

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Узунов Федор Владимирович

Должность: Ректор

Дата подписания: 30.09.2026 08:54:44

Уникальный программный ключ: fd935d10451b860e912264c0378f8418452b603f94388008a29877a6bcbf5

**АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
«ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ»**

«УНИВЕРСИТЕТ ЭКОНОМИКИ И УПРАВЛЕНИЯ»

Факультет экономики, управления и юриспруденции

Кафедра управления и бизнес-информатики



УТВЕРЖДАЮ

Проректор по учебно-
методической работе

Г.П. Узунова

«02» февраля 2026 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

**КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА
ИНФОРМАЦИИ**

Направление подготовки

10.03.01 «Информационная безопасность»

Профиль

Безопасность компьютерных систем

Квалификация выпускника: бакалавр

Для всех
форм обучения

Симферополь, 2026 г.

1. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

Средства оценивания в ходе текущего контроля:

- устные опросы в ходе семинарских занятий;
- рефераты;
- тестирование;
- практические задания, выполняемые в ходе семинарского (практического) занятия или рекомендуемые для самостоятельной работы.

Коды компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения по дисциплине
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты соответствующих проектных решений	ОПК-10.1. Выбирает принципы формирования политики информационной безопасности в информационных системах ОПК-10.2. Подбирает и конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности

1.1 Вопросы к текущему контролю

1. Понятие «объект информатизации» (ОИ). Классификация объектов по категориям важности обрабатываемой информации согласно требованиям регуляторов РФ (ФСТЭК/ФСБ).
2. Этапы создания комплексной системы защиты информации (КСЗИ) на объекте: от предпроектного обследования до ввода в эксплуатацию.
3. Модель угроз безопасности информации: порядок построения, источники угроз, уязвимости и способы реализации угроз применительно к конкретному объекту.
4. Роль аттестационных испытаний объектов информатизации. Перечень документов, необходимых для аттестации ОИ по требованиям безопасности информации.
5. Разработка политики информационной безопасности организации. Уровни детализации политик (общая политика, частные политики, стандарты и процедуры).
6. Организация режима коммерческой тайны на предприятии: юридические основания, определение перечня сведений и введение физической маркировки носителей.
7. Требования к персоналу, имеющему доступ к защищаемой информации. Порядок оформления допуска, обучение сотрудников и действия при увольнении.
8. Инвентаризация информационных активов и классификация информационных ресурсов. Создание реестра активов (*Asset Management*).
9. Планирование непрерывности бизнеса (*BCP*) и восстановления после сбоев (*DRP*): роль КСЗИ в обеспечении доступности критических процессов.
10. Юридическая значимость электронного документооборота. Использование электронной подписи и меток доверенного времени в рамках жизненного цикла документа.
11. Технические каналы утечки информации: классификация (электромагнитные, акустические, виброакустические, материально-вещественные).

12. Побочные электромагнитные излучения и наводки (ПЭМИН): физическая природа возникновения и методы оценки защищенности средств вычислительной техники.
13. Способы защиты информации от утечки за счет ПЭМИН: экранирование помещений, использование генераторов шума («белого шума», «речеподобной помехи»).
14. Акустическая и виброакустическая защита выделенных помещений: контроль звукоизоляции ограждающих конструкций и инженерных систем (вентиляция, двери, окна).
15. Поиск и локализация технических каналов утечки информации: методика проведения специальных исследований (СИ) и инструментального контроля.
16. Защита телефонных линий связи от несанкционированного съема информации и использования диктофонов.
17. Концепция эшелонированной обороны периметра объекта: основное ограждение, запретная зона, система охранного телевидения (СОТ), освещение.
18. Системы контроля и управления доступом (СКУД): идентификаторы, считыватели, контроллеры. Интеграция СКУД с системами видеонаблюдения и охранной сигнализации.
19. Обеспечение пожарной безопасности серверных помещений и центров обработки данных (ЦОД): автоматическое газовое пожаротушение и требования к огнезадерживающим перегородкам.
20. Контроль параметров микроклимата в технологических помещениях (температура, влажность, запыленность). Системы мониторинга среды в серверных стойках.
21. Защита кабельных распределительных сетей: правила прокладки слаботочных линий, установка коммутационных шкафов, предотвращение несанкционированных врезок.
22. Противодействие несанкционированному проносу устройств (телефонов, накопителей) в контролируемую зону: работа инспекционно-досмотровых комплексов и металлодетекторов.
23. Аппаратный модуль доверенной загрузки (АМДЗ): функции, место установки (до ОС), примеры отечественных решений («Аккорд», «Соболь») и их отличие от парольной защиты BIOS/UEFI.
24. Средства антивирусной защиты на уровне шлюза и рабочих станций. Централизованное управление политиками *Endpoint Protection*.
25. Межсетевое экранирование внутри объекта (микросегментация): разделение сети на зоны безопасности (серверная, пользовательская, гостевая) и фильтрация трафика между ними.
26. Системы обнаружения вторжений (IDS/IPS): размещение сенсоров на объекте, анализ сигнатур и аномалий сетевого трафика.
27. Управление съемными носителями информации: технические средства контроля подключения USB-устройств и отчуждаемых дисков.
28. Криптографическая защита каналов связи внутри объекта (виртуальные частные сети — VPN уровня узла или сегмента).
29. Резервное копирование и восстановление данных как элемент комплексного обеспечения: правило «3-2-1», хранение резервных копий вне основного контура объекта.
30. Взаимодействие подсистем комплексной защиты: интеграция событий из СЗИ НСД, СКУД, СОТ и SIEM-системы для выявления комплексных инцидентов ИБ.

1.2 Темы рефератов:

1. **Методология формирования модели угроз безопасности информации** для конкретного объекта информатизации (на примере государственной информационной системы или АСУ ТП критической инфраструктуры).
2. **Категорирование объектов критической информационной инфраструктуры (КИИ) в РФ:** правовые основы, этапы процедуры и требования к защите согласно Ф3-187.

