

fd935d10451b860e912264c0378f84494f27b9b683f94388088e29877a6b1bf5

Кафедра «Управление и бизнес-информатика»

«02» февраля 2026 г



КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Безопасность компьютерных систем

Бакалавр

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-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.1. Использует типовые криптографические средства защиты информации, в том числе средства электронной подписи ОПК-9.2. Применяет методы и средства технической защиты информации для решения задач профессиональной деятельности

1.1 Вопросы к текущему контролю

1. Дайте определение криптографии, криптоанализа и стеганографии. В чем принципиальное различие между защитой факта передачи сообщения и защитой содержания сообщения?
2. Раскройте содержание триады Керкгоффа («секретность системы должна зависеть только от секретности ключа»). Почему в современной ИБ стойкость алгоритма считается известной злоумышленнику?
3. Что такое алфавит, открытый текст, шифротекст, ключ и алгоритм преобразования? Приведите формальную математическую модель процесса шифрования и расшифрования.
4. Классификация методов шифрования: симметричные и асимметричные криптосистемы. Сравнение их преимуществ, недостатков и основных областей применения.
5. Различие между блочными и поточными шифрами. Понятие режима работы блочного шифра (на примере ECB, CBC).
6. Что такое гаммирование? Операция сложения по модулю два (XOR) и её роль в построении современных шифров.
7. Стандарт шифрования данных *DES (Data Encryption Standard)*. История создания, размер блока, длина ключа и причины его устаревания (атака методом полного перебора).
8. Российский стандарт симметричного блочного шифрования ГОСТ 34.12-2015 (блоки «Магма» и «Кузнечик»). Размер блока, длина ключа и структура раундов.
9. Американский стандарт шифрования *AES (Advanced Encryption Standard, Rijndael)*. Варианты длины ключа (128/192/256 бит) и количество раундов преобразования.
10. Поточковый шифр RC4: принцип работы на основе регистра сдвига с обратной связью (*LFSR*) или генератора псевдослучайных чисел. Уязвимости алгоритма.

11. Режим сцепления блоков шифротекста (*CBC — Cipher Block Chaining*). Как этот режим решает проблему детерминированности шифрования одинаковых блоков открытого текста?
12. Управление ключами в симметричных системах. Проблема распределения ключей (*Key Distribution Problem*). Протокол Диффи-Хеллмана как средство выработки общего секрета.
13. Принцип работы асимметричной криптографии (криптосистемы с открытым ключом). Роль открытого и закрытого ключей. Математическая основа односторонних функций с «потайным входом».
14. Алгоритм *RSA*. Математическая база (сложность факторизации больших целых чисел), процессы генерации ключей, шифрования и цифровой подписи.
15. Российские стандарты асимметричной криптографии: ГОСТ Р 34.10-2012 (формирование и проверка электронной подписи) и ГОСТ Р 34.11-2012 (функция хэширования «Стрибог»).
16. Криптография на эллиптических кривых (*ECC — Elliptic Curve Cryptography*). Преимущества перед классическим *RSA* при сохранении эквивалентного уровня стойкости.
17. Инфраструктура открытых ключей (*PKI — Public Key Infrastructure*). Назначение цифрового сертификата и роль удостоверяющего центра (*CA — Certificate Authority*).
18. Протокол установления защищенного соединения *TLS (Transport Layer Security)*. Как в рамках одной сессии используются и симметричное, и асимметричное шифрование?
19. Криптографическая хэш-функция. Требования к ней: необратимость, стойкость к коллизиям (первому и второму роду), эффект лавины.
20. Семейство алгоритмов *SHA (Secure Hash Algorithm)*: эволюция от *SHA-0/1* до *SHA-2* и *SHA-3*. Почему использование *MD5* и *SHA-1* недопустимо для новых систем?
21. Код аутентификации сообщения (*MAC — Message Authentication Code*). Отличие *MAC* от простой хэш-функции. Концепция *HMAC*.
22. Электронная цифровая подпись (*ЭЦП*). Процесс формирования подписи (хэширование + шифрование хэша закрытым ключом) и процесс проверки.
23. Понятие теоретической (совершенной) стойкости шифра. Шифр Вернама (*One-Time Pad*) как единственный абсолютно стойкий метод. Условия его практической реализации.
24. Вычислительная стойкость современных шифров. Понятие сложности атаки (полный перебор, атака на основе известных/выбранных открытых текстов).
25. Основные методы криптоаналитического вскрытия: линейный и дифференциальный криптоанализ. На каких свойствах преобразований они строятся?
26. Атаки по побочным каналам (*Side-channel attacks*): временной анализ, анализ потребляемой мощности. Почему программная реализация алгоритма может быть менее безопасной, чем аппаратная?
27. Целостность данных vs Конфиденциальность. Почему шифрование само по себе не гарантирует неизменность сообщения? Использование имитовставки (*MIC/MICV*).
28. Жизненный цикл криптографических ключей: генерация, распределение, хранение, смена, архивация и уничтожение. Требования к датчикам случайных чисел (*ДСЧ / TRNG*).
29. Аппаратные модули безопасности (*HSM — Hardware Security Module*). Задачи, которые решают эти устройства, и защита ключей от извлечения.

30. Правовое регулирование использования СКЗИ (средств криптографической защиты информации) в РФ. Классы защиты КС1, КС2, КС3, КВ, КА и условия их применимости.

