

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Узунов Федор Владимирович

Должность: Ректор

Дата подписания: 50.09.2026 08:54:44

Уникальный программный ключ:

fd935d10451b860e912264c0378f8448452b603f94388008e29877a6bcbf5

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

«УНИВЕРСИТЕТ ЭКОНОМИКИ И УПРАВЛЕНИЯ»

Факультет экономики, управления и юриспруденции

Кафедра «Управление и бизнес-информатика»



УТВЕРЖДАЮ

Проректор по учебно-методической работе

_____/ Г.П. Узунова

«05» февраля 2026 г

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Направление подготовки

10.03.01 «Информационная безопасность»

Профиль

Безопасность компьютерных систем

Квалификация выпускника

Бакалавр

Для всех

форм обучения

Симферополь, 2026

1. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

Средства оценивания в ходе текущего контроля:

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

Код компетенции	Результаты освоения ОПОП (содержание компетенций)	Планируемые результаты освоения дисциплины
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	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. Дайте определение понятию «информационная безопасность». Чем оно отличается от защиты информации?
2. Перечислите и раскройте содержание трех основных свойств информации (триада КИД: конфиденциальность, целостность, доступность).
3. Что такое угроза, уязвимость и риск в контексте информационной безопасности? Как они взаимосвязаны?
4. Назовите основные виды угроз информационной безопасности (естественные, искусственные, случайные, преднамеренные) с примерами каждой категории.
5. Раскройте понятие активов информационной безопасности. Приведите примеры материальных и нематериальных активов организации.
6. Какие существуют подходы к оценке стоимости информационных активов компании?
7. Опишите жизненный цикл информации в организации и связанные с ним риски на каждом этапе.
8. В чем заключается принцип экономической целесообразности внедрения мер защиты информации?
9. Какова структура российского законодательства в области защиты информации? Назовите ключевые федеральные законы (например, ФЗ-149, ФЗ-152, ФЗ-187).
10. Роль регуляторов (ФСТЭК России, ФСБ России, Банк России) в системе обеспечения информационной безопасности в РФ.

11. Основные положения международного стандарта ISO/IEC 27001. Структура высокоуровневой структуры (HLS) стандартов систем менеджмента.
12. В чем разница между сертификацией системы менеджмента ИБ и аттестацией объекта информатизации?
13. Требования трудового и гражданского кодексов РФ в части ответственности сотрудников за нарушение режима коммерческой тайны.
14. Особенности правового регулирования защиты критической информационной инфраструктуры (КИИ) в Российской Федерации.
15. Понятие импортозамещения в сфере средств защиты информации: нормативная база и требования к субъектам КИИ.
16. Что такое политика информационной безопасности верхнего уровня? Каковы ее обязательные разделы?
17. Распределение ролей и ответственности в системе управления ИБ (владелец актива, офицер безопасности, пользователь, администратор).
18. Зачем нужен реестр рисков и план обработки рисков? Методы реагирования на риски (снижение, принятие, уклонение, передача).
19. Управление доступом как организационная мера: принципы наименьших привилегий и разделения обязанностей.
20. Порядок проведения служебных расследований инцидентов информационной безопасности внутри организации.
21. Кадровая безопасность: процедуры проверки персонала при найме и действия при увольнении сотрудника (принцип увольнения — *offboarding*).
22. Организация физической безопасности объектов ИТ-инфраструктуры (доступ в серверные, охрана периметра).
23. Процесс идентификации и классификации информационных активов. Для чего нужна маркировка носителей информации?
24. Модели управления непрерывностью бизнеса (*BCP* — Business Continuity Planning и *DRP* — Disaster Recovery Planning). Различия и цели.
25. Жизненный цикл инцидента информационной безопасности (классификация, регистрация, реагирование, анализ причин, извлечение уроков).
26. Внутренний и внешний аудит информационной безопасности: цели, периодичность и критерии оценки эффективности.
27. Пентесты (тесты на проникновение) и сканирование уязвимостей: отличия методик и их место в процессе управления ИБ.

28. Ключевые показатели эффективности (KPI) и результативности (KRI) службы информационной безопасности.

29. Экономическая эффективность инвестиций в информационную безопасность (ROSI — Return on Security Investment). Формула расчета и ее компоненты.

30. Сформулируйте техническое задание на внедрение базового набора средств защиты для малого предприятия (перечислите классы необходимых средств: антивирус, межсетевой экран, система резервного копирования, средство двухфакторной аутентификации) и обоснуйте выбор каждого класса.

1.2 Темы рефератов

1. **Сравнительный анализ международных и российских стандартов управления информационной безопасностью** (ISO/IEC 27001, NIST SP 800-53, ГОСТ Р ИСО/МЭК 27001). Проблемы гармонизации требований.
2. **Экономическая эффективность систем защиты информации.** Методы оценки возврата инвестиций в информационную безопасность (ROSI) и совокупной стоимости владения (TCO).
3. **Управление рисками информационной безопасности:** качественная и количественная оценка. Стратегии обработки рисков: снижение, принятие, уклонение и передача на аутсорсинг.
4. **Роль человеческого фактора в нарушении режима информационной безопасности.** Психология социальной инженерии и методы повышения осведомленности персонала (*Security Awareness*).
5. **Особенности обеспечения информационной безопасности в условиях массового перехода на удаленную работу.** Защита домашних офисов, управление доступом к корпоративным ресурсам через публичные сети.
6. **Правовые основы защиты персональных данных в Российской Федерации.** Практика применения ФЗ-152 «О персональных данных» и ответственность за нарушения.
7. **Обеспечение информационной безопасности критической информационной инфраструктуры (КИИ)** в соответствии с требованиями ФЗ-187. Категорирование объектов КИИ.
8. **Разработка и внедрение политики информационной безопасности предприятия.** Структура документа, уровни детализации (верхнеуровневая политика, стандарты, процедуры) и жизненный цикл политик.
9. **Организационные и технические аспекты расследования инцидентов информационной безопасности.** Принципы форензики (компьютерной криминалистики), сбор цифровых доказательств и сохранение цепочки хранения.
10. **Проблема внутреннего нарушителя (*Insider Threat*):** классификация угроз, модели поведения и превентивные меры контроля (DLP-системы, поведенческий анализ — UBA/UEBA).
11. **Процессный подход к управлению ИБ:** интеграция процессов менеджмента информационной безопасности со смежными процессами ИТ-управления (ITIL, COBIT).
12. **Управление непрерывностью бизнеса (BCP) и аварийное восстановление (DRP)** как элементы системы управления информационной безопасностью. Планирование послеаварийного восстановления ИТ-инфраструктуры.

