МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И.о. директора факультета математики и компьютерных наук имени профессора Н. И. Червякова
Т. А. Гробова

ПРОГРАММА ГОСУДАРСТВЕННОГО ЭКЗАМЕНА

Специальность	10.05.03 Информационная безопасность автоматизированных систем
Специализация	Анализ безопасности информационных систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в	11 семестре

РАЗРАБОТАНО:

Доцент кафедры вычислительной математики и кибернетики
Лапина М. А.

Ставрополь, 2026

1. Цели и задачи государственного экзамена

Заключительный этап теоретического обучения специалиста в высшем учебном заведении состоит в подготовке и сдаче государственного экзамена. Государственный экзамен по специальности 10.05.03 «Информационная безопасность автоматизированных систем» специализация «Анализ безопасности информационных систем» преследует цель провести оценку степени профессиональной подготовки выпускника по использованию теоретических знаний, практических навыков и умений, уровня сформированности компетенций для решения профессиональных задач на уровне, требуемом федеральным государственным образовательным стандартом высшего образования по специальности 10.05.03 «Информационная безопасность автоматизированных систем» с учетом специфики учебного процесса и региональных особенностей вуза.

Государственный экзамен по специальности 10.05.03 «Информационная безопасность автоматизированных систем» проводится в форме итогового междисциплинарного экзамена.

Основная задача государственного экзамена – выявление способности студентов к решению теоретических и практических задач на междисциплинарном уровне

Задачами государственного экзамена являются:

– определение соответствия подготовки студента выпускного курса СКФУ требованиям ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем» и уровня теоретической и практической его подготовки;

– принятие решения о присвоении квалификации (степени) по результатам государственной итоговой аттестации и выдаче выпускнику Университета соответствующего диплома государственного образца о высшем профессиональном образовании;

– разработка рекомендаций, направленных на совершенствование качества подготовки специалистов, на основании результатов работы государственной аттестационной комиссии.

2. Перечень компетенций, уровень сформированности которых должен быть проверен на государственном экзамене.

Код компетенции	Формулировка
ОПК-(№)	Общепрофессиональные компетенции
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
ОПК-9	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты, сетей и систем передачи информации
ОПК-12	Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных

Код компетенции	Формулировка
	систем
ПК-(№)	Профессиональные компетенции
ПК-1	Способен оценивать уровень безопасности компьютерных систем и сетей
ПК-3	Способен разрабатывать средства защиты информации
ПК-7	Способен организовывать и проводить работы по технической защите информации
ПК-8	Способен разрабатывать системы защиты информации автоматизированных систем
ПК-9	Способен формировать требования к защите информации в автоматизированных системах

3. Структура государственного экзамена

Государственный экзамен включает вопросы, задачи по следующим дисциплинам учебного плана подготовки специалистов по специальности 10.05.03 «Информационная безопасность автоматизированных систем»:

1) Безопасность сетей ЭВМ;
2) Безопасность систем баз данных;
3) Комплексное обеспечение информационной безопасности автоматизированных систем;
4) Организационное и правовое обеспечение информационной безопасности;
5) Защита информации от утечки по техническим каналам;
6) Построение подсистем информационной безопасности информационных систем

Экзамен предполагает:

1. Ответ экзаменуемого по теоретическим вопросам.
2. Практическое выполнение задания.

Государственный экзамен проводится по билетам, составленным в соответствии с программой экзамена. Структура экзаменационного билета состоит из 3 пунктов, соответствующих 3 различным дисциплинам. Каждый билет содержит 2 теоретических вопроса и практический вопрос.

4. Содержание государственного экзамена

Программа государственного экзамена по специальности 10.05.03 «Информационная безопасность автоматизированных систем» включает основополагающие темы следующих учебных дисциплин:

4.1 Безопасность сетей ЭВМ

Постановка задачи распределенной обработки данных; классификация сетей по способам распределения данных, сравнительная характеристика различных типов сетей; основы организации и функционирования сетей; сетевые операционные системы; основные сетевые стандарты; средства взаимодействия процессов в сетях; распределенная обработка информации в системах клиент-сервер; одноранговые сети; безопасность ресурсов сети; средства идентификации и аутентификации; методы разделения ресурсов и технологии разграничения доступа; средства повышения надежности функционирования сетей; интеграция локальных сетей в региональные и глобальные сети; организация сетей на базе операционных систем NetWare; организация вычислительных сетей на базе операционных систем Windows; организация вычислительных сетей на базе операционных систем Unix; основные протоколы, службы, функционирование, средства обеспечения безопасности, средства управления и контроля, генерация, сопровождение и разработка приложений;

неоднородные вычислительные сети; глобальная сеть Internet; основные службы и предоставляемые услуги, технологии обеспечения безопасности, основные протоколы, функционирование, разработка и сопровождение приложений, особенности реализации на различных платформах, стандарты; перспективы развития; основные механизмы обеспечения безопасности и управления распределенными ресурсами; языковые средства представления информации в Internet; организация корпоративных сетей Internet.

4.2 Безопасность систем баз данных

Общие принципы построения баз данных: реляционная, иерархическая и сетевая модели; распределенные базы данных в сетях ЭВМ; общая характеристика, назначение и возможности систем управления базами данных (СУБД); языковые средства СУБД для различных моделей данных; языковые средства манипулирования данными в реляционных СУБД; языковые средства описания данных реляционных СУБД; особенности языковых средств управления и обеспечения безопасности данных в реляционных СУБД; оптимизация производительности и характеристик доступа к базам данных; средства обеспечения безопасности баз данных: средства идентификации и аутентификации объектов баз данных, языковые средства разграничения доступа, концепция и реализация механизма ролей, организация аудита событий в системах баз данных; средства контроля целостности информации, организация взаимодействия СУБД и базовой ОС, журнализация, средства создания резервных копии и восстановления баз данных, технологии удаленного доступа к системам баз данных, тиражирование и синхронизация в распределенных системах баз данных; задачи и средства администратора безопасности баз данных; средства реализации диалогового интерфейса и подготовки отчетов в языках СУБД; средства автоматизации проектирования баз данных.

4.3 Комплексное обеспечение информационной безопасности автоматизированных систем

Атаки на автоматизированную систему; защита информации в компьютерных сетях; способы реализации угроз в вычислительных сетях; деструктивные действия на информацию; способы организации сокрытия информации и вредоносных программ; уничтожение свидетельств несанкционированного доступа; сетевые компьютерные атаки; переполнение буфера; фальсификация DNS имени в информационных системах; системы обнаружения и предотвращения вторжений; системы защиты от утечек информации DLP; жизненный цикл компьютерных вирусов; процесс заражения вирусами; проникновение вируса на компьютер; поиск объектов заражения; подготовка вирусных копий; механизмы противодействия антивирусом; виды вредоносных действий; классификация компьютерных вирусов: сетевые черви, троян, антивирусная защита; методы обнаружения вредоносных программ; взаимодействие заказчика, исполнителя и управлений ФСБ и ФСТЭК России в процессе аттестации объекта информатизации.

4.4 Организационное и правовое обеспечение информационной безопасности

Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации; конституционные гарантии прав граждан на информацию и механизм их реализации; понятие и виды защищаемой информации по законодательству РФ; государственная тайна как особый вид защищаемой информации; конфиденциальная информация; система защиты государственной тайны; правовой режим защиты государственной тайны; правовое регулирование взаимоотношений администрации и персонала в области защиты информации; правовые режимы конфиденциальной информации; лицензирование и сертификация в области защиты информации, в том числе государственной тайны; правовые основы защиты информации с использованием технических средств (защита от технических разведок, применение и разработка шифровальных средств, электронная цифровая подпись и т.д.); защита интеллектуальной собственности; правовая регламентация охранной деятельности; международное законодательство в области защиты информации. Преступления в сфере

компьютерной информации; экспертиза преступлений в области компьютерной информации; криминалистические аспекты проведения расследований.

4.5 Защита информации от утечки по техническим каналам

Виды источники и носители защищаемой информации; демаскирующие признаки объектов наблюдения и сигналов; опасные сигналы и их источники; побочные электромагнитные излучения и наводки; структура, классификация и основные характеристики технических каналов утечки информации; классификация технической разведки; основные этапы и процедуры добывания информации технической разведкой; возможности видов технической разведки; концепция и методы инженерно-технической защиты ин формации; методы и средства инженерной защиты и технической охраны объектов; скрытие объектов наблюдения; скрытие речевой информации в каналах связи; энергетическое скрытие акустических информативных сигналов; обнаружение и локализация закладных устройств, подавление их сигналов; подавление опасных сигналов акустоэлектрических преобразователей; экранирование и компенсация информативных полей; подавление информативных сигналов в цепях заземления и электропитания; подавление опасных сигналов; характеристика государственной системы противодействия технической разведке; нормативные документы по противодействию технической разведке; виды контроля эффективности защиты информации; основные положения методологии инженерно- технической защиты информации; методы расчета и инструментального контроля показателей защиты информации.