1.2 Темы рефератов

1. **Эволюция шифров от Древнего мира до XX века:** сравнительный анализ диска Энея, скиталы, шифра Цезаря и дисковых шифровальных машин (Enigma, Purple).
2. **Математические основы современной криптографии:** теория чисел в криптоанализе (простые числа, алгоритм Евклида, малая теорема Ферма, китайская теорема об остатках).
3. **Проблема распределения ключей:** исторический обзор методов передачи секретных ключей и математическое решение проблемы через протокол Диффи-Хеллмана.
4. **Принцип Керкгоффса и открытые алгоритмы:** история перехода от секретности механизмов к секретности ключей в военном деле и коммерческом секторе.
5. **Стойкость криптосистем: теоретическая vs вычислительная.** Абсолютно стойкие шифры (блокнот Вернама) и практические ограничения их использования.
6. **Стандарт DES (Data Encryption Standard):** архитектура сети Фейстеля, критика длины ключа со стороны Агентства национальной безопасности США и его историческое значение.
7. **Российский стандарт ГОСТ 34.12-2015 («Кузнечик»):** структура S-блоков, линейные и диффузионные преобразования, сравнение с международными аналогами.
8. **Американский стандарт AES (Rijndael):** операции SubBytes, ShiftRows, MixColumns и AddRoundKey. Математическое поле Галуа $GF(2^8)$ как основа преобразований.
9. **Режимы работы блочных шифров:** детальный анализ режимов ECB, CBC, CFB, OFB и CTR. Проблемы «шаблонного шифрования» в режиме ECB.
10. **Потоковые шифры на основе регистров сдвига (LFSR):** генератор Геффа и самоусеченный генератор (SSG). Применение потоковых шифров в мобильной связи.
Алгоритм RSA: математическая сложность задачи факторизации больших чисел. Процесс генерации ключей, уязвимости при использовании малых экспонентов.
11. **Криптография на эллиптических кривых (ECC):** преимущества перед RSA в мобильных устройствах и технологиях Интернета вещей (IoT). Стандарты Suite B и ГОСТ Р 34.10-2012.
12. **Инфраструктура открытых ключей (PKI):** роль удостоверяющих центров (CA), иерархия доверия и жизненный цикл цифрового сертификата (X.509).
13. **Атаки на асимметричную криптографию:** атака Винера на малые значения закрытого показателя d , атаки по времени выполнения (*timing attacks*) Пола Кокрейна.
14. **Протокол обмена ключами Диффи-Хеллмана:** работа в конечном поле и на эллиптических кривых (ECDH). Уязвимость к атаке «человек посередине» (*MitM*) и способы её нейтрализации.
16. **Семейство хэш-функций SHA:** эволюция от уязвимого SHA-1 к семейству SHA-2 (SHA-256, SHA-512) и принципиально новому дизайну SHA-3 (Кецсак).
17. **Код аутентификации сообщения (MAC) и HMAC:** обеспечение целостности и подлинности данных без использования асимметричной подписи.

18. **Атаки поиска коллизий:** парадокс дней рождения в криптоанализе. Практическое вскрытие MD5 и создание поддельных сертификатов цифровой подписи.
19. **Электронная подпись в юридически значимом документообороте РФ:** различия между усиленной квалифицированной (*УКЭП*) и неквалифицированной (*УНЭП*) подписью согласно ФЗ-63.
20. **Анализ защищенности протокола TLS 1.3:** отказ от устаревших алгоритмов (RSA для обмена ключами, RC4, CBC), использование режима аутентифицированного шифрования (*AEAD*).
21. **Постквантовая криптография:** угрозы квантовых компьютеров для современных стандартов. Основные направления защиты: криптография на решетках, многомерные квадратичные уравнения, изогении эллиптических кривых.
22. **Аппаратные средства хранения ключей:** устройство и принципы работы доверенных платформенных модулей (*TPM*) и аппаратных модулей безопасности (*HSM*).
23. **Скрытые каналы и стеганография:** метод наименьшего значащего бита (*LSB*), стеганография во вложениях социальных сетей и сетевых протоколах.
24. **Белый ящик криптографии (*White-Box Cryptography*):** защита реализации симметричных алгоритмов в программном обеспечении, где злоумышленник имеет полный контроль над средой исполнения.

1.3 Тестовые задания

1. Какой российский стандарт определяет алгоритм блочного шифрования «Кузнечик»? а) ГОСТ 28147-89. б) ГОСТ Р 34.10-2012. в) ГОСТ Р 34.11-2012. г) ГОСТ Р 34.12-2015. (Правильный ответ: г)
2. Как называется математическая операция, которая преобразует сообщение произвольной длины в строку фиксированной длины (хэш), и при этом является необратимой? а) Шифрование. б) Хэширование. в) Стеганография. г) Кодирование. (Правильный ответ: б)
3. В асимметричной криптосистеме ключ, который хранится в секрете и используется для формирования электронной подписи или расшифрования данных: а) Открытый ключ. б) Сессионный ключ. в) Закрытый (приватный) ключ. г) Мастер-ключ. (Правильный ответ: в)
4. Что из перечисленного является основным недостатком режима ECB (*Electronic Codebook*) при использовании блочных шифров? а) Низкая скорость работы на современных процессорах. б) Сохранение статистических закономерностей открытого текста (проблема «шаблонного шифрования»). в) Невозможность параллельных вычислений. г) Требование использования вектора инициализации (*IV*). (Правильный ответ: б)
5. Какой американский стандарт является общепринятым мировым стандартом симметричного шифрования (преемником DES)? а) RSA. б) AES. в) SHA-256. г) Diffie-Hellman. (Правильный ответ: б)
6. Какая математическая задача лежит в основе стойкости алгоритма RSA? а) Задача дискретного логарифмирования. б) Задача факторизации (разложения на множители) больших целых чисел. в) Задача поиска кратчайшего вектора в решетке. г) Задача коммивояжера. (Правильный ответ: б)
7. Для чего предназначена инфраструктура открытых ключей (*PKI — Public Key Infrastructure*)? а) Для ускорения процесса симметричного шифрования. б) Для связывания открытого ключа с личностью его владельца посредством цифрового сер-