13. **Аутсорсинг информационной безопасности:** критерии выбора провайдера *MSSP* (Managed Security Service Provider), модель разделения ответственности и риски передачи функций на внешнее управление.
14. **Эволюция кибератак и современные модели нарушителей.** От классического хакерства до политически мотивированных группировок (*APT*) и хактивизма: тактики, техники и процедуры (*TTP*).
15. **Импортозамещение средств защиты информации в РФ:** нормативно-правовое регулирование, проблемы совместимости отечественного ПО и аппаратных платформ, переход на доверенные программно-аппаратные комплексы.

Методические рекомендации по написанию реферата:

- **Структура работы:** каждый реферат должен включать введение (актуальность, цель, задачи), основную часть из 2–3 глав, заключение (выводы) и список источников.
- **Актуализация темы:** при выборе темы рекомендуется привязывать ее к конкретной отрасли (например, банковский сектор для темы №7 или ритейл для темы №6), чтобы добавить практической ценности.
- **Источники:** обязательным требованием является использование не только учебников, но и актуальных нормативных актов (законов, приказов ФСТЭК/ФСБ), а также аналитических отчетов профильных компаний.

1.3 Тестовые задания

1. Что из перечисленного входит в классическую триаду информационной безопасности (CIA)? а) Скорость, Доступность, Цена. б) Конфиденциальность, Целостность, Доступность. в) Контроль, Идентификация, Авторизация. г) Серверы, Сети, Данные. (Правильный ответ: б)
2. Как называется преднамеренное действие или бездействие, которое может привести к нарушению режима ИБ? а) Уязвимость. б) Актив. в) Угроза. г) Риск. (Правильный ответ: в)
3. Какой основной закон Российской Федерации регулирует отношения в сфере защиты персональных данных? а) ФЗ-149 «Об информации...». б) ФЗ-63 «Об электронной подписи». в) Уголовный кодекс РФ. г) ФЗ-152 «О персональных данных». (Правильный ответ: г)
4. С точки зрения управления рисками, что такое «уязвимость»? а) Вероятность реализации угрозы. б) Потенциальная причина нежелательного инцидента. в) Недостаток актива или группы активов, который может быть использован угрозой. г) Финансовый ущерб от взлома системы. (Правильный ответ: в)
5. Кто несет основную ответственность за информационную безопасность в конкретном бизнес-подразделении компании? а) Системный администратор. б) Владелец информационного актива. в) Рядовой пользователь компьютера. г) Внешний аудитор. (Правильный ответ: б)
6. Как расшифровывается аббревиатура DLP в контексте средств защиты информации? а) Data Loss Prevention (Предотвращение утечек данных). б) Digital Local Protection (Цифровая локальная защита). в) Direct Link Protocol (Протокол прямой связи). г) Data Level Priority (Приоритет уровня данных). (Правильный ответ: а)
7. Принцип предоставления пользователю минимально необходимых прав для выполнения его работы называется: а) Принцип наименьших привилегий. б) Принцип единого входа (SSO). в) Принцип избыточности. г) Принцип разделения обязанностей. (Правильный ответ: а)