4.6 Построение подсистем информационной безопасности информационных систем

Понятие сложной системы: элементы и подсистемы, управление и информация, самоорганизация. Основные принципы системного подхода при создании сложных систем. Понятие качества и эффективности: характеристики качества, показатели и критерии эффективности, методические вопросы оценки эффективности сложных систем. Функциональная и обеспечивающая часть сложной системы. Технология функционирования сложной системы. Цели и задачи проектирования. Структуризация предметной области. классификация объектов проектирования. Жизненный цикл автоматизированной системы. Этапы проектирования системы. Организация работ, функции заказчиков и разработчиков. Практические методы реализации моделей безопасности. Ядра безопасности. Мониторинг взаимодействий в системе. Архитектура защищенных систем. Технологический цикл реализации защищенной системы обработки и хранения информации. Реализация систем контроля доступа. Способы представления информации о правах доступа.

5. Перечень примерных вопросов для подготовки к государственному экзамену

Студенты, прошедшие курс обучения по специальности «Информационная безопасность автоматизированных систем», специализация «Анализ безопасности информационных систем» в результате обучения должны знать:

Безопасность сетей ЭВМ

1. Стек протоколов IPSec. Архитектура протоколов, режимы использования, ограничения. Протоколы AH и ESP.
2. Технологии межсетевого экранирования. Основные схемы включения и режимы работы межсетевых экранов.
3. Виды и способы применения трансляции IP адресов и портов транспортного уровня. Виды трансляций сетевых адресов, детальное описание области применения и специфика каждого вида.
4. Протоколы и технологии туннелирования на канальном уровне. Основные типы протоколов, область применения, ограничения.
5. Аутентификация пользователей на телекоммуникационном оборудовании в соответствии со стандартом IEEE 802.1X. Схема взаимодействия супликанта, аутентификатора и сервера аутентификации. Способы аутентификации.

6. Использование прокси-серверов в качестве инструмента контроля и управления трафиком. Особенности реализации технологии проксирования HTTPS трафика в корпоративных сетях.

7. Системы обнаружения вторжений. Методы анализа сетевой информации, классификация систем обнаружения атак, компоненты и архитектура.

8. Технологии защиты сетей на канальном уровне. Основные угрозы и способы их нейтрализации.

9. Политика безопасности информационной сети организации. Структура политики безопасности организации, базовая и специализированная политики.

10. Технологии виртуальных частных сетей (VPN). Понятия и функции VPN, классификация VPN по способу организации защищенных каналов.

11. Безопасность систем электронной почты в Интернет. Безопасность протоколов SMTP/POP3/IMAP.

12. Технологии и средства защиты электронной корреспонденции. Нежелательная корреспонденция («спам») и борьба с нею.

13. Протоколы управления и диагностики. Обеспечение безопасности протоколов.

14. Протоколы маршрутизации. Обеспечение безопасности протоколов.

15. Безопасность службы доменных имен Интернета.

16. Широковещательная рассылка. Основные виды протоколов, использующих широковещательную рассылку. Обеспечение информационной безопасности при их работе.

Безопасность систем баз данных

1. Структурная модель защищенной базы данных. Общая характеристика угроз безопасности баз данных.

2. Защита интерфейсов в БД. Защита интерфейса пользователя БД. Защита интерфейса администратора БД

3. Поддержание целостности данных в системах управления базами данных. Логическая и физическая целостность баз данных.

4. Реализация произвольного управления доступом в системах управления базами данных.

5. Шифрование паролей в СУБД Oracle. Алгоритм парольной защиты.

6. Анализ атак на пароли в СУБД Oracle. Силовая атака. Атака по словарю и парадокс дней рождений. Эквивалентная длина хешей и паролей.

7. Разведка паролей в СУБД Oracle. Подмена пакетов. Пароли в трассировочных файлах. Пароли и OEM Grid Control. Внедрение скрытого пользователя.

8. Технология информационной безопасности в БД на примере Oracle IRM.

9. Технология аудита в СУБД Oracle.

10. Реализация моделей разграничения доступа на примере зарубежных СУБД.

11. Назовите основные компоненты подсистемы защиты базы данных.

12. Какие наиболее общие подходы к вопросу обеспечения безопасности данных поддерживается в современных СУБД?

13. Перечислите наиболее известные современные СУБД.

14. Опишите алгоритм проверки аутентификации пользователя в MSSQLServer.

15. Для чего используется механизм разграничения доступа на уровне СУБД.

Комплексное обеспечение информационной безопасности автоматизированных систем

1. Методика определения состава защищаемой информации. Классификация информации по видам тайн и степеням конфиденциальности.

2. Технологическое построение комплексной системы защиты информации. Факторы, влияющие на выбор состава комплексной системы защиты информации.

3. Управление комплексной системой защиты информации. Планирование, контроль деятельности.

4. Схема осуществления атаки на автоматизированную систему. Термины и определения. Задачи защиты информации в компьютерных сетях. Способы реализации угроз в вычислительных сетях. Деструктивные действия на информацию.

5. Типовые способы организации сокрытия информации и вредоносных программ. Уничтожение свидетельств несанкционированного доступа.

6. Типичный сценарий сетевой компьютерной атаки. Нарушения безопасности доступа к памяти. Переполнение буфера. Подмена ARP. Фальсификация DNS имени в информационных системах.

7. Системы обнаружения и предотвращения вторжений. Системы защиты от утечек информации DLP.

8. Жизненный цикл компьютерных вирусов. Процесс заражения вирусами. Проникновение вируса на компьютер. Активация. Поиск объектов заражения. Подготовка вирусных копий.

9. Перечислите основные этапы построения комплексных систем защиты информации.

10. Какие задачи решаются в ходе разработки и внедрения КСЗИ?

11. Сертификация средств защиты информации по требованиям безопасности информации (общие положения, организационная структура системы сертификации, процедура сертификации и контроля, требования к нормативным и методическим документам по сертификации средств защиты информации).

12. Перечислите процессы выполняемые при обеспечении защиты информации в ходе эксплуатации аттестованной информационной системы.

13. Лицензирование деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны.

Организационное и правовое обеспечение информационной безопасности

1. Система органов обеспечения информационной безопасности. Общие функции органов государственной власти в области ИБ.

2. Техническое регулирование в области защиты информации. Перечень видов деятельности предприятий в области защиты информации, подлежащих лицензированию ФСБ и ФСТЭК.

3. Порядок аттестации объектов информатизации в области защиты информации.

4. Организация доступа должностных лиц и граждан к сведениям, составляющим государственную тайну.

5. Законодательные основы лицензирования отдельных видов деятельности в Российской Федерации. Основы лицензирования деятельности организаций в области защиты информации и государственной тайны.

6. Нормы ответственности за правонарушения в информационной сфере.

7. Общие положения методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

8. Порядок определения актуальных угроз безопасности персональных данных в информационных системах персональных данных.

9. Понятие информационной системы персональных данных. Классификация информационных данных в информационных системах персональных данных.

10. Общие положения основных мероприятий по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных.

11. Способы контроля целостности программного обеспечения и аппаратных средств.

12. Способы и средства контроля доступа к автоматизированным системам и рабочему месту пользователя.

Защита информации от утечки по техническим каналам

1. Порядок проведения работ по оценке защищенности информации от ее утечки по каналам ПЭМИН.

2. Понятие, структура и общая характеристика технического канала утечки информации. Аппаратура для оценки защищенности технических средств от утечки информации по каналам ПЭМИН.

3. Общая характеристика физических средств защиты, задачи, решаемые физическими средствами, рубежи защиты, классы систем физической защиты.

4. Общая характеристика каналов утечки речевой конфиденциальной информации. Единицы измерения в акустике.

5. Общая характеристика технических средств и методов пресечения разглашения конфиденциальной информации. Основные акустические параметры речевых сигналов.

6. Особенности распространения акустических сигналов в выделенных помещениях и средства защиты от утечки информации по техническим каналам.

7. Характеристика технических каналов утечки информации при ее передаче по каналам связи, методов и средств защиты. Порядок работы с поисковыми приборами в проводных линиях. Рефлектометрия.

8. Определение, структура и характеристики визуально-оптического канала утечки видовой информации. Методы и средства защиты информации от утечки по визуально-оптическим каналам.

9. Построение и общие характеристики закладных и радиозакладных устройств. Методы снятия информации с помощью микрофонов, диктофонов, линий телефонной связи, радиозакладок. Нелинейная локация.

10. Трансформаторная схема канала утечки информации на основе телефонного адаптера. Основные способы и технические средства защиты электролиний, линий связи и средств обработки информации.

Построение подсистем информационной безопасности информационных систем

1. Основные принципы системного подхода при создании сложных систем. Задачи и компоненты системного анализа сложных систем. Понятие сложной проблемы.