- тификата. в) Для хранения паролей пользователей в зашифрованном виде. г) Для генерации истинно случайных чисел. (Правильный ответ: б)
8. Какое свойство НЕ является обязательным требованием к криптографической хэш-функции? а) Необратимость (невозможность восстановить текст по хэшу). б) Стойкость к коллизиям (трудность найти два разных текста с одинаковым хэшем). в) Обратимость (возможность декодирования исходного сообщения). г) Лавинный эффект (изменение одного бита входа меняет множество бит выхода). (Правильный ответ: в)
9. Протокол установления защищенного соединения между браузером пользователя и веб-сервером, использующий гибридную схему шифрования: а) HTTP. б) FTP. в) TLS / SSL. г) ICMP. (Правильный ответ: в)
10. Какой тип атаки основан на измерении времени выполнения операций, потребляемой мощности процессора или электромагнитного излучения во время работы криптографического устройства? а) Атака полным перебором (*Brute Force*). б) Дифференциальный криптоанализ. в) Линейный криптоанализ. г) Атака по побочным каналам (*Side-channel attack*). (Правильный ответ: г)
11. Установите правильную последовательность этапов классической атаки «человек посередине» (*MitM*) при обмене ключами по протоколу Диффи-Хеллмана: А) Атакующий перехватывает и подменяет публичные значения участников, пересылая им свои собственные. Б) Участники (Алиса и Боб) иницируют сеанс связи и генерируют свои закрытые ключи. В) Участники вычисляют общий секретный ключ, ошибочно полагая, что получили значение партнера. Г) Атакующий устанавливает два независимых защищенных канала: один с Алисой, другой с Бобом. Ответ: Б, А, Г, В.
12. Установите правильную иерархию документов в системе управления криптографическими ключами от общего к частному: А) Рабочие инструкции оператора *HSM* (пошаговый алгоритм инициализации). Б) Политика управления ключами (*Key Management Policy* — декларация целей). В) Регламент генерации и распределения ключей (конкретные требования к ролям). Ответ: Б, В, А.
13. Установите правильный порядок математических действий при формировании электронной подписи по алгоритму RSA: А) Зашифрование полученного хэша закрытым ключом отправителя. Б) Вычисление криптографического хэша от сообщения. В) Передача получателю исходного текста вместе с цифровой подписью. Г) Проверка подлинности сертификата отправителя через цепочку доверия *PKI*. Ответ: Б, А, В, Г.
14. Установите правильную последовательность фаз жизненного цикла криптографического ключа согласно стандарту NIST SP 800-57: А) Использование ключа для операций шифрования или подписи. Б) Генерация ключевого материала с использованием одобренного ДСЧ. В) Архивация или уничтожение ключа после окончания срока действия. Г) Резервное копирование и надежное хранение копии ключа. Ответ: Б, Г, А, В.
15. Установите правильную последовательность раундов преобразования в одном цикле (раунде) алгоритма AES (*Rijndael*): А) Сложение раундового ключа с состоянием (*AddRoundKey*). Б) Нелинейная замена байтов (*SubBytes*). В) Смещение строк состояния (*ShiftRows*). Г) Смешивание столбцов (*MixColumns*). Ответ: Б, В, Г, А.
16. Установите правильную последовательность действий администратора безопасности при компрометации закрытого ключа удостоверяющего центра (CA): А) Публикация серийного номера ключа в списке отзыва сертификатов (*CRL*). Б) Оповещение всех доверяющих сторон об инциденте. В) Инициализация процедуры генерации новой пары ключей и корневого сертификата. Г) Немедленное прекращение выпуска новых сертификатов на данном ключе. Ответ: Г, Б, А, В.

17. Установите правильную хронологию принятия государственных стандартов шифрования в России (от самого старого к самому новому): А) ГОСТ Р 34.10-2012 (Электронная подпись). Б) ГОСТ 28147-89 (Симметричное блочное шифрование «Магма»). В) ГОСТ Р 34.12-2015 (Введение блочного шифра «Кузнечик»). Ответ: Б, В, А.
18. Установите правильную последовательность установления TLS-соединения (упрощенная схема классического обмена): А) Согласование набора алгоритмов (*Cipher Suite*) сервером. Б) Запрос клиента (*ClientHello*) со списком поддерживаемых версий и шифров. В) Переход на зашифрованный режим передачи данных (*Finished-сообщения*). Г) Передача сервером своего сертификата с открытым ключом (*ServerHello/Certificate*). Ответ: Б, А, Г, В.
19. Установите правильную последовательность проверки целостности дистрибутива программы пользователем: А) Вычисление контрольной суммы скачанного файла на своем компьютере. Б) Скачивание эталонного хэш-значения с официального сайта разработчика. В) Сравнение полученного результата с эталонным значением. Г) Нахождение ссылки на скачивание программного обеспечения. Ответ: Г, Б, А, В.
20. Установите правильную последовательность применения режимов работы симметричного шифра для обеспечения защиты от повтора сообщений (*replay protection*): А) Использование вектора инициализации (*IV*) или счетчика. Б) Разбиение потока данных на блоки. В) Накопление поппе (числа, используемого один раз) на стороне приемника. Г) Побитовое сложение гаммы шифра с открытым текстом. Ответ: Б, А, Г, В.
21. Установите правильную последовательность уровней реализации криптоанализа по сложности доступа к объекту (от самого простого к самому сложному): А) Атака по побочным каналам (анализ потребления энергии/времени). Б) Криптоанализ на основе только шифротекста (*Ciphertext-only*). В) Полный физический доступ к устройству и возможность его вскрытия. Г) Возможность выбора открытого текста для шифрования (*Chosen-plaintext attack*). Ответ: Б, Г, А, В.
22. Установите правильную последовательность процессов внутри сети Фейстеля (на примере раунда DES): А) Применение S-блоков (нелинейная подстановка). Б) Расширение правой половины блока путем дублирования некоторых бит. В) Начальная перестановка всего блока данных (*IP*). Г) Сложение расширенной части с раундовым ключом. Ответ: В, Б, Г, А.
23. Установите правильную иерархию ключей в архитектуре иерархической системы управления ключами (*Master Key -> ...*): А) Сессионный ключ (для шифрования конкретного массива данных). Б) Мастер-ключ (хранится в *HSM*, используется для шифрования других ключей). В) Ключи шифрования ключей (*KEK* — защищают группы сессионных ключей). Ответ: Б, В, А.
24. Установите правильную последовательность усиления пароля перед его сохранением в базе данных (процесс создания хэша): А) Многократное повторение функции хеширования (итерации/*stretching*). Б) Добавление уникальной случайной строки («соль» — *salt*) к паролю. В) Выбор пользователем исходного пароля. Г) Вычисление финального хэш-значения для записи в БД. Ответ: В, Б, А, Г.
25. Установите правильную последовательность действий при проверке корректности сертификата X.509 браузером: А) Поиск издателя (вышестоящего *CA*) в хранилище доверенных корневых центров. Б) Математическая проверка подписи текущего сертификата с помощью открытого ключа издателя. В) Извлечение сертификата из цепочки, присланной сервером. Г) Проверка срока действия и отсутствия серийного номера в списках отзыва (*CRL/OCSP*). Ответ: В, А, Б, Г.
26. Установите правильную временную шкалу развития криптографии (эпохи): А) Эпоха компьютеров и асимметричной криптографии (Диффи-Хеллман, *RSA*). Б) Эпоха механических и электромеханических машин (Энигма, *Purple*). В) Эпоха