8. Какой международный стандарт является основным для построения систем менеджмента информационной безопасности (СМИБ)? а) ISO 9001. б) ISO/IEC 27001. в) IEEE 802.11. г) ГОСТ 34. (Правильный ответ: б)
9. Что понимается под инцидентом информационной безопасности? а) Плановое обновление антивирусных баз. б) Любое нежелательное или непредвиденное событие, имеющее отношение к безопасности информации. в) Ежегодный аудит ИТ-инфраструктуры. г) Установка нового межсетевого экрана. (Правильный ответ: б)
10. Метод атаки, основанный на использовании человеческой психологии и побуждении человека совершить ошибку, называется: а) Брутфорс (перебор паролей). б) Социальная инженерия. в) DDoS-атака. г) Фишинговое сканирование портов. (Правильный ответ: б)
11. Установите правильную последовательность этапов обработки инцидента информационной безопасности: А) Ликвидация последствий (очистка систем, восстановление данных). Б) Обнаружение и регистрация подозрительной активности. В) Постинцидентный анализ и извлечение уроков. Г) Локализация (сдерживание) угрозы для предотвращения ее распространения. Ответ: Б, Г, А, В.
12. Установите правильную иерархию документов системы управления информационной безопасностью от общего к частному: А) Рабочие инструкции (пошаговые алгоритмы действий). Б) Политика ИБ верхнего уровня (декларация намерений руководства). В) Стандарты и регламенты (конкретные требования к процессам). Ответ: Б, В, А.
13. Установите правильный порядок жизненного цикла риска информационной безопасности: А) Выбор и реализация метода обработки риска (снижение, передача, принятие). Б) Идентификация активов, угроз и уязвимостей. В) Количественная или качественная оценка вероятности и ущерба. Г) Постоянный мониторинг эффективности принятых мер контроля. Ответ: Б, В, А, Г.
14. Установите правильную последовательность процесса аутентификации пользователя в корпоративной системе: А) Предоставление доступа к ресурсам согласно полномочиям. Б) Предъявление идентификатора (логина) пользователем. В) Проверка подлинности предъявленного фактора (пароля, токена, биометрии). Г) Регистрация учетной записи администратором и назначение прав. Ответ: Г, Б, В, А.
15. Установите правильную последовательность уровней защиты в классической модели эшелонированной обороны (*Defense in Depth*): А) Физический уровень (замки, охрана, видеонаблюдение). Б) Сетевой уровень (межсетевые экраны, сегментация сети). В) Уровень приложений и данных (шифрование, контроль доступа на уровне СУБД). Г) Уровень политик и процедур (организационные меры). Ответ: Г, А, Б, В.
16. Установите правильную последовательность разработки политики информационной безопасности: А) Утверждение документа руководством организации. Б) Анализ бизнес-требований и применимого законодательства. В) Публикация политики и ознакомление с ней персонала. Г) Написание чернового варианта текста (проекта) политики. Ответ: Б, Г, А, В.
17. Установите правильную последовательность фаз тестирования на проникновение (*пентеста*): А) Сбор информации и разведка (поиск целей, сканирование портов). Б) Получение финального отчета и рекомендаций по устранению уязвимостей. В) Попытки эксплуатации выявленных уязвимостей (получение доступа). Г) Планирование работ и определение границ тестирования. Ответ: Г, А, В, Б.
18. Установите правильную последовательность внедрения патча (исправления безопасности) на критически важный сервер: А) Тестирование исправления на изолированной тестовой среде. Б) Развертывание патча на продуктивном сервере. В) Мониторинг работоспособности сервера после обновления. Г) Создание полной резервной копии системы перед вмешательством. Ответ: Г, А, Б, В.

19. Установите правильную последовательность классификации информационного актива: А) Присвоение итогового грифа конфиденциальности (например, «Коммерческая тайна»). Б) Определение владельца актива. В) Оценка ценности актива и потенциального ущерба при его потере. Г) Инвентаризация (выявление) самого актива. Ответ: Г, Б, В, А.
20. Установите правильную последовательность применения защитных мер в процессе обеспечения целостности электронного документа: А) Вычисление криптографического хэша (контрольной суммы) документа. Б) Подписание полученного хэш-значения электронной подписью автора. В) Передача документа и подписи получателю. Г) Повторное вычисление хэша полученного документа и проверка подлинности подписи. Ответ: А, Б, В, Г.
21. Документ, устанавливающий обязательные для всех сотрудников правила работы с информационными активами и ответственность за их нарушение, называется _____. (Правильный ответ: политика информационной безопасности)
22. Процесс оценки вероятности реализации угрозы и размера потенциального ущерба для информационного актива называется оценкой _____. (Правильный ответ: рисков)
23. Свойство информации, гарантирующее ее точность и полноту, а также защиту от несанкционированного изменения, называется _____. (Правильный ответ: целостностью)
24. Организационная мера защиты, при которой критически важная операция разделяется между двумя или более сотрудниками для предотвращения мошенничества, называется принципом _____ обязанностей. (Правильного ответа: разделения / SoD — Segregation of Duties)
25. Процесс перевода информационных активов из бумажных или устаревших цифровых форматов в единую структурированную базу данных для обеспечения их сохранности и быстрого поиска называется _____ данных. (Правильный ответ: оцифровкой / миграцией)
26. Программное обеспечение, предназначенное для предотвращения случайной или преднамеренной передачи конфиденциальной информации за пределы корпоративной сети, относится к классу систем _____. (Правильный ответ: предотвращения утечек данных / DLP)
27. Процесс восстановления работоспособности ИТ-систем и доступа к данным после серьезного сбоя (например, пожара в дата-центре) описывается планом аварийного _____. (DRP). (Правильный ответ: восстановления)
28. Свойство системы, подтверждающее, что субъект или ресурс является именно тем, за кого себя выдает, называется _____. (Правильный ответ: подлинностью / аутентичностью)
29. Документированная процедура, описывающая пошаговые действия персонала при обнаружении компьютерного вируса или хакерской атаки, называется планом реагирования на _____. (Правильный ответ: инциденты)
30. Показатель того, как часто система должна быть доступна для выполнения своих функций (например, 99,9% времени в год), закрепляется в соглашении об уровне обслуживания и называется коэффициентом _____. (Правильный ответ: доступности)

1.4 Задания

1. **Ситуация №1.** Сотрудник отдела продаж, увольняясь из компании, скопировал на личную флеш-карту базу клиентов для использования на новом месте работы.