2. Определения понятий качества, эффективности, характеристики, свойства, параметра, показатели и критерии эффективности.

3. Задачи управления сложными системами, характеристика основных групп функций системы. Понятие цикла и контура управления.

4. Технологии обнаружения информационных атак.

5. Понятия и проблемы информационных конфликтов и войн.

6. Понятие VPN. Виды, варианты реализации и основные компоненты VPN. Архитектура и принципы построения защищенных систем.

7. Технологии систем контроля доступа. Способы представления информации о правах доступа.

8. Технология ViPNet. Структура сети ViPNet, принципы модификации справочно-ключевой структуры сети. События явной и неявной компрометации ключевых данных и действия при компрометации. Формирование ключей при изменениях в структуре сети.

9. События явной и неявной компрометации ключевых данных и действия при компрометации. Формирование ключей при изменениях в структуре сети.

10. Характеристика технологии управления рисками. Этапы построения защищенной автоматизированной системы.

11. Инфраструктура с открытыми ключами (PKI).

12. Межсетевое взаимодействие: виды межсетевых мастер-ключей, экспорт и импорт данных для межсетевого взаимодействия.

13. Виды межсетевых экранов,поколения межсетевых экранов. Демилитаризованные зоны информационно-телекоммуникационной инфраструктуры.

задания для проверки умений и навыков (повышенный уровень)

Студенты, прошедшие курс обучения по специальности «Информационная безопасность автоматизированных систем», специализация «Защищенные автоматизированные системы управления» в результате обучения должны уметь и владеть следующими навыками решения задач:

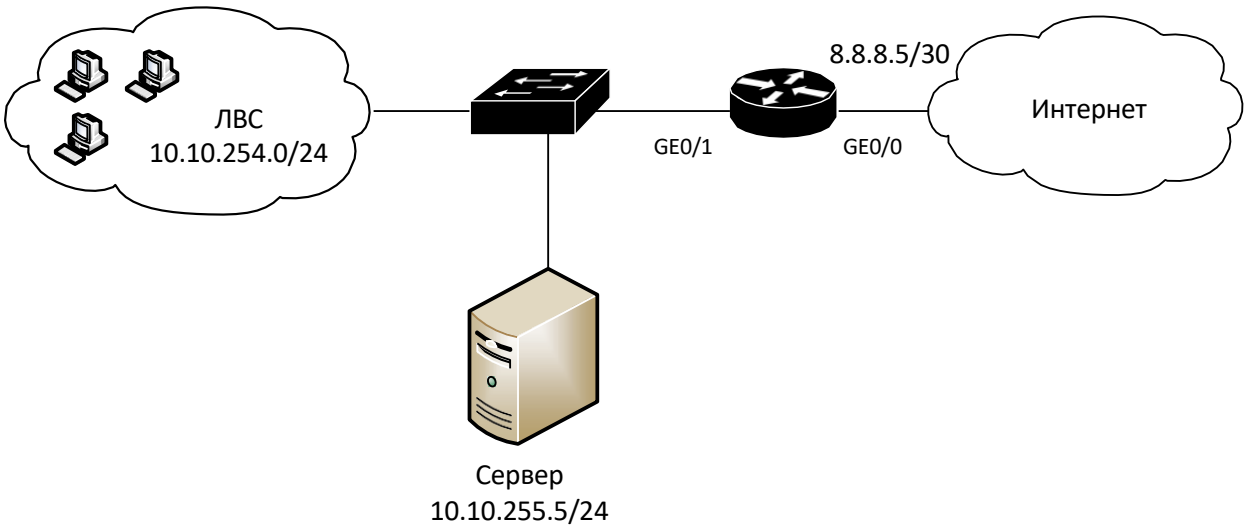
1. В компьютерной сети предприятия, представленной на схеме, имеется сегмент автоматизированных рабочих мест и серверный сегмент. Условием нормальной работы сети предприятия является взаимодействие АРМ сотрудников и сервера, доступ АРМ сотрудников в сеть интернет с инициированием соединения из ЛВС, доступ из сети интернет к web-сайту предприятия, размещенному на этом же сервере по протоколу HTTP, а также блокировка доступа к внешним сервисам DNS и NTP. Проанализируйте файл конфигурации маршрутизатора и поясните, будет ли выполнено условие нормальной работы сети предприятия. В случае невыполнения условия предложите изменения в конфигурацию для обеспечения требований.

Конфигурационный файл маршрутизатора предприятия:

```
!
!
interface GigabitEthernet0/0
ip address 8.8.8.5 255.255.255.252
ip nat outside
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/1.10
encapsulation dot1Q 10
ip address 10.10.254.1 255.255.255.0
ip nat inside
!
interface GigabitEthernet0/1.20
encapsulation dot1Q 20
ip address 10.10.255.1 255.255.255.0
ip nat inside
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
```

```
!
interface Vlan1
no ip address
shutdown
!
ip nat inside source list 101 interface GigabitEthernet0/0 overload
ip nat inside source static tcp 10.10.254.5 81 8.8.8.6 80
ip classless
!
ip flow-export version 9
!
!
access-list 101 permit ip 10.10.254.0 0.0.0.255 any
access-list 101 deny ip any any
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end
```

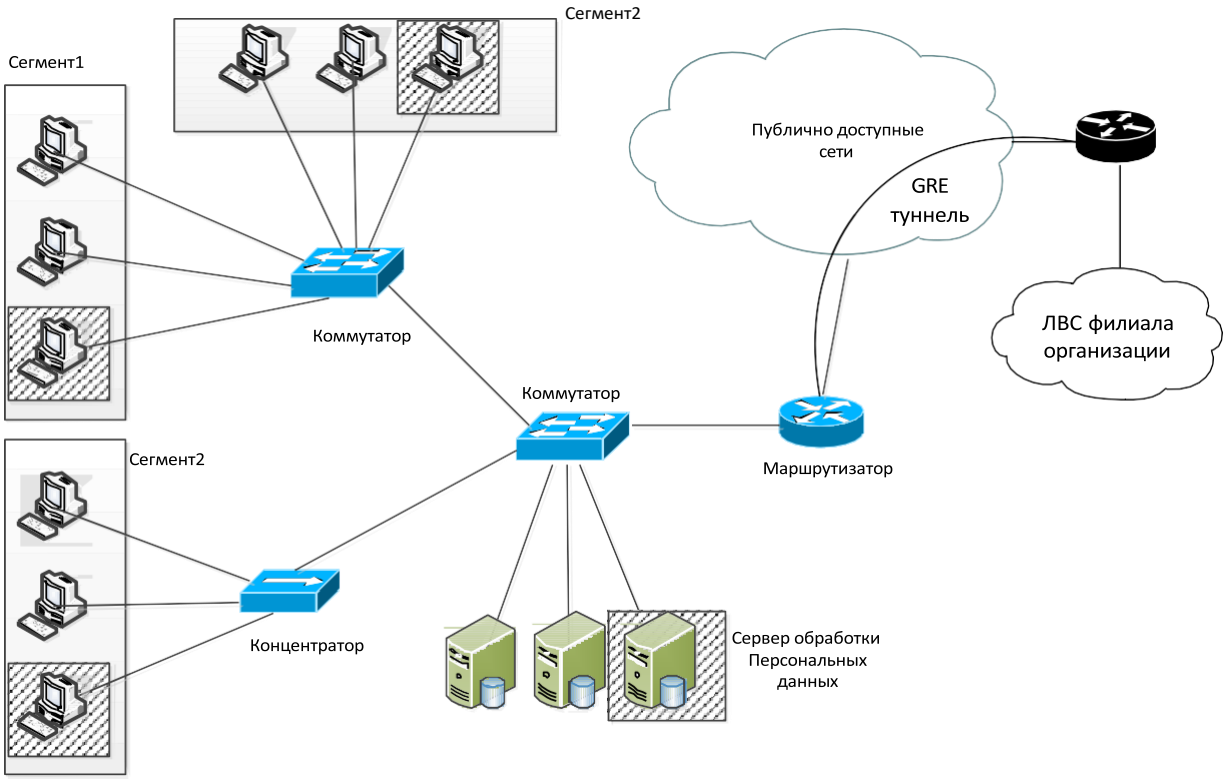
Схема сети предприятия:



2. В территориально-распределенной сети предприятия предполагается обработка персональных данных автоматизированным способом. Для ИСПДн необходимо обеспечить первый уровень защищенности (для ИСПДн актуальны угрозы 1-го типа в соответствии с ПП №1119 от 01.11.2012 года). Составленная модель угроз указывает на слабую защищенность передаваемой информации как внутри сети, так и по открытым

(неконтролируемым) каналам связи. Предложите и детально опишите решение по защите персональных данных, передаваемых по каналам связи внутри корпоративной сети предприятия и по открытым каналам связи. Штрихованной областью выделены рабочие места сотрудников, на которых предполагается обработка ПДн, дополнительно обработка ПДн предполагается на всех АРМ филиала.