3. **Разработка технического задания на создание комплексной системы защиты информации (КСЗИ):** структура документа, типовые ошибки при определении требований.
4. **Процесс аттестации объекта информатизации:** порядок проведения аттестационных испытаний, программа и методики проверок, оформление «Аттестата соответствия».
5. **Роль организационно-распорядительной документации** в обеспечении режима коммерческой тайны на предприятии (положения, инструкции, журналы учета).
6. **Управление рисками информационной безопасности на уровне объекта:** сравнительный анализ методик ФСТЭК России и международного стандарта ISO/IEC 27005.
7. **План обеспечения непрерывности бизнеса (BCP) и восстановления после катастроф (DRP):** интеграция планов реагирования на ЧС с системой физической охраны объекта.
8. **Особенности комплексного обеспечения защиты информации на объектах малого и среднего предпринимательства (МСП):** бюджетные решения и приоритизация мер.
9. **Технические каналы утечки информации за счет побочных электромагнитных излучений и наводок (ПЭМИН):** физические принципы возникновения и методы инструментального контроля.
10. **Способы пространственного и линейного зашумления:** расчет необходимой мощности генераторов шума для маскировки информативных сигналов.
11. **Акустическая защита выделенных помещений:** современные методы виброакустического зашумления ограждающих конструкций (стен, окон, труб отопления).
12. **Специальные проверки и специальные исследования (СП и СИ) технических средств:** методика поиска внедренных электронных устройств перехвата информации («закладок»).
13. **Защита телефонных переговоров:** технические средства предотвращения утечки через абонентские линии и противодействия высокочастотному навязыванию.
14. **Контроль эффективности принятых мер защиты:** использование комплексов радиомониторинга и нелинейной локации для проверки помещений перед совещаниями.
15. **Интегрированные системы безопасности (ИСБ) объекта:** архитектура объединения охранно-пожарной сигнализации, СКУД и видеонаблюдения в единый контур управления.
16. **Биометрические системы идентификации в составе СКУД:** надежность распознавания лиц и отпечатков пальцев, защита биометрических шаблонов от компрометации.
17. **Обеспечение пожарной безопасности серверных комнат и дата-центров:** сравнение газовых, порошковых и аэрозольных систем пожаротушения применительно к электронному оборудованию.
18. **Инженерная защита периметра охраняемой территории:** классификация заграждений, типы датчиков пересечения границы и тактика расстановки постов охраны.
19. **Защита распределительных пунктов и коммутационных узлов ЛВС:** требования к замкам, датчикам вскрытия шкафов и видеонаблюдению за точками концентрации кабелей.
20. **Противодействие визуальному съему информации:** применение защитных пленок на окна, фильтров конфиденциальности для мониторов и архитектурное планирование рабочих мест.
21. **Аппаратные модули доверенной загрузки (АМДЗ):** эволюция от контроля целостности файлов к контролю запуска гипервизоров и контейнеров.
22. **Микросегментация корпоративной сети:** программно-определяемые межсетевые экраны (NSX, VPC Security Groups) как замена традиционной защиты периметра.

23. **Комплексная защита беспроводных сетей предприятия:** риски использования Wi-Fi, настройка контроллеров WLC, внедрение протокола WPA3 Enterprise.
24. **Централизованный сбор и корреляция событий ИБ:** роль SIEM-систем в объединении логов от СЗИ НСД, антивирусов, СКУД и инженерных систем здания.
25. **Защита цепочки поставок оборудования:** проверка поставляемых серверов и сетевого оборудования на наличие аппаратных закладок и несанкционированных модификаций прошивок.
26. **Организация контролируемой зоны (КЗ):** режим прохода персонала и посетителей, учет материальных пропусков, правила работы мобильных групп быстрого реагирования.
27. **Экологическая безопасность объекта информатизации:** системы мониторинга температуры, влажности и протечек воды в кроссовых и серверных залах.
28. **Использование беспилотных летательных аппаратов (БПЛА) для охраны периметра крупных промышленных объектов:** преимущества перед стационарными камерами и правовые ограничения полетов.
29. **Защита виртуальной инфраструктуры (vSphere, Hyper-V):** изоляция трафика управления, защита vMotion и контроль доступа администраторов облака.
30. **Аудит физической безопасности методом «Red Teaming»:** проведение легализованных попыток проникновения на объект для оценки реальной устойчивости службы охраны.

1.3 Тестовые задания

1. **Что является первичным этапом при создании комплексной системы защиты информации (КСЗИ) на объекте?** а) Закупка сертифицированного оборудования б) Категорирование объекта и классификация обрабатываемой информации в) Установка межсетевых экранов по периметру сети г) Обучение сотрудников правилам пользования паролями *Правильный ответ: б (Обоснование: невозможно выбрать адекватные меры защиты, не зная ценности информации и уровня угроз для конкретного объекта).*
2. **Какой документ регламентирует требования к защите объектов критической информационной инфраструктуры (КИИ) в РФ?** а) Ф3-152 «О персональных данных» б) Ф3-149 «Об информации...» в) Ф3-187 «О безопасности КИИ РФ» г) ГОСТ Р 57580.1-2017 *Правильный ответ: в*
3. **Как называется комплекс мер по защите речевой информации от утечки через строительные конструкции (стены, окна, трубы отопления)?** а) Защита от ПЭМИН б) Виброакустическое зашумление в) Скремблирование телефонных линий г) Экранирование серверной комнаты *Правильный ответ: б*
4. **Побочные электромагнитные излучения и наводки (ПЭМИН) возникают в результате...** а) Ошибок в программном коде операционной системы б) Физических процессов изменения тока и напряжения в цепях технических средств обработки информации в) Несанкционированного доступа в помещение с компьютерами г) Использования нелегального программного обеспечения *Правильный ответ: б*
5. **Для чего предназначен аппаратный модуль доверенной загрузки (АМДЗ), устанавливаемый до старта ОС?** а) Для шифрования жесткого диска в фоновом режиме после входа пользователя б) Для контроля целостности программной среды и аппаратной конфигурации компьютера до передачи управления загрузчику ОС в) Для обнаружения вирусов в оперативной памяти во время работы Windows/Linux г) Для автоматического создания резервных копий BIOS *Правильный ответ: б*
6. **В чем заключается принцип эшелонированной обороны (Defense in Depth) применительно к объекту информатизации?** а) Использование только одного, но максимально дорогого средства защиты б) Создание нескольких последовательных рубежей защиты (периметр — сеть — хост — приложение — данные) в) Отказ от физической охраны в пользу исключительно криптографической защиты г) Размещение

всех серверов в одном защищенном помещении без разделения прав доступа *Правильный ответ: б*

7. Система контроля и управления доступом (СКУД) относится к мерам... а) Только криптографической защиты б) Инженерно-технической и физической защиты в) Организационно-правовой защиты г) Антивирусной защиты рабочих станций *Правильный ответ: б*