Служба безопасности обнаружила это за день до его последнего рабочего дня. **Вопрос:** Какие организационные и технические меры были нарушены? Кто несет ответственность за утечку — сотрудник или компания? *(Правильный ответ: Нарушен принцип обеспечения конфиденциальности и процедура оффбординга (увольнения). Ответственность несут обе стороны: сотрудник — дисциплинарную и гражданскую, компания — недостаточный контроль доступа и отсутствие DLP-системы.)*

2. **Ситуация №2.** Системный администратор раз в неделю делает резервное копирование серверов, но ни разу не проверял возможность восстановления данных из этих копий. В результате сбоя оборудования выяснилось, что архивы повреждены. **Вопрос:** Какой критический этап управления непрерывностью бизнеса был пропущен? *(Правильный ответ: Тестирование процедур восстановления (DR-тест). Резервная копия без подтвержденной возможности восстановления считается отсутствующей.)*
3. **Ситуация №3.** Бухгалтер получил по электронной почте письмо от «генерального директора» с требованием срочно оплатить счет нового контрагента, перейдя по ссылке и введя корпоративные логин и пароль. Письмо выглядело подлинным. **Вопрос:** Как называется данный тип атаки и какой базовый защитный механизм должен был предотвратить компрометацию учетных данных? *(Правильный ответ: Фишинг (или ВЕС-атака). Двухфакторная аутентификация (MFA) предотвратила бы доступ злоумышленника при краже пароля.)*
4. **Ситуация №4.** В компании внедрена политика чистых столов и экранов. Однако менеджер привык оставлять разблокированный ноутбук на рабочем месте во время обеденного перерыва. **Вопрос:** К какому типу угроз относится данная ситуация и как ее классифицировать согласно модели STRIDE? *(Правильный ответ: Угроза несанкционированного доступа (спуфинг/подмена сессии). Это нарушение физической и операционной безопасности со стороны инсайдера.)*
5. **Ситуация №5.** При проведении тендера на закупку антивирусного ПО отдел ИБ выбрал самое дешевое решение, которое защищает только рабочие станции, игнорируя защиту почтовых шлюзов и файловых серверов. **Вопрос:** Какой экономический показатель стал приоритетом вместо совокупной стоимости владения (ТСО) и какие риски это создает? *(Правильный ответ: Приоритет отдан капитальным затратам (CAPEX), а не операционным (OPEX) и риск-ориентированному подходу. Создается риск заражения всей сети через неприкрытые каналы.)*
6. **Ситуация №6.** Инженер технической поддержки выдал новому сотруднику права администратора на своем компьютере «для удобства установки рабочих программ», хотя для должности сотрудника достаточно прав обычного пользователя. **Вопрос:** Какой фундаментальный принцип управления доступом нарушен? *(Правильный ответ: Принцип наименьших привилегий / Least Privilege.)*
7. **Ситуация №7.** Компания перенесла всю инфраструктуру в публичное облако, полагая, что провайдер теперь полностью отвечает за безопасность их данных. **Вопрос:** Как называется модель распределения ответственности, которую проигнорировала компания, и за что именно она продолжает отвечать сама? *(Правильный ответ: Модель общей ответственности (Shared Responsibility Model). Компания отвечает за свои данные, настройки доступа, шифрование и управление пользователями.)*
8. **Ситуация №8.** На годовом собрании акционеров директор по ИБ представил отчет, где единственным показателем эффективности было количество заблокированных вирусов на периметре. **Вопрос:** Почему этот набор метрик является неполным для оценки зрелости системы управления ИБ? Назовите два недостающих типа показателей. *(Правильный ответ: Отсутствуют показатели времени обнару-*

жения/сдерживания инцидентов (MTTD, MTTR) и показатели остаточного риска / соответствия бюджету.)

9. **Ситуация №9.** Разработчики выкладывают код приложения в открытый репозиторий вместе с файлами конфигурации, содержащими ключи API к платежной системе. **Вопрос:** На каком этапе жизненного цикла безопасной разработки (SDLC) произошел сбой и какая автоматизированная проверка должна была это остановить? *(Правильный ответ: Этап контроля кода (Code Review) или статического анализа (SAST).)*
10. **Ситуация №10.** Сторонний подрядчик, проводивший ремонт в серверной, подключил свой рабочий ноутбук к сетевому порту на стене, обойдя систему контроля доступа в само помещение. **Вопрос:** Какой вид контроля (физический или технический) оказался неэффективным и почему? *(Правильный ответ: Технический контроль (управление сетевым доступом / NAC). Физическая безопасность помещения не спасает от подключения к активным сетевым розеткам вне защищенных стоек.)*
11. **Ситуация №11.** Сотрудник открыл вложение в письме, после чего все файлы на его диске и в общих папках оказались зашифрованы. Злоумышленники требуют выкуп в криптовалюте. **Вопрос:** Какова первая техническая мера изоляции инцидента, которую должна предпринять служба ИБ? *(Правильный ответ: Немедленное отключение зараженной машины от локальной сети и Wi-Fi для предотвращения распространения вируса-шифровальщика.)*
12. **Ситуация №12.** Руководство требует установить срок хранения логов (журналов событий) всего 7 дней, чтобы сэкономить место на серверах, хотя отраслевой стандарт требует 1 год. **Вопрос:** Какую проблему создаст такое решение при расследовании инцидента, произошедшего месяц назад? *(Правильный ответ: Невозможность проведения ретроспективного анализа и установления причинно-следственной связи из-за отсутствия доказательной базы.)*
13. **Ситуация №13.** Офицер безопасности обнаружил, что один из топ-менеджеров использует личный облачный диск для пересылки чертежей новой продукции компании. **Вопрос:** Как называется эта угроза и какой класс технических средств предназначен для борьбы с ней? *(Правильный ответ: Теневые ИТ (Shadow IT) и непреднамеренная утечка данных. Для борьбы используются системы класса CASB (Cloud Access Security Broker) и DLP.)*
14. **Ситуация №14.** После успешного прохождения внешнего аудита на соответствие ISO 27001 руководство решило расформировать комитет по информационной безопасности для экономии бюджета. **Вопрос:** Какое долгосрочное последствие это повлечет для сертификата соответствия? *(Правильный ответ: Потерю сертификации при следующем надзорном аудите из-за нарушения требования об анализе со стороны руководства и постоянном улучшении СМИБ.)*
15. **Ситуация №15.** При расчете окупаемости внедрения системы защиты (ROSI) аналитик указал снижение вероятности взлома на 100%. **Вопрос:** В чем методологическая ошибка такого расчета? *(Правильный ответ: Ни одна система защиты не снижает риск до нуля; всегда остается остаточный риск. Вероятность нельзя занулять, можно лишь снизить ущерб или вероятность реализации.)*
16. **Ситуация №16.** Сотрудник колл-центра записал свой пароль на стикере и приклеил его под клавиатуру. Уборщица в вечернее время использовала этот компьютер для выхода в интернет. **Вопрос:** Помимо нарушения политики паролей, какой еще важный аспект безопасности был скомпрометирован? *(Правильный ответ: Аудит и подотчетность. Все действия, совершенные уборщицей, в системных журналах будут зафиксированы как действия легитимного сотрудника.)*
17. **Ситуация №17.** Компания закупила дорогостоящее средство защиты, но сэкономила на обучении штатных администраторов работе с ним. Устройство работает с