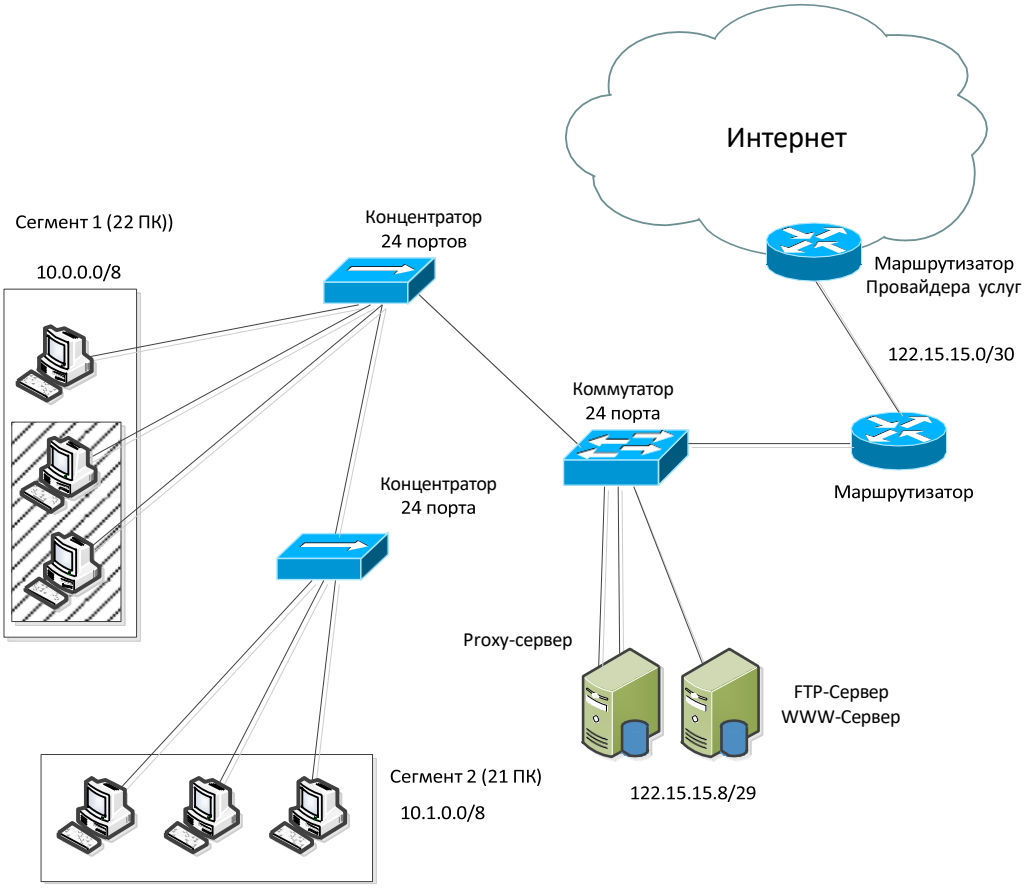
Схема сети организации:



3. На рисунке приведена структура ЛВС учреждения. Все серверное и сетевое оборудование установлено в специально оборудованных помещениях. Кабельная инфраструктура смонтирована вдоль стен на высоте 3м открытым способом. Доступ в сеть Интернет для всех сотрудников учреждения в сегменте №1 реализован через прокси-сервер. Доступ в сеть Интернет для всех сотрудников предприятия в сегменте №2 реализован посредством динамической трансляции адресов (NAPT), организованной на маршрутизаторе. Штрихованной областью выделены станции управления сетью.

Предложите организационные и технические мероприятия по повышению уровня информационной безопасности локального сегмента сети и серверного сегмента (в том числе с учетом замены активного оборудования). Обоснуйте каждое из предлагаемых мероприятий.

В техническом решении необходимо: обеспечить контроль и управляемость доступа к серверному сегменту как из ЛВС организации, так и из сети Интернет; обеспечить контролируемый доступ к внутренним ресурсам и сети Интернет для АРМ всех сотрудников учреждения; обеспечить защиту трафика внутри ЛВС средствами сетевого и телекоммуникационного оборудования от НСД, нарушения целостности и доступности.



4. На координаторе HW1 проверьте перечень туннелируемых ресурсов. Найдите и исправьте ошибку.

Исключите из диапазона туннелируемых координатором HW1 ресурсов IP-адрес компьютера, на котором функционирует программный комплекс ViPNet Client.

5. Проверьте корректность настройки межсетевого экрана туннелируемых узлов на координаторе HW1. Найдите и исправьте ошибку.

Уменьшите параметр MSS в настройках ViPNet Client на узле Клиент до значения 40 байт.

6. Настройки конфигурационного файла iplir на обоих координаторах верны, координаторы могут взаимодействовать по сети, но связи по зашифрованному каналу нет.

Какую системную настройку необходимо поменять для восстановления работоспособности защищенной сети ViPNet?

На координаторе HW2 настройте функцию DHCP на интерфейсе eth2 для автоматического присвоения IP-адреса узлам сети 192.168.2.0/27.

7. На координаторе HW2 настройте межсетевой экран таким образом, чтобы туннелируемые им узлы могли взаимодействовать с web-сайтами в сети Интернет.

На координаторе HW2 измените пароль для входа в пользовательский режим.

8. Настройте доступ к WEB-интерфейсу координатора HW1 для узла сети с IP-адресом 10.0.1.88/24.

На координаторе HW1 измените пароль для входа в привилегированный режим.

9. На координаторе HW2 настройте функцию L2overIP для взаимодействия с координатором HW1.

На координаторе HW1 измените пароль для входа в привилегированный режим.

10. На координаторе HW2 настройте межсетевой экран таким образом, чтобы туннелируемые им узлы могли взаимодействовать с web-сайтами в сети Интернет.

На координаторе HW2 измените пароль для входа в пользовательский режим.

11. Заполнить таблицу в соответствии с моделью разграничения доступом и актуальных угроз информационной безопасности баз данных в соответствии с заданными ресурсами.

Информационные ресурсы	Относительная ценность	Категории доступа	Угрозы
финансовая информация			
информация о товарообороте			
описание информационной системы			
описание систем защиты информации			

12. Заполнить таблицу в соответствии с моделью разграничения доступом в соответствии с заданными ресурсами.

	Категория пользователей 1	Категория пользователей 2
финансовая информация	Категории доступа	Категории доступа
информация о товарообороте	Категории доступа	Категории доступа
описание информационной системы	Категории доступа	Категории доступа
описание систем защиты информации	Категории доступа	Категории доступа

13. Заполнить таблицу в соответствии с актуальными угрозами информационной безопасности баз данных в соответствии с заданными ресурсами.

	Угроза 1	Угроза 2

финансовая информация	Источники и способы реализации	Источники и способы реализации
информация о товарообороте	Источники и способы реализации	Источники и способы реализации
описание информационной системы	Источники и способы реализации	Источники и способы реализации
описание систем защиты информации	Источники и способы реализации	Источники и способы реализации

14. Заполнить таблицу в соответствии с актуальными угрозами информационной безопасности баз данных в соответствии с заданными ресурсами.

	Угроза 1	**Угроза 2**
финансовая информация	Методы и средства защиты	Методы и средства защиты
информация о товарообороте	Методы и средства защиты	Методы и средства защиты
описание информационной системы	Методы и средства защиты	Методы и средства защиты
описание систем защиты информации	Методы и средства защиты	Методы и средства защиты

15. Составить фрагмент матрицы доступа на основе «Модели матрицы доступа» объектов БД, в которой содержится: финансовая информация, информация о товарообороте, описание информационной системы, описание систем защиты информации к соответствующим субъектам, а именно финансового директора, главного бухгалтера, системного администратора, администратора по безопасности.

16. Составить матрицу доступа, использующую “Модель Харрисона, Руззо и Ульмана” для БД, в которой содержится: финансовая информация, информация о товарообороте, описание информационной системы, описание систем защиты информации к соответствующим субъектам, а именно финансового директора, главного бухгалтера, системного администратора, администратора по безопасности.

17. Создать проект модели защищенной базы данных.

18. Разработать классификацию интерфейсов администратора баз данных.

19. Разработать подсистему защиты копии базы данных, с которой работает клиент.

20. Разработать систему защиты канала передачи данных между сервером и клиентами.

21. Определите какие из подсистем должны применяться для обеспечения безопасности локальной информационной системы, имеющей подключение к сети интернет и обрабатывающей информацию ограниченного распространения, не содержащую сведений, составляющих государственную тайну.

22. Определите какие из подсистем обеспечения безопасности должны применяться для информационной системы, распределённой по нескольким зданиям в пределах одной контролируемой территории и обрабатывающей информацию ограниченного распространения, не содержащую сведений, составляющих государственную тайну.