8. Аттестат соответствия объекта информатизации подтверждает, что... а) На объекте установлено оборудование только отечественного производства б) Реализованная система защиты соответствует требованиям нормативных документов для данного класса защищенности в) Все сотрудники имеют высшее техническое образование г) Срок действия лицензий на программное обеспечение истекает не ранее чем через 5 лет *Правильный ответ: б*

9. Какое средство наиболее эффективно предотвращает визуальный съём информации с экрана монитора посторонними лицами в офисе? а) Генератор акустического шума б) Программное затемнение экрана через 5 минут неактивности в) Фильтр конфиденциальности (Privacy Filter), ограничивающий угол обзора г) Антивирусная программа *Правильный ответ: в*

10. Микросегментация корпоративной сети направлена на... а) Увеличение общей скорости интернет-канала б) Изоляцию потоков трафика между отдельными рабочими нагрузками внутри дата-центра для предотвращения бокового перемещения злоумышленника (Lateral Movement) в) Объединение всех компьютеров организации в один широковебательный домен г) Упрощение настройки Wi-Fi роутера в переговорной комнате *Правильный ответ: б*

11. Системы охранного телевидения (СОТ) в составе комплексного объекта выполняют функцию... а) Детектирования побочных электромагнитных излучений б) Предотвращения попыток несанкционированного физического проникновения и видеодокументирования событий в) Шифрования сетевого трафика между филиалами компании г) Контроля температуры в серверном шкафу *Правильный ответ: б*

12. Что проверяется в ходе специальных исследований (СИ) технических средств на объекте? а) Наличие лицензионных наклеек на корпусах ПК б) Уровень информативных сигналов в линиях связи и цепях питания, способных создать канал утечки за счет ПЭМИН в) Скорость записи данных на жесткие диски г) Соответствие версии драйверов видеокарты последним обновлениям производителя *Правильный ответ: б*

13. Интеграция СКУД с системой пожарной сигнализации необходима для того, чтобы... а) Автоматически блокировать все двери при обнаружении дыма б) Автоматически разблокировать замки на путях эвакуации при срабатывании тревоги в) Включать сирену каждый раз, когда сотрудник прикладывает карту доступа г) Передавать фотографии входящих лиц на пульт МЧС *Правильный ответ: б*

14. Какая мера защиты относится к организационным мероприятиям? а) Установка решеток на окна первого этажа б) Подписание обязательства о неразглашении конфиденциальной информации (NDA) новым сотрудником в) Монтаж генератора белого шума в кабинете руководителя г) Настройка политики сложности паролей в Active Directory *Правильный ответ: б*

15. Централизованный сбор логов от СЗИ НСД, антивирусов, СКУД и систем видеонаблюдения обычно реализуется с помощью... а) Текстовых редакторов на каждом узле б) SIEM-системы (Security Information and Event Management) в) Электронных таблиц Excel г) Локальных принтеров для печати журналов событий *Правильный ответ: б*

16. Процесс присвоения объекту информатизации определенной категории важности в зависимости от масштаба негативных последствий нарушения безопасности информации называется _____ объекта. (*Правильный ответ: категорированием*)

17. Утечка речевой информации через вибрацию элементов здания (труб отопления, стен), вызванную звуковыми волнами, классифицируется как _____ канал утечки. *(Правильный ответ: виброакустический)*
18. Устройство, предназначенное для контроля целостности программной и аппаратной среды компьютера до момента передачи управления операционной системе, называется аппаратным модулем _____ загрузки. *(Правильный ответ: доверенной / АМДЗ)*
19. Для маскировки информативных побочных электромагнитных излучений от средств вычислительной техники применяются генераторы _____ сигналов (помех). *(Правильный ответ: шума / зашумляющих)*
20. Система, объединяющая средства охранно-пожарной сигнализации, контроля доступа и видеонаблюдения в единый программно-аппаратный комплекс с общим пультом управления, называется _____ системой безопасности. *(Правильный ответ: интегрированной)*
21. Процедура официального подтверждения того, что система защиты объекта соответствует требованиям нормативных документов по безопасности информации, называется _____ объектов информатизации. *(Правильный ответ: аттестацией)*
22. Разделение локальной сети на изолированные сегменты (зоны) для предотвращения бокового перемещения злоумышленника внутри периметра организации называется микросегментацией или внутренним _____. *(Правильный ответ: сегментированием / зонированием)*
23. Физическое лицо, незаконно проникшее на территорию охраняемого объекта или получившее доступ к информационным ресурсам без разрешения, классифицируется как внешний _____. *(Правильный ответ: нарушитель)*
24. Совокупность инженерно-технических средств (ограждения, датчики, посты охраны), предназначенных для предотвращения несанкционированного физического проникновения на территорию, составляет систему _____ защиты. *(Правильный ответ: физической / инженерно-технической)*
25. В Российской Федерации требования к защите автоматизированных систем управления технологическими процессами (АСУ ТП) на критически важных объектах устанавливаются Приказом ФСТЭК России № _____. *(Правильный ответ: 239)*

26. Соответствие между каналом утечки и физическим явлением

Канал утечки	Физическое явление / Среда
1. Акустический	А. Наводки в линиях электропитания и заземления при работе процессора.
2. Электромагнитный (ПЭМИН)	Б. Распространение звуковых волн в воздушной среде помещения.
3. Виброакустический	В. Передача данных по радиоканалу с помощью скрытого передатчика («закладки»).
4. Материально-вещественный	Г. Перенос конфиденциальной информации на физических носителях (бумага, флешки).
5. Электрический	Д. Преобразование звука в вибрацию ограждающих конструкций

Канал утечки

Физическое явление / Среда

(стен, окон).

Правильные ответы: 1–Б, 2–А, 3–Д, 4–Г, 5–В.

27. Соответствие между средством защиты и его назначением

Средство защиты

Назначение

1. СКУД (Контроль доступа)

А. Обнаружение вторжений в сетевой трафик и анализ аномалий L3-L7 уровней.

2. SIEM-система

Б. Управление правами входа сотрудников в здание и конкретные помещения.

3. IPS (Система предотвращения вторжений)

В. Централизованный сбор событий ИБ, корреляция логов и оповещение об инцидентах.

4. Межсетевой экран (Firewall)

Г. Активная блокировка сетевых пакетов, содержащих сигнатуры атак.

5. DLP-система

Д. Фильтрация трафика между сетями и контроль состояния сессий.

Е. Контроль каналов передачи данных для предотвращения утечек документов вовне.