настройками по умолчанию. **Вопрос:** Как называется риск эксплуатации средств защиты с небезопасными настройками? (*Правильный ответ: Риск неправильной конфигурации / Misconfiguration risk.*)

18. **Ситуация №18.** В договоре с облачным провайдером отсутствует пункт о финансовой ответственности (штрафах) за простой сервиса более 4 часов. **Вопрос:** Как называется юридически значимый документ, регулирующий уровень доступности услуг, который был составлен некорректно? (*Правильный ответ: Соглашение об уровне обслуживания — SLA / Service Level Agreement.*)
19. **Ситуация №19.** Организация обрабатывает биометрические данные сотрудников (отпечатки пальцев для входа в офис), но не включила этот процесс в уведомление для Роскомнадзора. **Вопрос:** Какое юридическое последствие грозит организации помимо штрафа? (*Правильный ответ: Предписание об обработке персональных данных без надлежащего уведомления, требование прекратить обработку и уничтожить незаконно собранные биометрические данные.*)
20. **Ситуация №20.** При проектировании отказоустойчивого кластера инженеры разместили оба сервера в одной серверной стойке рядом друг с другом. **Вопрос:** Какой ключевой принцип проектирования высокой доступности (*High Availability*) нарушен и какой риск это создает? (*Правильный ответ: Нарушено физическое разделение / Anti-affinity. Возникает единая точка отказа: пожар, протечка или сбой питания в одной стойке выведут из строя оба узла одновременно.*)

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; Письменные работы: рефераты, тестовые задания; Практические задания; Рефераты и доклады по темам (вопросам), вынесенным на самостоятельную работу.	Оценка выступлений на практическом (семинарском) занятии, проверка заданий, устный опрос, оценивание докладов, рефератов	отлично хорошо 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 семинарских занятиях

Шкала оценивания	Показатели	Критерии
Отлично	1. Полнота выполнения практического и тестового задания (полнота ответа); 2. Своевременность выполнения задания; 3. Последовательность и рациональность выполнения практического задания (логичность и четкость ответа);	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 поставленные теоретические и тестовые вопросы, в которых обучающийся показал всестороннее системное знание программного материала, усвоение основной и дополнительной литературы, четкое владение понятийным аппаратом.
Хорошо	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.	отлично

	Реферат раскрывает поднятую проблематику в полном объеме. 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; 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.	хорошо
	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 экзамена;
- практические задания экзамена.

Код компетенции	Результаты освоения ОПОП (содержание компетенций)	Планируемые результаты освоения дисциплины
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	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 экзамену

1. Дайте определение информационной безопасности (ИБ). Чем управление ИБ отличается от технического обеспечения защиты информации?
2. Раскройте содержание классической триады КИД (конфиденциальность, целостность, доступность) на примере банковской системы.
3. Дополнительные свойства информации: неотказуемость, подотчетность, достоверность и аутентичность.
4. Понятие информационного актива. Методы классификации и оценки стоимости активов организации.
5. Определения угрозы, уязвимости и риска. Формула расчета уровня риска (*Likelihood* $\times$ *Impact*).
6. Классификация угроз ИБ по источникам возникновения (естественные, техногенные, антропогенные) и мотивам (шпионаж, хактивизм, киберпреступность).
7. Принцип эшелонированной обороны (*Defense in Depth*): уровни реализации в корпоративной сети.
8. Принципы наименьших привилегий (*Least Privilege*) и разделения обязанностей (*Separation of Duties*).
9. Стратегии обработки рисков: снижение, принятие, уклонение, передача. Примеры ситуаций для каждой стратегии.
10. Концепция остаточного и приемлемого риска. Кто в организации утверждает уровень приемлемого риска?
11. Понятие «владелец информационного актива» и его роль в системе управления доступом.
12. Экономическая целесообразность мер защиты. Точка оптимального вложения средств в информационную безопасность.
13. Структура российского законодательства в сфере ИБ. Роль Конституции РФ и федеральных законов.
14. ФЗ-149 «Об информации, информационных технологиях и о защите информации»: ключевые определения и обязанности обладателя информации.
15. ФЗ-152 «О персональных данных». Уровни защищенности персональных данных при их обработке в ИСПДн.
16. Требования к согласию субъекта персональных данных на обработку его данных.
17. Обязанности оператора при обращении или запросе субъекта ПДн.
18. Трансграничная передача персональных данных: условия и ограничения согласно российскому законодательству.
19. ФЗ-187 «О безопасности критической информационной инфраструктуры (КИИ)». Субъекты КИИ и категорирование объектов.
20. Регуляторы в области ИБ в РФ: полномочия ФСТЭК России, ФСБ России и Банка России.
21. Лицензирование деятельности по технической защите конфиденциальной информации (ТЗКИ) и разработке СЗИ.
22. Правовой режим коммерческой тайны. Порядок введения режима КТ и дисциплинарная ответственность сотрудников.
23. Уголовная ответственность за преступления в сфере компьютерной информации (глава 28 УК РФ: ст. 272, 273, 274).
24. Государственная система защиты информации в РФ. Сертификация и аттестация объектов информатизации.