23. Определите какие из подсистем обеспечения безопасности должны применяться для информационной системы, распределённой по нескольким зданиям в пределах одной контролируемой территории, имеющей подключение к сети интернет и обрабатывающей

информацию ограниченного распространения, не содержащую сведений, составляющих государственную тайну.

24. Определите какие из подсистем обеспечения безопасности должны применяться для информационной системы, распределённой по нескольким зданиям в пределах одного населённого пункта, использующей для передачи защищаемой информации арендованные выделенные каналы связи, имеющей подключение к сети интернет и обрабатывающей информацию ограниченного распространения, не содержащую сведений, составляющих государственную тайну.

25. Определите какие из подсистем обеспечения безопасности должны применяться для информационной системы, распределённой по нескольким зданиям в пределах одного населённого пункта, использующей для передачи защищаемой информации сеть интернет и обрабатывающей информацию ограниченного распространения, не содержащую сведений, составляющих государственную тайну.

26. Проведите классификацию информационной системы по требованиям приказа ФСТЭК №17 имеющую региональный масштаб и средний уровень значимости.

27. Проведите классификацию информационной системы по требованиям приказа ФСТЭК №17 имеющую федеральный масштаб и средний уровень значимости.

28. Проведите классификацию информационной системы по требованиям приказа ФСТЭК №17 имеющую объектовый масштаб и средний уровень значимости.

29. Определите уровень защищённости в соответствии с требованиями постановления Правительства РФ №1119 для информационной системы, обрабатывающей биометрические персональные данные не сотрудников организации в объеме менее 100 000, для которой актуальны угрозы 3 типа.

30. Определите уровень защищённости в соответствии с требованиями постановления Правительства РФ №1119 для информационной системы, обрабатывающей иные персональные данные сотрудников организации в объеме более 100 000, для которой актуальны угрозы 1 типа.

6. Список рекомендуемой литературы

6.1. Основная литература:

1. Глухарев, М. Л.
    Технические средства защиты информации Электронный ресурс / Глухарев М. Л., Исаева М. Ф. : учебное пособие. - Санкт-Петербург : ПГУПС, 2018. - 55 с. - ISBN 978-5-7641-112-4, экземпляров неограничено

2. Ермакова, А. Ю.
    Методы и средства защиты компьютерной информации Электронный ресурс / Ермакова А. Ю. : учебное пособие. - Москва : РТУ МИРЭА, 2020. - 223 с., экземпляров неограничено

3. Комаров, С. А.
    Правовое регулирование обеспечения информационной безопасности и защиты персональных данных : монография / С.А. Комаров, Е.В. Мицкая ; под ред. С. А. Комарова. - Москва|Берлин : Директ-Медиа, 2019. - 169 с. - http://biblioclub.ru/. - Библиогр.: с. 129-140., экземпляров неограничено

4. Кукарцев, В. В. Теория баз данных Электронный ресурс : Учебник / В. В. Кукарцев, Р. Ю. Царев, О. А. Антамошкин. - Красноярск : Сибирский федеральный университет, 2017. - 180 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 978-5-7638-3621-9, экземпляров неограничено

5. Лапонина, О.Р.
    Межсетевое экранирование Электронный ресурс : учебное пособие / О.Р. Лапонина. - Межсетевое экранирование,2020-07-28. - Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. - 344 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-4487-0078-1, экземпляров неограничено

6. Мальцев, В. А.
    Правовое обеспечение информационной безопасности в российской федерации Электронный ресурс / Мальцев В.

А. : учебно-методическое пособие. - Воронеж : ВГУ, 2017. - 40 с., экземпляров неограничено

7. Мирошников, А. И.
    Архитектура систем управления базами данных Электронный ресурс : Учебное пособие / А. И. Мирошников. - Липецк : Липецкий государственный технический университет, ЭБС АСВ, 2018. - 94 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 978-5-88247-879-6, экземпляров неограничено

8. Никифоров, С. Н.
    Методы защиты информации. Шифрование данных Электронный ресурс / Никифоров С. Н. : учебное пособие. - 2-е изд., стер. - Санкт-Петербург : Лань, 2019. - 160 с. - ISBN 978-5-8114-4042-9, экземпляров неограничено

9. Рагозин Ю.Н. Инженерно-техническая защита информации [Электронный ресурс] : учебное пособие по физическим основам образования технических каналов утечки информации и по практикуму оценки их опасности / Ю.Н. Рагозин. — Электрон. текстовые данные. — СПб. : Интермедия, 2018. — 168 c. — 978-5-4383-0161-5. — Режим доступа: http://www.iprbookshop.ru/73641.html

10. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства Электронный ресурс : Учебно-методическое пособие / Д. В. Фомин. - Саратов : Вузовское образование, 2018. - 218 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 978-5-4487-0297-6, экземпляров неограничено

11. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 c. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html

6.2. Дополнительная литература:

1. Алексеев В.А. Основы проектирования и реализации баз данных [Электронный ресурс] : методические указания к проведению лабораторных работ по курсу «Базы данных» / В.А. Алексеев. — Электрон. текстовые данные. — Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2014. — 26 c. — 2227-8397. http://www.iprbookshop.ru/55122.html

2. Безопасность систем баз данных [Электронный ресурс] : учебное пособие / А.В. Скрыпников [и др.]. — Электрон. текстовые данные. — Воронеж: Воронежский государственный университет инженерных технологий, 2015. — 144 c. — 978-5-00032-122-5. http://www.iprbookshop.ru/50628.html

3. Бехроуз, А.
    Криптография и безопасность сетей Электронный ресурс : учебное пособие / Фороузан А. Бехроуз ; ред. А.Н. Берлин. - Криптография и безопасность сетей,2020-11-14. - Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. - 782 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-4487-0143-6, экземпляров неограничено

4. Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 c. — 978-5-94774-821-5. http://www.iprbookshop.ru/52209.html

5. Голиков, А.М.
    Защита информации от утечки по техническим каналам Электронный ресурс : учебное пособие / А.М. Голиков. - Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. - 256 с. - Книга находится в базовой версии ЭБС IPRbooks., экземпляров неограничено

6. Кармановский, Н. С. Организационно-правовое и методическое обеспечение информационной безопасности Электронный ресурс : Учебное пособие / Н. С.

Кармановский, О. В. Михайличенко, Н. Н. Прохожев. - Организационно-правовое и методическое обеспечение информационной безопасности,2022-10-01. - Санкт-Петербург : Университет ИТМО, 2016. - 169 c. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 2227-8397, экземпляров неограничено

7. Кубанков А.Н. Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект [Электронный ресурс] : учебное пособие / А.Н. Кубанков, Н.Н. Куняев. — Электрон. текстовые данные. — М. : Всероссийский государственный университет юстиции (РПА Минюста России), 2014. — 78 c. — 978-5-89172-850-9. — Режим доступа: http://www.iprbookshop.ru/47262.html

8. Лапина М.А. Информационное право [Электронный ресурс] : учебное пособие для студентов вузов, обучающихся по специальности 021100 «Юриспруденция» / М.А. Лапина, А.Г. Ревин, В.И. Лапин. — Электрон. текстовые данные. — М. : ЮНИТИ-ДАНА, 2015. — 335 c. — 5-238-00798-1. — Режим доступа: http://www.iprbookshop.ru/52038.html

9. Мэйволд, Э.
    Безопасность сетей / Э. Мэйволд. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 572 c. : схем., ил. - http://biblioclub.ru/, экземпляров неограничено

10. Платонов, В. В. Программно-аппаратные средства защиты информации: учебник / В.В. Платонов. - М.: Академия, 2013. - 336 с.: ил. - (Высшее профессиональное образование) (Бакалавриат). - Прил.: с. 310-325. - Библиогр.: с. 326-327. http://www.iprbookshop.ru/366.html

11. Прохорова, О. В.
    Информационная безопасность и защита информации Электронный ресурс / Прохорова О. В. - 2-е изд., испр. - Санкт-Петербург : Лань, 2020. - 124 c. - ISBN 978-5-8114-4404-5, экземпляров неограничено

12. Тумбинская, М. В.
    Комплексное обеспечение информационной безопасности на предприятии Электронный ресурс / Тумбинская М. В., Петровский М. В. : учебник. - Санкт-Петербург : Лань, 2019. - 344 c. - ISBN 978-5-8114-3940-9, экземпляров неограничено

13. Щеглов, А. Ю.
    Математические модели и методы формального проектирования систем защиты информационных систем Электронный ресурс : Учебное пособие / А. Ю. Щеглов, К. А. Щеглов. - Математические модели и методы формального проектирования систем защиты информационных систем,2022-10-01. - Санкт-Петербург : Университет ИТМО, 2015. - 93 c. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 2227-8397, экземпляров неограничено

7. Организация и проведение государственного экзамена

Организация и проведение государственного экзамена строится в соответствии с основными требованиями «Положения о порядке проведения государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры в федеральном государственном автономном образовательном учреждении высшего образования «Северо-Кавказский федеральный университет», (новая редакция), утвержденного Ученым советом СКФУ от 07.12.2017 г., протокол № 4.