- классической криптографии (шифры сдвига, полиалфавитные шифры). Ответ: В, Б, А.
27. Установите правильную последовательность обработки данных в режиме счетчика (CTR): А) Инкремент (увеличение) значения счетчика для каждого следующего блока. Б) Шифрование значения счетчика ключевым потоком. В) Побитовое XOR (сложение) полученного ключевого потока с открытым текстом. Г) Формирование уникального начального значения счетчика (*nonce + counter*). Ответ: Г, Б, В, А.
28. Установите правильную последовательность проверки легитимности использования СКЗИ (средства криптографической защиты информации) в государственном органе РФ: А) Закупка сертифицированной версии продукта у вендора. Б) Определение модели угроз и требуемого класса защиты (КС1–КА). В) Получение лицензии ФСБ на работу с криптографией (если требуется регламентом). Г) Монтаж и ввод в эксплуатацию с составлением технического паспорта. Ответ: Б, В, А, Г.
29. Установите правильную последовательность возникновения коллизий в семействе хэш-функций *SHA* (от первого принятого стандарта до полной потери доверия): А) *SHA-1* (теоретические уязвимости стали практическими). Б) *MD5* (быстрое нахождение коллизий на обычном ПК). В) *SHA-2* (на текущий момент считается стойким). Ответ: В, А, Б.
30. Установите правильную последовательность слоев защиты в концепции «глубоко эшелонированной обороны» (*Defense in Depth*) применительно к защите базы данных: А) Шифрование самих таблиц или ячеек данных на уровне СУБД (*TDE / Column-level encryption*). Б) Физическая защита сервера (замки, видеонаблюдение). В) Контроль сетевого доступа (Межсетевой экран разрешает подключения только с IP-адресов приложений). Г) Управление доступом на уровне ОС и ролей пользователей (*RBAC*). Ответ: Б, В, Г, А.

1.4 Задания

1. **Ситуация.** Системный администратор ежедневно делает резервные копии базы данных, но ни разу не проводил тестовое восстановление. В результате сбоя оборудования выяснилось, что архивы повреждены и данные за последний месяц утеряны. **Вопрос:** Какой критический этап процесса обеспечения непрерывности бизнеса (BCP) был нарушен? Как это влияет на показатели *RPO* и *RTO*? (*Правильный ответ: Нарушен этап тестирования процедур восстановления (DR-тест). Фактическое значение RPO стремится к бесконечности для утраченных данных, а RPO по регламенту не достигнуто.*)
2. **Ситуация.** Бухгалтер получил письмо от «генерального директора» со ссылкой 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 тип атаки? Почему использование асимметричной подписи в корпоративной почте могло предотвратить этот инцидент? (*Правильный ответ: Фишинг (или спуфинг). Корректная S/MIME или PGP подпись гарантирует подлинность отправителя и целостность письма, позволяя почтовому клиенту пометить его как поддельное.*)
3. **Ситуация.** При проектировании отказоустойчивого кластера инженеры разместили оба сервера с репликами базы данных в одной серверной стойке друг над другом. **Вопрос:** Какой фундаментальный принцип проектирования высокой доступности (*High Availability*) нарушен? К какому типу риска приводит данная ошибка при возникновении пожара в дата-центре? (*Правильный ответ: Нарушено физическое*

разделение / Anti-affinity. Создана единая точка отказа — физическая стойка, что ведет к полной потере доступности сервиса одновременно для обоих узлов.)