25. Стандарт ISO/IEC 27001: область применения, структура требований и высокоуровневая структура (*HLS*).
26. Цикл Деминга (*PDCA*) как основа жизненного цикла системы менеджмента информационной безопасности (СМИБ).
27. Связка стандартов ISO 27001 (требования), ISO 27002 (каталог мер) и ISO 27005 (управление рисками).
28. Методология оценки рисков OCTAVE. Отличия от классического подхода ISO 27005.
29. Фреймворк NIST Cybersecurity Framework (CSF): пять основных функций (*Identify, Protect, Detect, Respond, Recover*).
30. Стандарты серии PCI DSS: назначение, сфера действия и основные группы требований для платежных систем.
31. Политика информационной безопасности верхнего уровня: обязательные разделы и порядок утверждения.
32. Виды организационно-распорядительной документации: политики, стандарты, процедуры, инструкции.
33. Процессный подход к управлению ИБ. Интеграция процессов СМИБ с ITSM (библиотекой ITIL).
34. Управление персоналом в контексте ИБ: проверка кандидатов при найме, обучение, оффбординг (увольнение).
35. Соглашение о неразглашении (*NDA*) и соглашение об использовании ИТ-ресурсов (*AUP* — *Acceptable Use Policy*).
36. Организация физической безопасности серверных помещений и дата-центров.
37. Жизненный цикл учетной записи пользователя: создание, изменение, блокировка, удаление.
38. Модели управления доступом: дискреционная (*DAC*), мандатная (*MAC*), ролевая (*RBAC*) и атрибутивная (*ABAC*).
39. Многофакторная аутентификация (*MFA*): факторы знания, владения и биометрии.
40. Технология однократного входа (*Single Sign-On, SSO*) и протоколы федерации удостоверений (*SAML, OIDC*).
41. Привилегированный доступ. Использование решений класса *PAM (Privileged Access Management)* и менеджеров паролей.
42. Гостевой доступ и управление учетными записями сторонних контрагентов.
43. Антивирусная защита нового поколения (*EDR* — *Endpoint Detection and Response*) против классических сигнатурных сканеров.
44. Межсетевые экраны следующего поколения (*NGFW*): функции глубокого анализа пакетов (*DPI*) и предотвращения вторжений (*IPS*).
45. Защита веб-приложений (*WAF*). Основные виды атак на уровне приложения (*OWASP Top 10*).
46. Криптографическая защита: симметричное и асимметричное шифрование, инфраструктура открытых ключей (*PKI*).
47. Электронная подпись: юридическая значимость и техническое устройство (усиленная квалифицированная ЭП).
48. Системы предотвращения утечек данных (*DLP*): методы работы (на сетевом шлюзе, на агенте рабочей станции).
49. Центры мониторинга ИБ (*SOC*). Назначение систем сбора событий (*SIEM*) и корреляции инцидентов.

50. Процесс управления инцидентами ИБ (согласно ISO 27035): этапы подготовки, обнаружения, сдерживания, ликвидации и извлечения уроков.
51. Компьютерная криминалистика (*Forensics*). Принципы сохранения цифровых доказательств и цепочки владения (*Chain of Custody*).
52. Тестирование на проникновение (*Penetration Testing*) и анализ защищенности (*Vulnerability Assessment*): отличия целей и методик.
53. Внутренний и внешний аудит ИБ. Периодичность проведения проверок и критерии оценки эффективности.
54. Красная, синяя и фиолетовая команды (*Red / Blue / Purple Teaming*) в практике проверки зрелости защиты.
55. Анализ воздействия на бизнес (*BIA*). Определение максимально допустимого времени простоя (*MTD/RTO*) и точки восстановления (*RPO*).
56. Планирование непрерывности бизнеса (*BCP*) и аварийного восстановления (*DRP*). Различия между целями этих документов.
57. Резервное копирование: правило «3-2-1», типы бэкапов (полный, дифференциальный, инкрементальный) и хранение вне офиса.
58. Экономические показатели ИБ: совокупная стоимость владения (*TCO*) и возврат инвестиций в безопасность (*ROSI*).
59. Ключевые показатели эффективности (*KPI*) и результативности (*KRI*) службы информационной безопасности.
60. Человеческий фактор и программа повышения осведомленности (*Security Awareness*). Методы противодействия социальной инженерии.

3.2. Практические задания к экзамену

Задание №1 Сотрудник компании скопировал базу клиентов на личную флеш-карту, аргументируя это необходимостью «доделать отчет дома».

- **Вопрос:** Какие базовые принципы информационной безопасности (конфиденциальность, целостность, доступность) нарушены? Кто является владельцем актива и кто несет ответственность за инцидент?
- **Требования к анализу:** Определить тип угрозы (внутренняя/внешняя), классифицировать нарушенные организационные меры и предложить алгоритм действий службы ИБ.

Задание №2 В ходе аудита выяснилось, что системный администратор делает резервные копии базы данных бухгалтерии ежедневно, но ни разу не проводил тестовое восстановление. В результате сбоя оборудования база оказалась повреждена, а архивы — нечитаемыми.

- **Вопрос:** Какой ключевой этап процесса обеспечения непрерывности бизнеса (*BCP*) был пропущен? К каким финансовым потерям это приведет?
- **Требования к анализу:** Объяснить разницу между *RPO* и *RTO* в данной ситуации и оценить эффективность управления ИТ-рисками.