Организационная подготовка к государственному экзамену проводится выпускающей кафедрой, учебно-методическим управлением в сроки, предусмотренные графиком учебного процесса.

Выпускающая кафедра разрабатывает программу государственного экзамена. Структура и содержание государственного экзамена определяется требованиями образовательного стандарта высшего образования Северо-Кавказского федерального университета по специальности 10.05.03 Информационная безопасность автоматизированных систем

Заведующие выпускающими кафедрами не позднее, чем за шесть месяцев до начала ГИА доводят до сведения обучающихся порядок проведения государственных

аттестационных испытаний (порядок подачи и рассмотрения апелляций), обеспечивают студентов программами ГИА, создают необходимые для подготовки условия и организуют проведение предэкзаменационных консультаций.

За 1 месяц до проведения государственного экзамена заведующие выпускающими кафедрами формируют и утверждают на заседании кафедры экзаменационные билеты.

Прием государственного экзамена проводится на заседании экзаменационной комиссии с участием не менее двух третий ее списочного состава.

Для работы экзаменационной комиссии секретарь данной комиссии представляет следующие документы: справки о выполнении учебного плана по каждому студенту, допущенного к ГИА в соответствии с приказом ректора СКФУ, экзаменационную ведомость по итогам проведения государственного экзамена.

Государственный экзамен проводится в сроки, установленные приказом ректора в соответствии с утвержденным графиком, который доводится до сведения.

При сдаче государственного экзамена допускается присутствие в аудитории не более 10 студентов. Каждый студент самостоятельно выбирает экзаменационный билет один раз посредством произвольного извлечения. Номер билета фиксируется секретарем ГЭК в соответствующем протоколе.

На подготовку к ответу предоставляется, как правило, 30 минут. При подготовке студент имеет право пользоваться программой государственного экзамена, а также с разрешения ГЭК – справочной литературой. Студенты, использующие при подготовке к ответу другую учебную литературу, с государственного экзамена удаляются. В протоколе данному студенту заносится запись «неудовлетворительно», студент удален с государственного экзамена за списывания. В экзаменационной ведомости студенту проставляется оценка «неудовлетворительно».

По окончанию ответа студента председатель и члены экзаменационной комиссии имеют право задавать дополнительные вопросы (как правило, не более трех). Секретарь комиссии вносит в протокол вопросы билета, дополнительные вопросы членов комиссии, а также общую характеристику ответа студента на все вопросы.

Продолжительность ответа на вопрос билета и дополнительные вопросы занимает, как правило, 30 минут.

После совещания комиссии в аудиторию приглашаются студенты и председатель комиссии объявляет результаты государственного экзамена. Результаты экзамена объявляются в день сдачи экзамена после оформления в установленном порядке протоколов заседаний экзаменационных комиссий и заполнения зачетных книжек студентов, в которых расписывается председатель и члены экзаменационной комиссии.

Студенты, не явившиеся на сдачу экзамена по уважительной причине, вправе пройти ее в течение 6 месяцев после завершения государственной итоговой аттестации. Студенты, получившие оценку «неудовлетворительно» или не явившиеся на сдачу экзамена по неуважительной причине, отчисляются.

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. 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. Срок проведения апелляции назначается в момент написания заявления обучающимся и доводится до его сведения под роспись. Решение

апелляционной комиссии является окончательным и пересмотру не подлежит. Апелляция на повторное проведение государственного аттестационного испытания не принимается.

8. Описание показателей и критериев оценивания компетенций, а также шкал оценивания
8.1 Описание показателей

Уровни сформированност и компетенци(ий), индикатора (ов)	Дескрипторы			
	Минимальный уровень не достигнут (неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
Компетенция: *ОПК-5*				
Результаты обучения: *Индикатор*: ИД-1$_{ОПК-5}$	Не предоставляет план по использованию Законодательства Российской Федерации в области информационной безопасности и защиты информации; систем защиты государственной тайны с перечнем сведений относящихся к конфиденциальной информации и способы ее защиты; принципов электронной подписи (ЭП); различных видов компьютерных вирусов; классификаций компьютерных преступлений; понятий и способов защиты интеллектуальной собственности; международного и российского права в области защиты информации; способов совершения преступлений в сфере компьютерной информации; правовых режимов защиты информации.	Предоставляет не полный план по использованию Законодательства Российской Федерации в области информационной безопасности и защиты информации; систем защиты государственной тайны с перечнем сведений относящихся к конфиденциальной информации и способы ее защиты; принципов электронной подписи (ЭП); различных видов компьютерных вирусов; классификаций компьютерных преступлений; понятийи способов защиты интеллектуальной собственности; международного и российского права в области защиты информации; способов совершения преступлений в сфере компьютерной информации; правовых режимов защиты информации	Предоставляет план по использованию Законодательства Российской Федерации в области информационно й безопасности и защиты информации; систем защиты государственной тайны с перечнем сведений относящихся к конфиденциальн ой информации и способы ее защиты; принципов электронной подписи (ЭП); различных видов компьютерных вирусов; классификаций компьютерных преступлений; понятий и способов защиты интеллектуально й собственности; международного и российского права в области защиты информации; способов совершения преступлений в сфере компьютерной информации; правовых режимов защиты информации.	Предоставляет детально проработанный план по использованию Законодательства Российской Федерации в области информационной безопасности и защиты информации; систем защиты государственной тайны с перечнем сведений относящихся к конфиденциально й информации и способы ее защиты; принципов электронной подписи (ЭП); различных видов компьютерных вирусов; классификаций компьютерных преступлений; понятий и способов защиты интеллектуальной собственности; международного и российского права в области защиты информации; способов совершения преступлений в сфере компьютерной информации; правовых режимов защиты информации.

Результаты обучения: *Индикатор*: ИД-2$_{ОПК-5}$	Не предоставляет план по организации защиты на объекте; организации работы персонала с конфиденциальной информацией; разработке проектов нормативных документов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов	Предоставляет неполный план по организации защиты на объекте; организации работы персонала с конфиденциальн ой информацией; разработке проектов нормативных документов, регламентирую щих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов	Предоставляет план по организации защиты на объекте; организации работы персонала с конфиденциальн ой информацией; разработке проектов нормативных документов, регламентирую щих работу по защите информации, а также положений, инструкций и других организационно-распорядительн ых документов	Предоставляет детально проработанный план по организации защиты на объекте; организации работы персонала с конфиденциальной информацией; разработке проектов нормативных документов, регламентирующи х работу по защите информации, а также положений, инструкций и других организационно- распорядительны х документов
Результаты обучения: *Индикатор*: ИД-3$_{ОПК-5}$	Не предоставляет отчет с демонстрацией способности применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	Предоставляет неполный отчет с демонстрацией способности применять нормативные правовые акты, нормативные и методические документы, регламентирую щие деятельность по защите информации	Предоставляет отчет с демонстрацией способности применять нормативные правовые акты, нормативные и методические документы, регламентирую щие деятельность по защите информации	Предоставляет детальный отчет с демонстрацией способности применять нормативные правовые акты, нормативные и методические документы, регламентирующи е деятельность по защите информации
Компетенция: *ОПК-6*				
Результаты обучения: *Индикатор*: ИД-1$_{ОПК-6}$	С грубыми ошибками определяет критерии технологических процессов защиты информации для сопоставления с требованиями нормативных документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	С небольшими ошибками определяет критерии технологических процессов защиты информации для сопоставления с требованиями нормативных документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Некорректно определяет критерии технологических процессов защиты информации для сопоставления с требованиями нормативных документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	определяет критерии технологических процессов защиты информации для сопоставления с требованиями нормативных документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