4. **Ситуация.** Компания закупила самое дорогое средство защиты информации (например, DLP-систему), но установила его с настройками по умолчанию и не обучила персонал работе с консолью управления. Спустя полгода сеть была заражена через канал, который система могла заблокировать. **Вопрос:** Почему инвестиции в ИБ оказались неэффективными? Какое понятие из экономики ИБ описывает соотношение стоимости взлома и стоимости защиты в данном кейсе? *(Правильный ответ: Ошибка конфигурации и отсутствие процессов эксплуатации. Нарушен баланс между капитальными затратами (CAPEX) и операционными расходами (OPEX); показатель ROSI будет отрицательным.)*
5. **Ситуация.** Инженер технической поддержки выдал новому стажеру права локального администратора на ноутбуке «для удобства установки рабочих программ», хотя должностной инструкции достаточно прав обычного пользователя. **Вопрос:** Какой фундаментальный принцип контроля доступа нарушен? Приведите пример того, как злоумышленник может использовать эту ошибку для повышения привилегий. *(Правильный ответ: Принцип наименьших привилегий (Least Privilege). Злоумышленник, получив доступ под учетной записью стажера через вирус, сможет отключить антивирус или установить руткит благодаря правам админа.)*
6. **Ситуация.** Организация перенесла всю инфраструктуру в публичное облако. После утечки данных руководство обвинило провайдера в плохой защите. Провайдер сослался на условия договора, где указано, что клиент сам управляет правами доступа к своим базам данных. **Вопрос:** Как называется модель распределения ответственности, описывающая данную ситуацию? За какой именно слой безопасности отвечает компания-клиент? *(Правильный ответ: Модель общей ответственности (Shared Responsibility Model). Клиент несет ответственность за безопасность «внутри облака»: настройки ОС, СУБД, управление пользователями и шифрование своих данных.)*
7. **Ситуация.** Руководство требует внедрить систему защиты, которая математически гарантирует 100% защиту от всех существующих и будущих хакерских атак. **Вопрос:** В чем заключается методологическая ошибка требования руководства? Что такое «остаточный риск» и почему он никогда не равен нулю? *(Правильный ответ: Риск нельзя свести к нулю, только до приемлемого уровня. Остаточный риск всегда существует из-за уязвимостей нулевого дня, человеческого фактора и несовершенства технологий.)*
8. **Ситуация.** На сервере произошла утечка персональных данных. 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 технические средства класса мониторинга отсутствуют в компании? Почему отсутствие исторических логов делает невозможным соблюдение требований законодательства РФ о сроках уведомления регуляторов об утечках ПДн? *(Правильный ответ: Отсутствуют системы сбора событий (SIEM) и долгосрочное хранилище логов. Без первичных доказательств невозможно определить вектор атаки и масштаб ущерба для отчета перед РКН/ФСТЭК.)*
9. **Ситуация.** 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 публичный код? *(Правильный ответ: Этап безопасной сборки/верификации кода. Использование сканеров секретов (Secret Scanning) в CI/CD пайплайне и переменных окружения вместо жестко заданных ключей.)*

10. **Ситуация.** Сторонний электрик во время ремонта подключил свой личный заряженный ноутбук к сетевой розетке в коридоре офиса, получив полный доступ к внутренним ресурсам компании. **Вопрос:** Какой технический контроль оказался неэффективным? Что такое протоколы контроля сетевого доступа (NAC) и как они решают эту проблему? *(Правильный ответ: Неэффективна сегментация сети и физический контроль портов. NAC блокирует доступ устройству до тех пор, пока оно не пройдет проверку на наличие обновлений ОС и антивируса.)*
11. **Ситуация.** Сотрудник открыл вложение «Штрафы ГИБДД.pdf.exe», после чего все файлы на его компьютере и общих дисках зашифровались. Злоумышленники требуют выкуп в криптовалюте. **Вопрос:** Какова первая техническая мера изоляции инцидента согласно планам реагирования (IRP)? Нужно ли платить выкуп согласно рекомендациям регуляторов (например, ФСБ)? *(Правильный ответ: Немедленное отключение машины от ЛВС и Wi-Fi. Платить выкуп не рекомендуется, так как это поощряет преступников и не гарантирует получение ключа расшифрования.)*
12. **Ситуация.** 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 («тихий» период присутствия)? *(Правильный ответ: Невозможность проведения ретроспективного анализа. Улики будут уничтожены раньше, чем обнаружится факт компрометации, что нарушает требования комплаенса к хранению аудита.)*
13. **Ситуация.** Офицер безопасности обнаружил, что топ-менеджер регулярно отправляет чертежи новой продукции через личный аккаунт мессенджера со служебного ноутбука. **Вопрос:** Как называется эта угроза (Shadow IT)? Какой класс решений предназначен для блокировки таких несанкционированных каналов передачи данных? *(Правильный ответ: Shadow IT / Insider Threat. Для предотвращения используются системы предотвращения утечек данных (DLP) с контролем облачных сервисов и мессенджеров.)*
14. **Ситуация.** После успешного прохождения внешнего аудита ISO 27001 компания расформировала отдел ИБ для сокращения издержек, передав функции системным администраторам без изменения их должностных инструкций. **Вопрос:** Сохранит ли сертификат свою силу при следующем надзорном аудите? Требование какого принципа стандарта будет нарушено? *(Правильный ответ: Нет, сертификат будет аннулирован. Нарушен принцип выделения ресурсов, ответственности руководства и разделения обязанностей.)*
15. **Ситуация.** При расчете окупаемости внедрения фаервола аналитик указал снижение вероятности взлома на 100%. **Вопрос:** В чем грубая математическая ошибка такого расчета? Может ли вероятность реализации угрозы быть равна абсолютному нулю? *(Правильный ответ: Вероятность не может быть равна 0, всегда остается остаточный риск. Формула ROSI станет некорректной, так как деление на ноль или зануление риска физически невозможны.)*
16. **Ситуация.** Уборщица вечером воспользовалась оставленным разблокированным компьютером бухгалтера, чтобы зайти в социальные сети, случайно скачав вирус-шифровальщик. **Вопрос:** Помимо нарушения политики паролей, какой аспект информационной безопасности (из триады CIA) пострадал первым делом в момент использования чужого профиля? *(Правильный ответ: Подотчетность (Accountability). Все действия вируса в системе будут зафиксированы в журналах как легитимные действия бухгалтера.)*
17. **Ситуация.** 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 метрик в нем критически не хватает? *(Правильный ответ: Соглашение об*

уровне обслуживания — SLA. Не хватает показателей MTTR (среднее время восстановления) и финансовых санкций за недостижение аптайма.)