Правильные ответы: 1–Б, 2–В, 3–Г, 4–Д, 5–Е.

28. Соответствие между нормативным документом РФ и областью регулирования

Документ

Область регулирования

1. Ф3-152

А. Безопасность критической информационной инфраструктуры (КИИ).

2. Ф3-187

Б. Защита персональных данных граждан.

3. Приказ ФСТЭК №17

В. Лицензирование деятельности по разработке и производству средств криптографической защиты (СКЗИ).

4. Приказ ФСТЭК №21

Г. Защита государственных информационных систем (ГИС).

5. Постановление Правительства №1719 (или ПП №313)

Д. Защита персональных данных в информационных системах (технические меры).

Правильные ответы: 1–Б, 2–А, 3–Г, 4–Д, 5–В.

29. Соответствие между типом преграды/датчика и методом преодоления

Элемент системы охраны	Метод преодоления / Детектируемое событие
1. Магнитоконтактный датчик (СМК)	А. Пересечение невидимого инфракрасного луча человеком.
2. ИК-барьер (Активный извещатель)	Б. Изменение объема воздуха в помещении (движение).
3. Акустический датчик разбития стекла	В. Размыкание цепи при удалении магнита (открытие двери/окна).
4. Радиоволновой объемный датчик	Г. Улавливание специфического звука удара и звона осыпающихся осколков.
5. Датчик вскрытия корпуса прибора	Д. Разрыв петли охранного шлейфа при открытии крышки оборудования.

Правильные ответы: 1–В, 2–А, 3–Г, 4–Б, 5–Д.

30. Соответствие между этапом жизненного цикла КСЗИ и результатом этапа

Этап создания КСЗИ	Результат (выходной документ)
1. Предпроектное обследование	А. Модель угроз и модель нарушителя.
2. Проектирование (Разработка СТР)	Б. Отчет об обследовании и аналитическое обоснование необходимости защиты.
3. Разработка модели угроз	В. Задание на проектирование (ТЗ) и проектная документация.
4. Внедрение (инсталляция)	Г. Акт о завершении пусконаладочных работ и протоколы испытаний.
5. Аттестация	Д. Заключение по результатам инструментального контроля и «Аттестат соответствия».

Правильные ответы: 1–Б, 2–В, 3–А, 4–Г, 5–Д.

1.4 Практические задания

Задание 1. Опишите иерархию нормативной базы РФ в области защиты информации (ФЗ → Постановления Правительства → Приказы ФСТЭК/ФСБ). Каким документом

устанавливаются требования к мерам защиты персональных данных для ИСПДн? *(Ожидаемый ответ: ФЗ-152 «О персональных данных», приказ ФСТЭК №21).*

Задание 2. Раскройте содержание этапа категорирования объектов критической информационной инфраструктуры (КИИ). Какие критерии используются для определения значимости объекта согласно ФЗ-187? *(Ожидаемый ответ: социальная, политическая, экономическая, экологическая, оборонная значимость).*

Задание 3. Разработайте структуру политики информационной безопасности для условного предприятия. Перечислите не менее пяти обязательных разделов документа верхнего уровня. *(Ожидаемый ответ: цели, область применения, роли и обязанности, классификация активов, ответственность за нарушения).*

Задание 4. В чем заключается разница между сертификацией средства защиты информации (СЗИ) и аттестацией объекта информатизации (ОИ)? *(Ожидаемый ответ: СЗИ проверяется отдельно в лаборатории; ОИ проверяется комплексно на месте эксплуатации вместе с персоналом и средой).*

Задание 5. Составьте план мероприятий по защите коммерческой тайны при увольнении сотрудника, имевшего доступ к конфиденциальным базам данных. *(Ожидаемый ответ: отзыв доступа, аннулирование ключей, инструктаж о неразглашении, контроль выгрузки данных перед уходом).*

Задание 6. Постройте упрощенную модель нарушителя для отделения банка. Определите два типа нарушителей (внешний и внутренний), их возможную квалификацию и потенциальные цели. *(Ожидаемый ответ: хакер-фрилансер — кража денег со счетов; кассир — хищение БД клиентов для продажи).*

Задание 7. Проведите идентификацию уязвимостей для веб-сервера интернет-магазина согласно классификации CWE. Приведите примеры трех различных классов уязвимостей. *(Ожидаемый ответ: SQL-инъекция, XSS, небезопасная конфигурация сервера).*

Задание 8. Объясните принцип эшелонированной обороны (*Defense in Depth*) применительно к серверному сегменту сети. *(Ожидаемый ответ: защита периметра -> сегментация -> защита хоста (HIDS/HIPS) -> шифрование БД -> мониторинг логов).*

Задание 9. Что такое BCP (*Business Continuity Plan*) и DRP (*Disaster Recovery Plan*)? В чем их принципиальное различие в контексте комплексного обеспечения защиты? *(Ожидаемый ответ: BCP — как продолжать бизнес вообще (аренда офиса); DRP — как восстановить ИТ-инфраструктуру).*

Задание 10. Рассчитайте класс защищенности государственной информационной системы (ГИС), если в ней обрабатываются данные, позволяющие идентифицировать субъектов (ПДн 2-й категории), а масштаб системы — федеральный. *(Ожидаемый ответ: К1 или специальная ГИС согласно приказу ФСТЭК №17).*

Задание 11. Дайте определение технического канала утечки информации. Перечислите основные классы каналов (электромагнитные, акустические, материально-вещественные).

Задание 12. Опишите физический механизм возникновения наводок в сетях электропитания при работе монитора. Как называется метод защиты, использующий

зашумление линии питания? *(Ожидаемый ответ: фильтрация цепей питания или пассивное/активное экранирование).*

Задание 13. Сравните методы виброакустического зашумления оконных стекол и вентиляционных коробов. Какие типы преобразователей (излучателей) применяются в каждом случае? *(Ожидаемый ответ: пьезоэлектрические для стекол, электромагнитные/пьезоэлектрические для стен и труб).*

Задание 14. Назовите три основных параметра генератора шума, которые необходимо контролировать при проверке эффективности защиты выделенного помещения. *(Ожидаемый ответ: уровень спектральной плотности мощности, вид помехи (белый шум/речеподобная), отсутствие информативных сигналов в самой помехе).*

Задание 15. В чем суть метода «высокочастотного навязывания» в телефонных линиях? Какое оборудование используется для его обнаружения? *(Ожидаемый ответ: подача зондирующего сигнала высокой частоты в линию для модуляции его информативным сигналом микрофона; обнаруживается анализатором проводных коммуникаций).*