Результаты обучения: *Индикатор*: ИД-2$_{ОПК-6}$	С грубыми ошибками разрабатывает проекты инструкций, регламентов, положений и приказов по защите информации ограниченного доступа в организации; определяет политику контроля доступа работников к информации ограниченного доступа	С небольшими ошибками разрабатывает проекты инструкций, регламентов, положений и приказов по защите информации ограниченного доступа в организации; определяет политику контроля доступа работников к информации ограниченного доступа	Некорректно разрабатывает проекты инструкций, регламентов, положений и приказов по защите информации ограниченного доступа в организации; определяет политику контроля доступа работников к информации ограниченного доступа	разрабатывает проекты инструкций, регламентов, положений и приказов по защите информации ограниченного доступа в организации; определяет политику контроля доступа работников к информации ограниченного доступа
Результаты обучения: *Индикатор*: ИД-3$_{ОПК-6}$	С грубыми ошибками применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерных систем и сетей	С ошибками применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерных систем и сетей	Некорректно применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерных систем и сетей	применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерных систем и сетей
Компетенция: *ОПК-9*				
Результаты обучения: *Индикатор*: ИД-1$_{ОПК-9}$	Не подбирает: -содержания этапов построения компьютерных сетей; -эталонных моделей взаимодействия открытых систем; -принципов построения и функционирования систем и сетей передачи информации; типовых структур и принципов организации компьютерных сетей; основных телекоммуникационных протоколов; перспектив развития компьютерных сетей	Подбирает с грубыми ошибками: -содержания этапов построения компьютерных сетей; -эталонных моделей взаимодействия открытых систем; -принципов построения и функционирования систем и сетей передачи информации; типовых структур и принципов организации компьютерных сетей; основных телекоммуникационных протоколов; перспектив развития компьютерных сетей	Подбирает: -содержания этапов построения компьютерных сетей; -эталонных моделей взаимодействия открытых систем; -принципов построения и функционирования систем и сетей передачи информации; типовых структур и принципов организации компьютерных сетей; основных телекоммуникационных протоколов; перспектив развития компьютерных сетей	Подбирает и может обьяснить: -содержания этапов построения компьютерных сетей; -эталонных моделей взаимодействия открытых систем; -принципов построения и функционирования систем и сетей передачи информации; типовых структур и принципов организации компьютерных сетей; основных телекоммуникационных протоколов; перспектив развития компьютерных сетей

Результаты обучения: *Индикатор*: ИД-2$_{ОПК-9}$	Не умеет пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет; разрабатывает сетевые проекты с использованием базовых технологий; - оценивает работоспособность сетевых проектов; исследует характеристики сетевой активности созданных проектов.	На низком уровне пользуется сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет; разрабатывает сетевые проекты с использованием базовых технологий; - оценивает работоспособность сетевых проектов; исследует характеристики сетевой активности созданных проектов.	пользуется сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет; разрабатывает сетевые проекты с использованием базовых технологий; - оценивает работоспособность сетевых проектов; исследует характеристики сетевой активности созданных проектов.	Подбирает и пользуется сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет; разрабатывает сетевые проекты с использованием базовых технологий; - оценивает работоспособность сетевых проектов; исследует характеристики сетевой активности созданных проектов.
Результаты обучения: *Индикатор*: ИД-3$_{ОПК-9}$	Не выбирает оптимальный способ решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития сетей и систем передачи информации.	выбирает не оптимальный способ решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития сетей и систем передачи информации.	выбирает оптимальный способ решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития сетей и систем передачи информации.	выбирает лучший способ решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития сетей и систем передачи информации.
Компетенция: *ОПК-12*				
Результаты обучения: *Индикатор*: ИД-1$_{ОПК-12}$	Не предоставляет отчет, с пояснением в котором описывает операционные системы; критерии оценки эффективности и надежности средств защиты операционных систем; принципы организации и структуру подсистем защиты операционных систем семейства UNIX и Windows; функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами.	Предоставляет неполный отчет с пояснением в котором описывает операционные системы; критерии оценки эффективности и надежности средств защиты операционных систем; принципы организации и структуру подсистем защиты операционных систем семейства UNIX и Windows; функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами.	Предоставляет отчет, с полным пояснением в котором описывает операционные системы; критерии оценки эффективности и надежности средств защиты операционных систем; принципы организации и структуру подсистем защиты операционных систем семейства UNIX и Windows; функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами.	Предоставляет детальный отчет с полным пояснением в котором описывает операционные системы; критерии оценки эффективности и надежности средств защиты операционных систем; принципы организации и структуру подсистем защиты операционных систем семейства UNIX и Windows; функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами.

Результаты обучения: *Индикатор*: ИД-2$_{ОПК-12}$	Не предоставляет отчет, где демонстрирует способность использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; оценивать эффективность и надёжность защиты операционных систем; планировать политику безопасности операционных систем.	Предоставляет неполный отчет где демонстрирует способность использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; оценивать эффективность и надёжность защиты операционных систем; планировать политику безопасности операционных систем.	Предоставляет отчет, где демонстрирует способность использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; оценивать эффективность и надёжность защиты операционных систем; планировать политику безопасности операционных систем.	Предоставляет детальный отчет, где демонстрирует способность использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; оценивать эффективность и надёжность защиты операционных систем; планировать политику безопасности операционных систем.
Результаты обучения: *Индикатор*: ИД-3$_{ОПК-12}$	Не предоставляет отчет, где демонстрирует способность применять знания в области безопасности операционных систем при разработке автоматизированных систем.	Предоставляет неполный отчет где демонстрирует способность применять знания в области безопасности операционных систем при разработке автоматизированных систем.	Предоставляет отчет, где демонстрирует способность применять знания в области безопасности операционных систем при разработке автоматизированных систем.	Предоставляет детальный отчет, где демонстрирует способность применять знания в области безопасности операционных систем при разработке автоматизированных систем.
Компетенция: *ПК-1*				
Результаты обучения: *Индикатор*: ИД-3$_{ПК-1}$	Не предоставляет отчёт по результатам проведения анализа безопасности компьютерных систем.	Предоставляет неполный отчёт по результатам проведения анализа безопасности компьютерных систем.	Предоставляет отчёт по результатам проведения анализа безопасности компьютерных систем.	Предоставляет детальный отчёт по результатам проведения анализа безопасности компьютерных систем.
Результаты обучения: *Индикатор*: ИД-4$_{ПК-1}$	Не предоставляет отчёт по результатам проведения сертификации программно-аппаратных средств защиты информации и анализ результатов.	Предоставляет неполный отчёт по результатам проведения сертификации программно-аппаратных средств защиты информации и анализ результатов.	Предоставляет по результатам проведения сертификации программно-аппаратных средств защиты информации и анализ результатов.	Предоставляет по результатам проведения сертификации программно-аппаратных средств защиты информации и анализ результатов.
Результаты обучения: *Индикатор*: ИД-5$_{ПК-1}$	Не предоставляет отчёт по результатам проведения инструментального мониторинга защищенности компьютерных систем и сетей.	Предоставляет неполный отчёт по результатам проведения инструментального мониторинга защищенности компьютерных систем и сетей.	Предоставляет отчёт по результатам проведения инструментального мониторинга защищенности компьютерных систем и сетей.	Предоставляет детальный отчёт по результатам проведения инструментального мониторинга защищенности компьютерных систем и сетей.
Результаты обучения: *Индикатор*: ИД-6$_{ПК-1}$	Не предоставляет отчёт по результатам проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов.	Предоставляет неполный отчёт по результатам проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов.	Предоставляет отчет по результатам проведения экспертизы при расследовании компьютерных преступлений, правонарушений и	Предоставляет детальный отчёт по результатам проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов.

			инцидентов.	
Компетенция: *ПК-3*				
Результаты обучения: *Индикатор*: ИД-1$_{ПК-3}$	Не предоставляет отчёт по результатам разработки технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок.	Предоставляет неполный отчёт по результатам разработки технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок.	Предоставляет отчёт по результатам разработки технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок.	Предоставляет детальный отчёт по результатам разработки технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок.
Результаты обучения: *Индикатор*: ИД-2$_{ПК-3}$	Не предоставляет отчёт по результатам разработки технических средств защиты акустической речевой информации от утечки по техническим каналам.	Предоставляет неполный отчёт по результатам разработки технических средств защиты акустической речевой информации от утечки по техническим каналам.	Предоставляет отчёт по результатам разработки технических средств защиты акустической речевой информации от утечки по техническим каналам.	Предоставляет детальный отчёт по результатам разработки технических средств защиты акустической речевой информации от утечки по техническим каналам.
Результаты обучения: *Индикатор*: ИД-3$_{ПК-3}$	Не предоставляет отчёт по результатам разработки программно- технических средств защиты информации от несанкционированного доступа.	Предоставляет неполный отчёт по результатам разработки программно- технических средств защиты информации от несанкционированного доступа.	Предоставляет отчёт по результатам разработки программно- технических средств защиты информации от несанкционированного доступа.	Предоставляет детальный отчёт по результатам разработки программно-технических средств защиты информации от несанкционированного доступа.
Результаты обучения: *Индикатор*: ИД-4$_{ПК-3}$	Не предоставляет отчёт по результатам разработки технических средств контроля эффективности мер защиты информации от утечки за счет побочных электромагнитных излучений и наводок.	Предоставляет неполный отчёт по результатам разработки технических средств контроля эффективности мер защиты информации от утечки за счет побочных электромагнитных излучений и наводок.	Предоставляет отчёт по результатам разработки технических средств контроля эффективности мер защиты информации от утечки за счет побочных электромагнитных излучений и наводок.	Предоставляет детальный отчёт по результатам разработки технических средств контроля эффективности мер защиты информации от утечки за счет побочных электромагнитных излучений и наводок.
Результаты обучения: *Индикатор*: ИД-5$_{ПК-3}$	Не предоставляет отчёт по результатам разработки технических средств контроля эффективности мер защиты акустической речевой информации от утечки по техническим каналам.	Предоставляет неполный отчёт по результатам разработки технических средств контроля эффективности мер защиты акустической речевой информации от утечки по техническим каналам.	Предоставляет отчёт по результатам разработки технических средств контроля эффективности мер защиты акустической речевой информации от утечки по техническим каналам.	Предоставляет детальный отчёт по результатам разработки технических средств контроля эффективности мер защиты акустической речевой информации от утечки по техническим каналам.
Результаты обучения: *Индикатор*: ИД-6$_{ПК-3}$	Не предоставляет отчёт по результатам разработки программных (программно-технических) средств контроля	Предоставляет неполный отчёт по результатам разработки программных (программно-технических) средств контроля	Предоставляет отчёт по результатам разработки программных (программно-технических) средств	Предоставляет детальный отчёт по результатам разработки программных (программно- технических) средств контроля защищенности информации от