18. **Ситуация.** Установите правильную последовательность этапов классической электронной подписи: А) Вычисление хэша сообщения. Б) Шифрование полученного хэша закрытым ключом автора. В) Прикрепление полученной подписи к документу. Г) Передача документа и подписи получателю. Ответ: А, Б, В, Г.
19. **Ситуация.** Установите правильную иерархию криптографических алгоритмов по сложности взлома методом полного перебора (от самого слабого к самому стойкому): А) DES (56 бит). Б) ГОСТ 28147-89 (256 бит). В) AES-128 (128 бит). Ответ: А, В, Б.
20. **Ситуация.** Установите правильный порядок действий администратора при плановой смене мастер-ключа в HSM: А) Дешифрование всех данных старым ключом и перешифрование новым. Б) Генерация нового мастер-ключа внутри защищенного модуля. В) Резервное копирование старого ключа в архив. Г) Обновление ссылок на ключ в конфигурациях приложений. Ответ: В, Б, А, Г.
21. **Ситуация.** Установите соответствие между стандартом и объектом регулирования:
22. ГОСТ Р 34.10-2012 — ...
23. ГОСТ Р 34.12-2015 — ...
24. ГОСТ Р 34.11-2012 — ... А) Блочное шифрование. Б) Функция хэширования. В) Электронная подпись. Ответ: 1-В, 2-А, 3-Б.
25. **Ситуация.** Установите правильную временную шкалу принятия стандартов симметричного шифрования в РФ (от старейшего к новейшему): А) ГОСТ Р 34.12-2015 («Кузнечик»). Б) ГОСТ 28147-89 («Магма»). Ответ: Б, А.
26. **Ситуация.** Установите правильную фазу TLS-рукопожатия: А) Проверка сертификата сервера клиентом. Б) Согласование набора шифров (Cipher Suite). В) Переход на зашифрованный обмен Finished-сообщениями. Ответ: Б, А, В.
27. **Ситуация.** Установите правильную последовательность проверки целостности файла пользователем: А) Скачивание эталонного .sha256 файла с сайта. Б) Запуск утилиты хэширования на скачанном дистрибутиве. В) Побитовое сравнение двух строк. Ответ: А, Б, В.
28. **Ситуация.** Установите правильную архитектуру PKI снизу вверх (от конечного пользователя к корню): А) Промежуточный удостоверяющий центр. Б) Конечный пользователь (сертификат SSL/TLS). В) Корневой удостоверяющий центр (Root CA). Ответ: Б, А, В.
29. **Ситуация.** Установите правильную хронологию криптоанализа MD5: А) Практическое создание коллизии (поддельного сертификата). Б) Теоретические предположки дифференциального криптоанализа. В) Полный запрет использования в браузерах. Ответ: Б, А, В.
30. **Ситуация.** Установите уровни эшелонированной обороны (Defense in Depth) от внешнего края к данным: А) Шифрование самих файлов БД. Б) Межсетевой экран периметра. В) Контроль доступа на уровне ОС сервера. Ответ: Б, В, А.
31. **Ситуация.** Установите этапы обработки инцидента ИБ: А) Локализация (изоляция порта коммутатора). Б) Анализ причин (форензика). В) Обнаружение (алерт от SIEM). Г) Восстановление (развертывание из бэкапа). Ответ: В, А, Б, Г.
32. **Ситуация.** Установите слои модели OSI, на которых работают указанные механизмы защиты:
33. IPsec VPN — ...
34. TLS/SSL — ...
35. WPA2/WPA3 — ... А) Транспортный уровень (L4). Б) Канальный уровень (L2). В) Сетевой уровень (L3). Ответ: 1-В, 2-А, 3-Б.

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-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.1. Использует типовые криптографические средства защиты информации, в том числе средства электронной подписи ОПК-9.2. Применяет методы и средства технической защиты информации для решения задач профессиональной деятельности