Задание 16. Спроектируйте систему контроля и управления доступом (СКУД) для главного входа офисного здания. Обоснуйте выбор идентификаторов (карты Mifare, биометрия) и контроллеров. *(Ожидаемый ответ: двухфакторная аутентификация, сетевые контроллеры с автономией).*

Задание 17. Охарактеризуйте зоны безопасности дата-центра согласно стандарту TIA-942. Чем отличается зона «Core» от зоны «Operations»? *(Ожидаемый ответ: Core — машинный зал с серверами; Operations — рабочие места администраторов).*

Задание 18. Выберите тип автоматической установки пожаротушения (АУПТ) для серверной комнаты объемом 50 куб.м., заполненной электроникой под напряжением. Обоснуйте отказ от водяного тушения. *(Ожидаемый ответ: газовое пожаротушение (хладон, Noves 1230), так как вода вызывает короткое замыкание и коррозию).*

Задание 19. Опишите алгоритм действий службы охраны при срабатывании объемного ИК-датчика в ночное время в охраняемом помещении. *(Ожидаемый ответ: проверка видеоподтверждения -> вызов группы быстрого реагирования -> блокировка выходов -> осмотр помещения).*

Задание 20. Какова роль контрольно-пропускного пункта (КПП) в системе физической защиты? Перечислите технические средства, обязательные для автомобильного КПП промышленного объекта. *(Ожидаемый ответ: шлагбаум, досмотровое зеркало/рентген, считыватель карт, СКУД, связь с постом охраны).*

Задание 21. Объясните назначение аппаратного модуля доверенной загрузки (АМДЗ). Почему программный пароль BIOS/UEFI не считается достаточным средством защиты АРМ с гостайной? *(Ожидаемый ответ: АМДЗ работает до старта ОС и имеет неизвлекаемый ключ; пароль BIOS легко сбросить физически).*

Задание 22. Сравните возможности межсетевого экрана уровня пакетной фильтрации и прикладного шлюза (Application Layer Gateway/Proxy). Какой из них эффективнее защищает от атак на уровне HTTP? *(Ожидаемый ответ: прикладной шлюз, так как он понимает структуру протокола).*

Задание 23. Настройка микросегментации в виртуальной среде (например, VMware NSX). Как ограничить трафик между двумя веб-серверами, находящимися в одной подсети, чтобы они могли общаться только с базой данных? *(Ожидаемый ответ: создание правил Distributed Firewall на уровне гипервизора для каждого vNIC).*

Задание 24. Роль SIEM-системы в комплексной защите. Опишите процесс корреляции событий: пример того, как изолированные записи в логах СКУД и Windows Event Log складываются в инцидент взлома. *(Ожидаемый ответ: неудачный вход в здание после hours + серия неудачных попыток подбора пароля RDP = попытка несанкционированного доступа).*

Задание 25. Организация безопасного удаленного доступа сотрудников через VPN. Почему использование протокол PPTP в 2024 году недопустимо, и какой современный стандарт следует использовать? *(Ожидаемый ответ: PPTP небезопасен (MS-CHAPv2); L2TP/IPsec или TLS-based SSL VPN).*

Задание 26. Разработка инструкции по антивирусной защите. Какие действия пользователя должны быть строго запрещены политикой компании? *(Ожидаемый ответ: отключение антивируса, подключение личных флешек без проверки, запуск макросов из почты).*

Задание 27. Методика проведения внутреннего аудита информационной безопасности подразделения. Составьте чек-лист из 5 пунктов для проверки хранения бумажных документов. *(Ожидаемый ответ: наличие сейфов, опечатывание тумбочек, журнал выдачи ключей, чистота столов, уничтожение черновиков в шредере).*

Задание 28. Резервное копирование по правилу «3-2-1». Примените это правило к базе данных бухгалтерии организации. *(Ожидаемый ответ: 3 копии данных, на 2 разных носителях (сервер + NAS), 1 копия вне офиса (облако/ленты)).*

Задание 29. Противодействие социальной инженерии. Сотруднику звонит «администратор ИТ-отдела» и просит продиктовать код из СМС для «обновления сертификата». Каковы правильные действия сотрудника? *(Ожидаемый ответ: положить трубку, самостоятельно перезвонить в ИТ-отдел по известному номеру, сообщить о попытке атаки).*

Задание 30. Действия дежурной смены при обнаружении попытки физического проникновения в серверную комнату (сработал геркон двери). Опишите последовательность докладов и фиксации события. *(Ожидаемый ответ: немедленный доклад руководителю ИТ и начальнику СБ -> фиксация времени в журнале -> просмотр видеоархива -> составление акта о ложном срабатывании или инциденте).*

2. КРИТЕРИИ ОЦЕНИВАНИЯ ПРИ ПРОВЕДЕНИИ ТЕКУЩЕГО КОНТРОЛЯ

Вид контроля	Наименование работы	Наименование оценочных средств	Шкала оценивания
Текущий контроль	- Вопросы для обсуждения на занятиях; - Устные опросы по ранее изученному материалу;	Оценка выступлений на практическом (семинарском)	отлично хорошо

	- Письменные работы: рефераты, тестовые задания; - Практические задания; - Рефераты и доклады по темам (вопросам), вынесенным на самостоятельную работу.	занятия, проверка заданий и аудиторных работ, устный опрос, оценивание докладов, рефератов	удовлетворительно неудовлетворительно
--	--	--	--

Критерии оценивания устных ответов обучающихся

Шкала оценивания	Характеристика оценивания
отлично	оценивается ответ, который показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа.
хорошо	оценивается ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.
удовлетворительно	оценивается ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа.
неудовлетворительно	оценивается ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа.

