОК-7* *ОК-8* ОПК-5						
Средний балл							
Итоговая обобщенная оценка уровня сформированности компетенций *(отлично, хорошо, удовлетворительно)*							
Уровень сформированности компетенций *(повышенный, пороговый, допороговый)*							

Примечание. * Каждый показатель оценивается по 100-балльной шкале:

86-100 баллов - повышенный уровень (отлично)

70-85,9 баллов - пороговый уровень (хорошо)

61-69,9 баллов - пороговый уровень (удовлетворительно)

Подпись члена ГЭК_____ дата _____

Приложение 5

СВОДНАЯ ВЕДОМОСТЬ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ
ПО РЕЗУЛЬТАТАМ ЗАЩИТЫ ВКР

Группа _____ Направление __10.03.01 «Информационная безопасность»_____
Номер группы *Код направления подготовки, и профиль*

Присутствовали: Председатель:_____
Члены ГЭК:_____
ФИО членов ГЭК

ФИО обучающегося	***Уровень освоения компетенций, баллы***																																	Итоговый уровень сформированности компетенций*
	ОК-1	*ОК-2*	*ОК-3*	*ОК-4*	*ОК-5*	*ОК-6*	*ОК-7*	*ОК-8*	*ОК-9*	*ОПК-1*	*ОПК-2*	*ОПК-3*	*ОПК-4*	*ОПК-5*	*ОПК-6*	*ОПК-7*	*ПК-1*	*ПК-2*	*ПК-3*	*ПК-4*	*ПК-5*	*ПК-6*	*ПК-7*	*ПК-8*	*ПК-9*	*ПК-10*	*ПК-11*	*ПК-12*	*ПК-13*	*ПК-14*	*ПК-15*	*ПКВ-1*	*ПСК-1*	*ПСК-2*	

** Примечание:*
86-100 баллов - повышенный уровень (отлично), соответствует требованиям ФГОС ВО
70-85,9 баллов - пороговый уровень (хорошо), в основном соответствует требованиям ФГОС ВО
61-69,9 баллов - пороговый уровень (удовлетворительно), в основном соответствует требованиям ФГОС ВО

Председатель ГЭК_____ **ФИО**
(подпись)

Секретарь ГЭК _____ **ФИО**
(подпись)