Задание №3 Бухгалтер получил электронное письмо от «генерального директора» с пометкой «СРОЧНО! Оплатить счет», содержащее ссылку на веб-форму ввода корпоративных логина и пароля для доступа к новому сервису оплат. Ссылка визуально отличалась от корпоративного домена одним символом.

- **Вопрос:** Как называется данный вид атаки? На какой психологический фактор она рассчитана?
- **Требования к анализу:** Предложить три технических и одну организационную меру защиты, которые предотвратили бы компрометацию учетных данных.

Задание №4 Менеджер по продажам уволился из компании. Через месяц служба безопасности обнаружила, что он использует корпоративную почту бывшего работодателя для переписки с клиентами, переманивая их к конкуренту. Пароль от почты им не менялся две недели после увольнения.

- **Вопрос:** Нарушен ли какой-либо этап жизненного цикла учетной записи? Оцените риски для компании.
- **Требования к анализу:** Описать процедуру оффбординга (увольнения) сотрудника и указать, какие технические средства (например, *IAM*, *IdM*) автоматизируют этот процесс.

Задание №5 Компания закупила самое дорогое на рынке средство защиты от вредоносного ПО, однако установила его с настройками по умолчанию и не обучила администраторов работе с консолью управления. Спустя полгода сеть была заражена шифровальщиком через уязвимость, которую данное средство могло заблокировать при правильной настройке.

- **Вопрос:** Почему инвестиции в ИБ не окупились? Как называется риск эксплуатации средств защиты с небезопасными конфигурациями?
- **Требования к анализу:** Рассчитать показатель эффективности инвестиций в ИБ (*ROSI*) для данного кейса, если ущерб составил 1 млн руб., а стоимость решения — 200 тыс. руб.

Задание №6 Инженер технической поддержки выдал новому стажеру права локального администратора на ноутбуке «для удобства установки рабочих программ», хотя должностной инструкции стажера достаточно прав обычного пользователя.

- **Вопрос:** Какой фундаментальный принцип контроля доступа нарушен? Приведите пример того, как злоумышленник может использовать эту ошибку.
- **Требования к анализу:** Сравнить модели управления доступом *DAC* и *RBAC* применительно к данному случаю.

Задание №7 Организация перенесла всю инфраструктуру в публичное облако. После взлома базы данных руководство обвинило облачного провайдера в плохой защите. Провайдер сослался на условия договора.

- **Вопрос:** Как называется модель распределения ответственности, которая описывает данную ситуацию? За что именно отвечает клиент (пользователь облака)?
- **Требования к анализу:** Разграничить зоны ответственности в модели *Shared Responsibility Model*.

Задание №8 Директор требует внедрить систему защиты, которая гарантирует 100% защиту от всех существующих и будущих хакерских атак.

- **Вопрос:** В чем заключается методологическая ошибка требования руководства? Что такое «остаточный риск»?

- **Требования к анализу:** Объяснить руководству экономическую нецелесообразность попыток сведения риска к нулю.

Задание №9 На сервере произошла утечка персональных данных клиентов. Служба ИБ начала расследование только спустя 3 дня, так как мониторинг событий не велся, а журналы (*логи*) хранились всего 24 часа и были перезаписаны.

- **Вопрос:** Какие требования законодательства РФ (ФЗ-152) по срокам реагирования на инциденты ПДн нарушены? Почему отсутствие системы сбора логов критично для расследования?
- **Требования к анализу:** Назвать основные функции систем класса *SIEM*.

Задание №10 Разработчики выложили исходный код мобильного приложения в открытый репозиторий вместе с файлом конфигурации, где в открытом виде хранились ключи доступа (*API keys*) к платежному шлюзу.

- **Вопрос:** На каком этапе безопасного жизненного цикла разработки (*SDLC*) произошел сбой? Как автоматизированно предотвратить попадание секретов в код?
- **Требования к анализу:** Предложить методы сканирования кода (*SAST, SCA*).

Задание №11 Сторонний электрик во время ремонта подключил свой зараженный вирусами ноутбук к сетевой розетке в коридоре офиса, получив полный доступ к внутренним ресурсам компании.

- **Вопрос:** Какой вид контроля (физический или технический) оказался неэффективным? Что такое управление сетевым доступом (*NAC*)?
- **Требования к анализу:** Описать архитектуру гостевого сегмента сети (*Guest Wi-Fi*).

Задание №12 Сотрудник открыл вложение «Штрафы ГИБДД.pdf.exe», после чего все файлы на его компьютере и общих дисках зашифровались. Злоумышленники требуют выкуп.

- **Вопрос:** Какова первая техническая мера изоляции инцидента? Нужно ли платить выкуп согласно рекомендациям регуляторов?
- **Требования к анализу:** Составить краткий план реагирования на инцидент (*Incident Response Plan*) для этой ситуации.

Задание №13 Компания обрабатывает биометрические данные сотрудников (отпечатки пальцев для входа в офис), но не включила этот факт в уведомление Роскомнадзора об обработке ПДн.

- **Вопрос:** Какое юридическое последствие грозит организации? Чем обработка биометрии отличается от обработки обычных ПДн?
- **Требования к анализу:** Ссылка на конкретные статьи ФЗ-152.

Задание №14 При проектировании отказоустойчивого кластера инженеры разместили оба сервера в одной серверной стойке друг над другом.

- **Вопрос:** Какой принцип проектирования высокой доступности (*High Availability*) нарушен? Какой риск создает такая архитектура?
- **Требования к анализу:** Понятие единой точки отказа (*Single Point of Failure*).