Критерии оценивания работы обучающихся на практических и семинарских занятиях

Шкала оценивания	Показатели	Критерии
Отлично	1. Полнота выполнения практического и тестового задания (полнота ответа); 2. Своевременность	Задание решено самостоятельно. При этом составлен правильный алгоритм решения задания, в логических рассуждениях, в выборе формул и решении нет ошибок, получен верный ответ, задание решено рациональным способом. Дан правильный и исчерпывающий ответ на

Шкала оценивания	Показатели	Критерии
	выполнения задания; 3. Последовательность и рациональность выполнения практического задания	поставленные теоретические и тестовые вопросы, в которых обучающийся показал всестороннее системное знание программного материала, усвоение основной и дополнительной литературы, четкое владение понятийным аппаратом.
Хорошо	(логичность и четкость ответа); 4. Правильность ответов на вопросы; 5. Самостоятельность решения (владение дополнительным материалом); 6. Знание нормативно-законодательной базы и терминологии курса	Задание решено с помощью преподавателя. При этом составлен правильный алгоритм решения задания, в логическом рассуждении и решении нет существенных ошибок; правильно сделан выбор формул для решения; есть объяснение решения, но задание решено нерациональным способом или допущено не более двух несущественных ошибок, получен верный ответ. На поставленные теоретические и тестовые вопросы, при которых обучающийся показал достаточный уровень знаний основного программного материала: освоение информации лекционного курса и учебных пособий, овладение понятийным аппаратом, методикой исследований при попытке анализа различных ситуаций.
Удовлетворительно		Задание решено с подсказками преподавателя. Задание решено в общем виде. Обучающийся показал средний уровень знаний основного программного материала, но не мог убедительно аргументировать свой ответ, ошибся в использовании понятийного аппарата, показал недостаточные знания литературных источников.
Неудовлетворительно		Задание не решено. Обучающийся продемонстрировал значительные пробелы в знаниях основного программного материала, не аргументировал свой ответ, показал неудовлетворительные знания понятийного аппарата и специальной литературы.

Критерии оценивания рефератов

Средство контроля	Критерии оценивания	Шкала оценивания
Реферат	Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы. Реферат раскрывает поднятую проблематику в полном объеме.	отлично
	Основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата;	хорошо

	имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы. В реферате имеются неточности и предметная область выступления раскрыта не в полной мере.	
	Имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод. В реферате не в полной степени раскрыт понятийный аппарат, имеются существенные неточности в процессе формирования выводов.	удовлетворительно
	Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы. Тема реферата не раскрыта или выполнена не по существу ранее поставленного вопроса. Реферат не сдан / доклад не сделан.	неудовлетворительно

Критерии оценивания тестов

Средство контроля	Критерии оценивания – процент положительных ответов	Шкала оценивания
Тестирование	90-100	отлично
	70-89	хорошо
	40-69	удовлетворительно
	< 39	неудовлетворительно

3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Средства оценивания в ходе промежуточной аттестации:

- вопросы для зачета;
- тестовые задания к зачету.

Коды компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения по дисциплине
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты соответствующих проектных решений	ОПК-10.1. Выбирает принципы формирования политики информационной безопасности в информационных системах ОПК-10.2. Подбирает и конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности

3.1. Вопросы к зачету

1. Понятие «объект информатизации» (ОИ). Классификация объектов по уровню конфиденциальности обрабатываемой информации в РФ.
2. Жизненный цикл создания комплексной системы защиты информации (КСЗИ): основные этапы от обследования до аттестации.
3. Модель угроз безопасности информации: структура документа, источники угроз, уязвимости и способы реализации.
4. Роль ФСТЭК России в системе защиты информации. Основные нормативные документы (приказы №17, №21, №239) и области их применения.
5. Категорирование объектов критической информационной инфраструктуры (КИИ) согласно Ф3-187: критерии значимости и последствия присвоения категории.
6. Организационно-правовые режимы защиты информации: государственная тайна, коммерческая тайна, персональные данные. Различия в процедурах допуска.
7. Лицензирование деятельности в области защиты информации. В каких случаях организации необходима лицензия ФСБ или ФСТЭК для работы с СЗИ?
8. Аттестация объектов информатизации: цели, порядок проведения испытаний и юридическая сила «Аттестата соответствия».
9. Принципы построения КСЗИ: эшелонированная оборона (*Defense in Depth*), принцип наименьших привилегий, разделение обязанностей.
10. Планирование непрерывности бизнеса (BCP) и восстановления после сбоев (DRP): место информационной безопасности в обеспечении устойчивости предприятия.
11. Технические каналы утечки информации (ТКУИ): классификация и физическая природа возникновения акустических и виброакустических каналов.
12. Побочные электромагнитные излучения и наводки (ПЭМИН): механизмы возникновения информативных сигналов при работе СВТ.
13. Методы оценки защищенности выделенных помещений от утечки речевой информации (инструментальный контроль).
14. Способы предотвращения утечки по каналу ПЭМИН: экранирование, фильтрация цепей питания и заземления.
15. Активные методы защиты речевой информации: генераторы шума (белый шум, речеподобная помеха) и виброизлучатели.
16. Защита телефонных линий связи: методы обнаружения несанкционированных подключений и подавления диктофонов.
17. Специальные проверки (СП) и специальные исследования (СИ) технических средств: задачи процедур и применяемое оборудование.
18. Контроль эффективности принятых мер защиты информации: периодичность проверок и методика инструментального контроля зон доступности.
19. Концепция инженерной защиты периметра объекта: физические барьеры, освещение, технические средства обнаружения вторжения.
20. Системы контроля и управления доступом (СКУД): идентификаторы, считыватели, контроллеры. Интеграция с системами учета рабочего времени.
21. Биометрические системы идентификации: типы сканеров (отпечаток, лицо, радужка), оценка надежности (*FAR*, *FRR*) и защита биометрических шаблонов.
22. Системы охранного телевидения (СОТ): аналоговые и IP-камеры, видеоаналитика, глубина архива и интеграция с СКУД.
23. Обеспечение пожарной безопасности серверных помещений и ЦОД: требования к автоматическим установкам газового пожаротушения.
24. Контроль микроклимата в технологических помещениях: мониторинг температуры, влажности и протечек воды в кроссовых и серверных залах.
25. Защита распределительных пунктов (кроссов) и коммутационных шкафов: пломбирование, датчики вскрытия, ограничение доступа персонала.