	защищенности информации от несанкционированного доступа.	защищенности информации от несанкционированного доступа.	контроля защищенности информации от несанкционированного доступа.	несанкционированного доступа.
Компетенция: *ПК-7*				
Результаты обучения: *Индикатор*: ИД-1$_{ПК-7}$	Не предоставляет отчёт по результатам создания системы защиты информации в организации.	Предоставляет неполный отчёт по результатам создания системы защиты информации в организации.	Предоставляет отчёт по результатам создания системы защиты информации в организации.	Предоставляет детальный отчёт по результатам создания системы защиты информации в организации.
Результаты обучения: *Индикатор*: ИД-2$_{ПК-7}$	Не предоставляет отчёт по результатам ввода в эксплуатацию системы защиты информации в организации.	Предоставляет неполный отчёт по результатам ввода в эксплуатацию системы защиты информации в организации.	Предоставляет отчёт по результатам ввода в эксплуатацию системы защиты информации в организации.	Предоставляет детальный отчёт по результатам ввода в эксплуатацию системы защиты информации в организации.
Результаты обучения: *Индикатор*: ИД-3$_{ПК-7}$	Не предоставляет отчёт по результатам сопровождения системы защиты информации в ходе ее эксплуатации.	Предоставляет неполный отчёт по результатам сопровождения системы защиты информации в ходе ее эксплуатации.	Предоставляет отчёт по результатам сопровождения системы защиты информации в ходе ее эксплуатации.	Предоставляет детальный отчёт по результатам сопровождения истемы защиты информации в ходе ее эксплуатации.
Компетенция: *ПК-8*				
Результаты обучения: *Индикатор*: ИД-1$_{ПК-8}$	Не может тестировать системы защиты информации автоматизированных систем.	С ошибками тестирует системы защиты информации автоматизированных систем.	Не до конца тестирует системы защиты информации автоматизированных систем.	Тестирует системы защиты информации автоматизированных систем.
Результаты обучения: *Индикатор*: ИД-2$_{ПК-8}$	Не может разрабатывать проектные решения по защите информации в автоматизированных системах.	С ошибками разрабатывает проектные решения по защите информации в автоматизированных системах.	Не до конца разрабатывает проектные решения по защите информации в автоматизированных системах.	разрабатывает проектные решения по защите информации в автоматизированных системах.
Результаты обучения: *Индикатор*: ИД-3$_{ПК-8}$	Не может разрабатывать эксплуатационную документацию на системы защиты информации автоматизированных систем.	С ошибками разрабатывает эксплуатационную документацию на системы защиты информации автоматизированных систем.	Не до конца разрабатывает эксплуатационную документацию на системы защиты информации автоматизированных систем.	Разрабатывает эксплуатационную документацию на системы защиты информации автоматизированных систем.
Результаты обучения: *Индикатор*: ИД-4$_{ПК-8}$	Не может разрабатывать программные и программно-аппаратные средства для систем защиты информации автоматизированных систем.	С ошибками разрабатывает программные и программно-аппаратные средства для систем защиты информации автоматизированных систем.	Не до конца разрабатывает программные и программно-аппаратные средства для систем защиты информации автоматизированных систем.	Разрабатывает программные и программно- аппаратные средства для систем защиты информации автоматизированных систем.

Компетенция: *ПК-9*				
Результаты обучения: *Индикатор*: ИД-1$_{ПК-8}$	Не предоставляет отчет с обоснованием необходимости защиты информации в автоматизированной системе.	Предоставляет неполный отчет с обоснованием необходимости защиты информации в автоматизированной системе.	Предоставляет отчет с обоснованием необходимости защиты информации в автоматизированной системе.	Предоставляет детальный отчет с обоснованием необходимости защиты информации в автоматизированной системе.
Результаты обучения: *Индикатор*: ИД-2$_{ПК-8}$	Не предоставляет отчёт по результатам определения угроз безопасности информации, обрабатываемой автоматизированной системой.	Предоставляет неполный отчёт по результатам определения угроз безопасности информации, обрабатываемой автоматизированной системой.	Предоставляет отчёт по результатам определения угроз безопасности информации, обрабатываемой автоматизированной системой.	Предоставляет детальный отчёт по результатам определения угроз безопасности информации, обрабатываемой автоматизированной системой.
Результаты обучения: *Индикатор*: ИД-3$_{ПК-8}$	Не предоставляет отчёт по результатам разработки архитектуры системы защиты информации автоматизированной системы.	Предоставляет неполный отчёт по результатам разработки архитектуры системы защиты информации автоматизированной системы.	Предоставляет отчёт по результатам разработки архитектуры системы защиты информации автоматизированной системы.	Предоставляет детальный отчёт по результатам разработки архитектуры системы защиты информации автоматизированной системы.
Результаты обучения: *Индикатор*: ИД-4$_{ПК-8}$	Не предоставляет отчёт по результатам моделирования защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации.	Предоставляет неполный отчёт по результатам моделирования защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации.	Предоставляет отчёт по результатам моделирования защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации.	Предоставляет детальный отчёт по результатам моделирования защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации.

8.2 Критерии оценивания компетенций на государственном экзамене

Итоги государственного экзамена Государственная экзаменационная комиссия подводит на закрытом заседании. Решение об оценках принимается простым большинством голосов членов комиссии, участвующих в заседании.

В качестве критериев оценки ответа студентов выделяются:

– полнота раскрытия вопросов экзаменационного билета,

– логичность и последовательность изложения материала,

– аргументированность ответа студента,

– способность анализировать и сравнивать различные подходы к решению поставленной проблемы,

– готовность студента отвечать на дополнительные вопросы по существу экзаменационного билета.

Результаты государственного экзамена оцениваются как «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» выставляется студенту, верно ответившему на вопросы экзаменационного билета и дополнительные вопросы, глубоко и прочно усвоившему программный материал, исчерпывающе, последовательно, грамотно и логично его излагающему, в ответе которого тесно связываются теория с практикой. При этом студент не затрудняется с ответом при видоизменении задания, свободно справляется с задачами, вопросами и другими видами применения знаний, показывает знакомство с монографической литературой, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практической работы.

Оценка «хорошо» выставляется студенту, верно ответившему на 80% вопросов экзаменационного билета и дополнительных вопросов, твердо знающему программный материал, грамотно и по существу излагающему его, не допускающему существенных неточностей в ответе на вопрос, правильно применяющему теоретические положения при решении практических вопросов и задач, владеющему необходимыми знаниями и приемами их выполнения, демонстрирующему хорошие знания учебной литературы, нормативных актов, обладающему навыками анализа источников, знающему основные проблемы дисциплины, умеющему устанавливать основные причинно-следственные связи;

Оценка «удовлетворительно» выставляется студенту, верно ответившему на 60% вопросов экзаменационного билета и дополнительных вопросов, который имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, испытывает затруднения в применении нормативных актов.

Как правило, оценка «удовлетворительно» выставляется студентам, допустившим погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладающих необходимыми знаниями для их устранения под руководством преподавателя.

Оценка «неудовлетворительно» выставляется студенту, верно ответившему менее чем на 60% вопросов экзаменационного билета и не ответившему на дополнительные вопросы, демонстрирующему слабое знание содержания дисциплины, плохо ориентирующемуся в основных понятиях курса, не знающему значительной части программного материала, допускающему существенные ошибки, неуверенно с большим затруднением формулирующему практические знания, слабо владеющему законодательным материалом, не умеющему устанавливать причинно-следственные связи.

Студент, не сдавший государственный экзамен, не имеет права быть допущенным к защите выпускной квалификационной работы. Студент, не прошедший итоговые аттестационные испытания, отчисляется из вуза.

8.3. Описание шкалы оценивания

Государственный экзамен оценивается по 5-балльной системе.