Задание №15 Для экономии места на серверах руководство приказало сократить срок хранения журналов регистрации событий безопасности с одного года до двух недель.

- **Вопрос:** Какую проблему создаст это решение при расследовании сложной целевой атаки (APT), длившейся несколько месяцев?
- **Требования к анализу:** Баланс между стоимостью хранения данных и требованиями комплаенса.

Задание №16 Офицер безопасности обнаружил, что топ-менеджер регулярно отправляет чертежи новой продукции через личный аккаунт Telegram со служебного ноутбука.

- **Вопрос:** Как называется эта угроза (*Shadow IT*)? Какой класс решений (*DLP, CASB*) предназначен для блокировки таких каналов?
- **Требования к анализу:** Различия между контекстным и контентным анализом в *DLP*-системах.

Задание №17 После успешного прохождения внешнего аудита ISO 27001 компания сформировала отдел ИБ для сокращения издержек, передав функции системным администраторам.

- **Вопрос:** Сохранит ли сертификат свою силу при следующем надзорном аудите? Почему?
- **Требования к анализу:** Требования стандарта ISO 27001 к выделению ресурсов и ответственности руководства.

Задание №18 При расчете окупаемости внедрения фаервола аналитик указал снижение вероятности взлома на 100%.

- **Вопрос:** В чем грубая математическая и методологическая ошибка такого расчета?
- **Требования к анализу:** Формула *ROSI* и понятие остаточного риска.

Задание №19 Уборщица вечером воспользовалась оставленным без присмотра разблокированным компьютером бухгалтера, чтобы зайти в социальные сети, случайно скачав вирус.

- **Вопрос:** Помимо нарушения политики паролей, какой аспект подотчетности (*Accountability*) нарушен?
- **Требования к анализу:** Политика «чистого стола» и «заблокированного экрана».

Задание №20 В договоре с облачным провайдером отсутствует пункт о финансовой ответственности (штрафах) за простой сервиса более 4 часов.

- **Вопрос:** Как называется юридически значимый документ, регулирующий уровень доступности услуг? Каких еще метрик в нем не хватает?
- **Требования к анализу:** Понятия *SLA, SLO, KPI*.

Задание №21 Установите правильную последовательность этапов проведения оценки рисков ИБ: А) Выбор методов обработки рисков. Б) Идентификация активов, угроз и уязвимостей. В) Количественная оценка вероятности и ущерба. Г) Мониторинг и пересмотр рисков. (Ответ: Б, В, А, Г)

Задание №22 Установите правильную иерархию документов СМИБ от общего к частному: А) Рабочие инструкции. Б) Политика ИБ верхнего уровня. В) Стандарты и регламенты. (Ответ: Б, В, А)

Задание №23 Установите правильный порядок действий при увольнении ключевого администратора баз данных: А) Заблокировать учетные записи и сменить общие пароли. Б) Провести выходное интервью и отозвать физические пропуска. В) Передача дел преемнику под контролем руководителя. Г) Удаление из всех групп доступа и отзыв сертификатов подписи. (Ответ: Б, В, Г, А)

Задание №24 Установите правильную фазу инцидента, соответствующую действию: «Изоляция зараженного сегмента сети путем отключения порта коммутатора»: А) Ликвидация последствий. Б) Обнаружение. В) Сдерживание (Локализация). Г) Анализ причин. (Ответ: В)

Задание №25 Установите соответствие между термином и определением:

1. Фишинг — ...
2. Социальная инженерия — ...
3. Брутфорс — ... А) Психологическое манипулирование людьми с целью получения конфиденциальной информации. Б) Метод перебора всех возможных комбинаций пароля. В) Массовая рассылка поддельных писем для кражи данных. (Ответ: 1-В, 2-А, 3-Б)

Задание №26 Вычислите величину риска (по упрощенной формуле $V = P \times SS$), если вероятность реализации угрозы (P) составляет 0.2 (20%), а потенциальный ущерб (SS) оценивается в 5 000 000 рублей. Стоит ли тратить 800 000 рублей на внедрение защиты? (Ответ: Риск = 1 000 000 руб. Тратить 800 000 руб. экономически целесообразно, так как стоимость защиты меньше величины риска).

Задание №27 Рассчитайте коэффициент доступности системы, если за год (8760 часов) суммарное время простоя составило 4.38 часа. Соответствует ли это целевому показателю «три девятки» (99.9%)? (Ответ: Доступность = $(8760 - 4.38) / 8760 = 0.9995$ или 99.95%. Целевой показатель достигнут).

Задание №28 Составьте перечень обязательных разделов для «Политики использования съемных носителей информации» в банке. (Ответ: Цель, область применения, классификация носителей, правила шифрования, процедура инвентаризации, ответственность).

Задание №29 Опишите схему разделения обязанностей (SoD) для процесса выплаты счетов поставщикам в ERP-системе. Кто должен создавать заявку, кто утверждать, а кто подписывать платеж? (Ответ: Создает — бухгалтер; Утверждает — финансовый контролер; Подписывает (ЭП) — финансовый директор).

Задание №30 Проведите сравнительный анализ симметричного алгоритма ГОСТ 34.12-2015 («Кузнечик») и асимметричного RSA. Укажите главное преимущество и недостаток каждого в контексте передачи больших объемов данных. (Ответ: ГОСТ — быстр, но сложен в безопасной передаче ключа. RSA — решает проблему обмена ключом, но крайне медленен для больших файлов).

4. КРИТЕРИИ ОЦЕНИВАНИЯ ПРИ ПРОВЕДЕНИИ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Шкала оценивания уровня сформированности компетенций (по пятибалльной системе) экзамен

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 обладающим 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 – экзамен.

Форма проведения промежуточной аттестации – письменный экзамен