26. Противодействие проносу/провозу запрещенных предметов: работа металлодетекторов, интроскопов и систем нелинейной локации.
27. Аппаратный модуль доверенной загрузки (АМДЗ): архитектура («Соболь», «Аккорд»), функции контроля целостности и отличия от парольной защиты BIOS/UEFI.
28. Средства антивирусной защиты централизованного типа: архитектура сервера управления, обновление баз, политики для рабочих станций и почтовых шлюзов.
29. Межсетевое экранирование внутри корпоративной сети (микросегментация): принципы разделения трафика между сегментами бухгалтерии, разработки и гостевым Wi-Fi.
30. Системы обнаружения и предотвращения вторжений (IDS/IPS): сигнатурный и аномалийный методы анализа, размещение сенсоров в топологии сети.
31. Управление съемными носителями информации: программные средства блокировки USB-портов и контроля записи на отчуждаемые носители.
32. Резервное копирование как элемент КСЗИ: правило «3-2-1», использование ленточных библиотек (LTO) и облачных хранилищ для архивов.
33. Криптографическая защита каналов связи внутри объекта: применение VPN-концентраторов для объединения территориально распределенных сегментов ЛВС.
34. Системы мониторинга событий ИБ (SIEM): сбор логов от разрозненных источников (ОС, СУБД, СКУД) и корреляция событий для выявления инцидентов.
35. Особенности защиты платформ виртуализации (VMware vSphere, Hyper-V): изоляция гипервизора, защита консоли управления (vCenter/vSphere Client).
36. Безопасность контейнеризации (Docker/Kubernetes): различия в механизмах изоляции по сравнению с полными виртуальными машинами.
37. Защита беспроводных сетей стандарта Wi-Fi: эволюция протоколов шифрования (WEP -> WPA2 -> WPA3), типичные атаки на радиодоступ.
38. Интернет вещей (IoT) на объекте: специфические угрозы умных устройств (датчики климата, камеры) и методы их безопасной интеграции в сеть.
39. Использование беспилотных летательных аппаратов (БПЛА) для охраны периметра крупных промышленных объектов: преимущества перед стационарными камерами.
40. Организация службы реагирования на компьютерные инциденты (CSIRT/CERT) на предприятии: регламенты взаимодействия подразделений при обнаружении атаки.
41. Методология тестирования на проникновение (Penetration Testing): планирование работ, правила взаимодействия (Rules of Engagement) и отчетность.
42. Аудит физической безопасности методом «Red Teaming»: проведение легализованных попыток проникновения на объект для проверки бдительности охраны.
43. Расследование инцидентов (Forensics): порядок изъятия и анализа цифровых доказательств (логи, дампы памяти, видеозаписи).
44. Документационное обеспечение эксплуатации КСЗИ: журналы учета носителей, инструкции администраторов, планы восстановления.

3.2. Задания для зачета:

Задание 1. Опишите иерархию нормативной базы РФ в области защиты информации (ФЗ → Постановления Правительства → Приказы ФСТЭК/ФСБ). Каким документом устанавливаются требования к мерам защиты персональных данных для ИСПДн? (Ожидаемый ответ: ФЗ-152 «О персональных данных», приказ ФСТЭК №21).

Задание 2. Раскройте содержание этапа категорирования объектов критической информационной инфраструктуры (КИИ). Какие критерии используются для определения значимости объекта согласно ФЗ-187? (Ожидаемый ответ: социальная, политическая, экономическая, экологическая, оборонная значимость).

Задание 3. Разработайте структуру политики информационной безопасности для условного предприятия. Перечислите не менее пяти обязательных разделов документа верхнего уровня. *(Ожидаемый ответ: цели, область применения, роли и обязанности, классификация активов, ответственность за нарушения).*

Задание 4. В чем заключается разница между сертификацией средства защиты информации (СЗИ) и аттестацией объекта информатизации (ОИ)? *(Ожидаемый ответ: СЗИ проверяется отдельно в лаборатории; ОИ проверяется комплексно на месте эксплуатации вместе с персоналом и средой).*

Задание 5. Составьте план мероприятий по защите коммерческой тайны при увольнении сотрудника, имевшего доступ к конфиденциальным базам данных. *(Ожидаемый отзыв: аннулирование ключей, инструктаж о неразглашении, контроль выгрузки данных перед уходом).*

Задание 6. Постройте упрощенную модель нарушителя для отделения банка. Определите два типа нарушителей (внешний и внутренний), их возможную квалификацию и потенциальные цели. *(Ожидаемый ответ: хакер-фрилансер — кража денег со счетов; кассир — хищение БД клиентов для продажи).*

Задание 7. Проведите идентификацию уязвимостей для веб-сервера интернет-магазина согласно классификации CWE. Приведите примеры трех различных классов уязвимостей. *(Ожидаемый ответ: SQL-инъекция, XSS, небезопасная конфигурация сервера).*

Задание 8. Объясните принцип эшелонированной обороны (*Defense in Depth*) применительно к серверному сегменту сети. *(Ожидаемый ответ: защита периметра -> сегментация -> защита хоста (HIDS/HIPS) -> шифрование БД -> мониторинг логов).*

Задание 9. Что такое BCP (*Business Continuity Plan*) и DRP (*Disaster Recovery Plan*)? В чем их принципиальное различие в контексте комплексного обеспечения защиты? *(Ожидаемый ответ: BCP — как продолжать бизнес вообще (аренда офиса); DRP — как восстановить ИТ-инфраструктуру).*

Задание 10. Рассчитайте класс защищенности государственной информационной системы (ГИС), если в ней обрабатываются данные, позволяющие идентифицировать субъектов (ПДн 2-й категории), а масштаб системы — федеральный. *(Ожидаемый ответ: К1 или специальная ГИС согласно приказу ФСТЭК №17).*

Задание 11. Дайте определение технического канала утечки информации. Перечислите основные классы каналов (электромагнитные, акустические, материально-вещественные).

Задание 12. Опишите физический механизм возникновения наводок в сетях электропитания при работе монитора. Как называется метод защиты, использующий зашумление линии питания? *(Ожидаемый ответ: фильтрация цепей питания или пассивное/активное экранирование).*

Задание 13. Сравните методы виброакустического зашумления оконных стекол и вентиляционных коробов. Какие типы преобразователей (излучателей) применяются в каждом случае? *(Ожидаемый ответ: пьезоэлектрические для стекол, электромагнитные/пьезоэлектрические для стен и труб).*

Задание 14. Назовите три основных параметра генератора шума, которые необходимо контролировать при проверке эффективности защиты выделенного помещения. *(Ожидаемый ответ: уровень спектральной плотности мощности, вид помехи (белый шум/речеподобная), отсутствие информативных сигналов в самой помехе).*

Задание 15. В чем суть метода «высокочастотного навязывания» в телефонных линиях? Какое оборудование используется для его обнаружения? *(Ожидаемый ответ: подача зондирующего сигнала высокой частоты в линию для модуляции его информативным сигналом микрофона; обнаруживается анализатором проводных коммуникаций).*