3.1 Вопросы к экзамену

1. Основные понятия криптологии: криптография, криптоанализ, стеганография. Различия между защитой содержания и защитой факта передачи сообщения.
2. Принцип Керкгоффса и его современная интерпретация. Почему стойкость алгоритма не должна зависеть от секретности самого алгоритма?
3. Математическая модель симметричной криптосистемы. Понятия открытого текста, шифротекста, ключа и пространства ключей.
4. Классификация методов шифрования: потоковые и блочные шифры. Требования к современным криптографическим алгоритмам.
5. Логические операции в криптографии: сложение по модулю два (*XOR*) и его роль в построении шифров гаммирования.
6. Модулярная арифметика в криптографии: понятие кольца вычетов, обратимость элементов, использование в асимметричных алгоритмах.
7. Простые числа и их свойства. Задача проверки простоты чисел и её значение для генерации ключей RSA.
8. Дискретное логарифмирование в конечном поле. Сложность задачи как основа стойкости протоколов Диффи-Хеллмана и DSA.
9. Понятие односторонней функции с «потайным входом» (*trapdoor one-way function*). Примеры таких функций.
10. Абсолютно стойкие шифры. Теорема Шеннона. Условия практической реализации шифра Вернама (одноразового блокнота).
11. Архитектура сети Фейстеля. Принципы построения (рассеивание и перемешивание) по Клоду Шеннону.
12. Российский стандарт ГОСТ 28147-89 («Магма»). Структура S-блоков, количество раундов, режимы работы (замена, гаммирование, гаммирование с обратной связью).
13. Современный российский стандарт ГОСТ Р 34.12-2015. Блочный шифр «Кузнечик»: структура линейных и нелинейных преобразований, отличие от «Магмы».
14. Стандарт *DES (Data Encryption Standard)*: длина блока, длина ключа, структура раунда. Причины уязвимости DES перед методом полного перебора.
15. Тройной *DES (3DES/Triple DEA)*. Механизм *EDE (Encrypt-Decrypt-Encrypt)* и увеличение эффективной длины ключа.
16. Американский стандарт *AES (Advanced Encryption Standard, Rijndael)*. Операции *SubBytes*, *ShiftRows*, *MixColumns*, *AddRoundKey*.
17. Поле Галуа $GF(2^8)$ и его применение в алгоритме AES для выполнения операций замены и смешивания столбцов.
18. Режимы сцепления блоков: *ECB*, *CBC*, *CFB*, *OFB*. Проблема детерминированности режима *ECB* («шаблонное шифрование»).
19. Потоковый шифр RC4: принцип работы генератора псевдослучайных чисел. Критические уязвимости алгоритма и причины отказа от него в протоколах TLS/SSL.
20. Сравнение аппаратной и программной реализации симметричных шифров. Преимущества использования инструкций *AES-NI*.
21. История возникновения асимметричной криптографии. Проблема распределения ключей (*Key Distribution Problem*) и решение через протокол Диффи-Хеллмана (*DH*).
22. Алгоритм RSA: математическая база (сложность факторизации). Процессы генерации ключевой пары, шифрования и расшифрования.

23. Скорость работы RSA. Использование малых экспонент ($e=3$, $e=65537$) и связанные с этим риски безопасности.
24. Протокол обмена ключами Диффи-Хеллмана в конечном поле (*Finite Field DH*) и на эллиптических кривых (*ECDH*).
25. Цифровая подпись по схеме RSA. Процесс формирования подписи (хэш + закрытый ключ) и процесс проверки (открытый ключ).
26. Российские стандарты ЭЦП: ГОСТ Р 34.10-2012. Использование группы точек эллиптической кривой над конечным полем.
27. Хэш-функции как составная часть цифровой подписи. Свойства необратимости и стойкости к коллизиям.
28. Инфраструктура открытых ключей (*PKI*). Назначение цифрового сертификата стандарта X.509 и роль удостоверяющего центра (*CA*).
29. Цепочка доверия (*Chain of Trust*). Проверка валидности сертификата: пути сертификации, кросс-сертификация.
30. Списки отзыва сертификатов (*CRL*) и протокол онлайн-статуса сертификата (*OCSP*). Проблемы производительности и конфиденциальности при проверке отзыванных сертификатов.
31. Криптографическая хэш-функция: определение и основные требования (эффект лавины, стойкость к поиску прообраза и коллизий).
32. Семейство алгоритмов *MD* (*Message Digest*). Уязвимости MD4 и MD5, позволяющие проводить атаки поиска коллизий на обычном ПК.
33. Семейство *SHA* (*Secure Hash Algorithm*). Особенности SHA-1, причины его компрометации и перехода индустрии на SHA-2 и SHA-3.
34. Конструкция Меркла-Дамгора, используемая в большинстве хэш-функций (включая SHA-2). Парадокс дней рождения в криптоанализе.
35. Код аутентификации сообщения (*MAC — Message Authentication Code*). Отличие MAC от обычной хэш-функции (требование знания ключа).
36. *HMAC (Hash-based MAC)*. Структура конструкции (ipad/opad) и обеспечение целостности данных совместно с аутентификацией источника.
37. Режим имитовставки (*CMAC*) на основе блочных шифров (ГОСТ или AES). Применение в банковских смарт-картах и защищенных чипах.
38. Аутентифицированное шифрование (*Authenticated Encryption*, режимы *CCM*, *GCM*). Одновременное обеспечение конфиденциальности и целостности без отдельного вычисления MAC.
39. Функция растяжения ключа (*KDF — Key Derivation Function*). Применение PBKDF2, bcrypt, scrypt для защиты паролей от атак полным перебором.
40. Специализированные хэш-функции для легковесной криптографии (например, семейства PHOTON, SPONGENT) и их применение в IoT.
41. Жизненный цикл криптографического ключа: генерация, распределение, хранение, смена, архивация, отзыв и уничтожение.
42. Источники энтропии и датчики случайных чисел (*ДСЧ/TRNG* vs *ГПСЧ/PRNG*). Требования NIST к качеству случайности для генерации ключей.
43. Иерархия ключей: мастер-ключи, ключи шифрования ключей (*KEK*) и сессионные (данные) ключи. Принцип разделения зон ответственности.
44. Аппаратные модули безопасности (*HSM*) и доверенные платформенные модули (*TPM*). Защита ключей от извлечения из оперативной памяти.
45. Протокол установления защищенного соединения TLS 1.2: Handshake-процесс, выбор Cipher Suite, обмен ключами и проверка подлинности сервера.
46. Нововведения протокола TLS 1.3: отказ от слабых алгоритмов (RSA key exchange, CBC), обязательное использование Perfect Forward Secrecy (*PFS*).