Задание 16. Спроектируйте систему контроля и управления доступом (СКУД) для главного входа офисного здания. Обоснуйте выбор идентификаторов (карты Mifare, биометрия) и контроллеров. *(Ожидаемый ответ: двухфакторная аутентификация, сетевые контроллеры с автономией).*

Задание 17. Охарактеризуйте зоны безопасности дата-центра согласно стандарту TIA-942. Чем отличается зона «Core» от зоны «Operations»? *(Ожидаемый ответ: Core — машинный зал с серверами; Operations — рабочие места администраторов).*

Задание 18. Выберите тип автоматической установки пожаротушения (АУПТ) для серверной комнаты объемом 50 куб.м., заполненной электроникой под напряжением. Обоснуйте отказ от водяного тушения. *(Ожидаемый ответ: газовое пожаротушение (хладон, Noves 1230), так как вода вызывает короткое замыкание и коррозию).*

Задание 19. Опишите алгоритм действий службы охраны при срабатывании объемного ИК-датчика в ночное время в охраняемом помещении. *(Ожидаемый ответ: проверка видеоподтверждения -> вызов группы быстрого реагирования -> блокировка выходов -> осмотр помещения).*

Задание 20. Какова роль контрольно-пропускного пункта (КПП) в системе физической защиты? Перечислите технические средства, обязательные для автомобильного КПП промышленного объекта. *(Ожидаемый ответ: шлагбаум, досмотровое зеркало/рентген, считыватель карт, СКУД, связь с постом охраны).*

Задание 21. Объясните назначение аппаратного модуля доверенной загрузки (АМДЗ). Почему программный пароль BIOS/UEFI не считается достаточным средством защиты АРМ с гостайной? *(Ожидаемый ответ: АМДЗ работает до старта ОС и имеет неизвлекаемый ключ; пароль BIOS легко сбросить физически).*

Задание 22. Сравните возможности межсетевого экрана уровня пакетной фильтрации и прикладного шлюза (Application Layer Gateway/Proxy). Какой из них эффективнее защищает от атак на уровне HTTP? *(Ожидаемый ответ: прикладной шлюз, так как он понимает структуру протокола).*

Задание 23. Настройка микросегментации в виртуальной среде (например, VMware NSX). Как ограничить трафик между двумя веб-серверами, находящимися в одной подсети, чтобы они могли общаться только с базой данных? *(Ожидаемый ответ: создание правил Distributed Firewall на уровне гипервизора для каждого vNIC).*

Задание 24. Роль SIEM-системы в комплексной защите. Опишите процесс корреляции событий: пример того, как изолированные записи в логах СКУД и Windows Event Log складываются в инцидент взлома. *(Ожидаемый ответ: неудачный вход в здание после ...)*

hours + серия неудачных попыток подбора пароля RDP = попытка несанкционированного доступа).

Задание 25. Организация безопасного удаленного доступа сотрудников через VPN. Почему использование протокол PPTP в 2024 году недопустимо, и какой современный стандарт следует использовать? *(Ожидаемый ответ: PPTP небезопасен (MS-CHAPv2); L2TP/IPsec или TLS-based SSL VPN).*

Задание 26. Разработка инструкции по антивирусной защите. Какие действия пользователя должны быть строго запрещены политикой компании? *(Ожидаемый ответ: отключение антивируса, подключение личных флешек без проверки, запуск макросов из почты).*

Задание 27. Методика проведения внутреннего аудита информационной безопасности подразделения. Составьте чек-лист из 5 пунктов для проверки хранения бумажных документов. *(Ожидаемый ответ: наличие сейфов, опечатывание тумбочек, журнал выдачи ключей, чистота столов, уничтожение черновиков в шредере).*

Задание 28. Резервное копирование по правилу «3-2-1». Примените это правило к базе данных бухгалтерии организации. *(Ожидаемый ответ: 3 копии данных, на 2 разных носителях (сервер + NAS), 1 копия вне офиса (облако/ленты)).*

Задание 29. Противодействие социальной инженерии. Сотруднику звонит «администратор ИТ-отдела» и просит продиктовать код из СМС для «обновления сертификата». Каковы правильные действия сотрудника? *(Ожидаемый ответ: положить трубку, самостоятельно перезвонить в ИТ-отдел по известному номеру, сообщить о попытке атаки).*

Задание 30. Действия дежурной смены при обнаружении попытки физического проникновения в серверную комнату (сработал геркон двери). Опишите последовательность докладов и фиксации события. *(Ожидаемый ответ: немедленный доклад руководителю ИТ и начальнику СБ -> фиксация времени в журнале -> просмотр видеоархива -> составление акта о ложном срабатывании или инциденте).*

4. ОСНОВНЫЕ КРИТЕРИИ ОЦЕНИВАНИЯ ПРИ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Шкала оценивания уровня сформированности универсальной компетенций (зачет с оценкой)

Формируемые уровни освоения компетенций	Критерии оценивания	Шкала оценивания
---	---------------------	------------------

Высокий уровень	Изложено правильное понимание вопроса, четко и самостоятельно дан исчерпывающий ответ, содержание раскрыто полно, профессионально, грамотно. Обучающимся усвоена взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии. Отражает успешное и систематическое применение навыков и умений по данной дисциплине в соответствии с ФГОС.	отлично
Базовый уровень	Изложено правильное понимание вопроса, дано достаточно подробное описание предмета ответа, приведены и раскрыты в тезисной форме основные понятия, относящиеся к предмету ответа. Ответ отражает полное знание учебно-программного материала, систематический характер знаний по дисциплине, а также наличие базового уровня овладения практическими умениями и навыками по данной дисциплине в соответствии с ФГОС	хорошо
Пороговый уровень	Ответ отражает теоретические знания основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии. Данная оценка может быть выставлена обучающемуся, допустившему неточности в ответе, но обладающими необходимыми знаниями для их устранения под руководством преподавателя, отмечен начальный уровень овладения практическими умениями и навыками по данной дисциплине в соответствии с ФГОС	удовлетворительно
Неудовлетворительный уровень	При ответе обучающегося обнаружено отсутствие знаний, умений и навыков и/или фрагментарные знания основного учебно-программного материала.	неудовлетворительно

Текущий контроль и промежуточная аттестация осуществляются в соответствии с «Положением о текущей и промежуточной аттестации обучающихся в Автономной некоммерческой организации «Образовательная организация высшего образования» «Университет экономики и управления».

Вид промежуточной аттестации – зачет с оценкой.

Форма проведения промежуточной аттестации – письменный зачет.