47. Протокол SSH (*Secure Shell*): механизм привязки хост-ключей (*TOFU — Trust on First Use*) и защита от атак типа MitM при первом подключении.
48. Система электронных сообщений *S/MIME* и *PGP*. Различия моделей доверия (иерархическая в *S/MIME* и "паутина доверия" в *PGP*).
49. Белое-box криптография (*White-Box Cryptography*). Попытка защитить реализацию алгоритма в ПО, где злоумышленник имеет полный контроль над средой исполнения.
50. Квантовая криптография (*QKD — Quantum Key Distribution*). Протокол BB84 и теоретическая невозможность перехвата ключа без внесения ошибок.
51. Методы криптоанализа: атака на основе только шифротекста (*COA*), известного открытого текста (*KPA*) и выбранного открытого текста (*CPA*).
52. Линейный и дифференциальный криптоанализ блочных шифров. Суть методов накопления вероятностей прохождения раундов.
53. Атаки по побочным каналам (*Side-channel attacks*): временной анализ (*timing attack*), анализ потребляемой мощности (*SPA/DPA*).
54. Социальная инженерия как метод обхода криптографической защиты. Психологические аспекты фишинга и кражи ключей.
55. Атака «человек посередине» (*Man-in-the-Middle*) в протоколе Диффи-Хеллмана. Необходимость аутентификации сторон для предотвращения данной атаки.
56. Атаки повторного воспроизведения (*Replay Attacks*) и способы защиты (использование nonce, временных меток, порядковых номеров пакетов).
57. Экономическая эффективность криптозащиты. Расчет возврата инвестиций в безопасность (*ROSI*) применительно к внедрению систем шифрования дисков.
58. Оценка стойкости современных алгоритмов в свете развития квантовых компьютеров. Постквантовая криптография (криптография на решетках).
59. Правовое регулирование СКЗИ в РФ. Классы защиты КС1, КС2, КС3, КВ, КА и условия их применения для различных типов информационных систем.
60. Сертификация средств криптографической защиты информации (СКЗИ) во ФСТЭК России и ФСБ России. Процедура проведения оценки соответствия (*ОКР*).

3.2. Практические задания к экзамену

Задание №1 Сотрудник IT-отдела для удаленного администрирования открыл на межсетевом экране RDP-доступ (порт 3389) ко всем серверам компании из любой точки интернета.

- **Вопрос:** Какая фундаментальная ошибка проектирования сети допущена? Какой тип атаки становится возможен в первую очередь?
- **Требования к анализу:** Предложить безопасную альтернативу (VPN, Zero Trust) и описать настройки фильтрации доступа.

Задание №2 Администратор базы данных установил пароль «Admin123» для учетной записи sa на SQL-сервере, доступном извне. Через сутки сервер был взломан методом грубой силы (*brute-force*).

- **Вопрос:** Какие технические меры контроля парольной политики были проигнорированы?
- **Требования к анализу:** Рассчитать примерное время перебора такого пароля при скорости 1000 попыток в секунду и предложить требования к сложности паролей согласно современным стандартам (NIST/ГОСТ).

Задание №3 Бухгалтер получил письмо с вложением «Акт сверки.pdf.exe». После запуска файла все документы на компьютере сменили расширения на .crypted, а на рабочем столе появилось требование выкупа.

- **Вопрос:** К какому классу криптографических преобразований прибегают злоумышленники? Почему антивирус не обнаружил файл сразу?
- **Требования к анализу:** Описать алгоритм действий по изоляции инцидента без уплаты выкупа и роль резервного копирования.

Задание №4 Компания использует протокол HTTPS для своего сайта, но сертификат выдан самоподписанным удостоверяющим центром, который не добавлен в хранилище доверенных корневых центров пользователей.

- **Вопрос:** Сработает ли шифрование трафика? Какую ошибку увидит браузер пользователя и какой вектор атаки это открывает?
- **Требования к анализу:** Объяснить разницу между конфиденциальностью соединения и проверкой подлинности сервера.

Задание №5 Разработчики выложили мобильное приложение в магазин вместе с файлом конфигурации, где API-ключ облачного хранилища хранился в открытом виде.

- **Вопрос:** На каком этапе жизненного цикла разработки (SDLC) произошел сбой? Как автоматизированно найти такие утечки до релиза?
- **Требования к анализу:** Предложить метод безопасного хранения секретов (например, использование переменных окружения или HashiCorp Vault).

Задание №6 В системе электронного документооборота используется электронная подпись, но проверка срока действия сертификата подписанта отключена программно для ускорения работы системы.

- **Вопрос:** В чем заключается риск использования отозванного (*revoked*) или просроченного сертификата?
- **Требования к анализу:** Описать механизм проверки статуса сертификата через протоколы CRL и OCSP.

Задание №7 Два администратора используют один общий логин `root` с одинаковым паролем для управления критическим сервером.

- **Вопрос:** Какой принцип информационной безопасности нарушен? Почему расследование инцидента в данном случае невозможно?
- **Требования к анализу:** Внедрить персональную идентификацию и двухфакторную аутентификацию (MFA).

Задание №8 Организация хранит ПДн клиентов в базе данных в открытом виде, полагаясь только на защиту периметра сетевым экраном.

- **Вопрос:** Что произойдет с данными при успешном *SQL-инъекционном* обходе экрана? Какое свойство ИБ будет безвозвратно утрачено?
- **Требования к анализу:** Применить принцип эшелонированной обороны: внедрить прозрачное шифрование БД (TDE) и маскирование данных.

Задание №9 При обмене ключами по протоколу Диффи-Хеллмана стороны не проверяют подлинность друг друга (отсутствует цифровая подпись параметров).

- **Вопрос:** Как называется атака, позволяющая злоумышленнику встать посередине (*MitM*) и подменить публичные ключи?
- **Требования к анализу:** Нарисовать схему перехвата сессии и показать, как аутентификация сторон предотвращает эту атаку.

Задание №10 Пароли пользователей в базе данных хранятся в виде хэш-функции MD5 без использования «соли».

- **Вопрос:** Почему злоумышленник, получив доступ к БД, мгновенно узнает пароли большинства пользователей?
- **Требования к анализу:** Использовать радужные таблицы (*Rainbow Tables*) для демонстрации уязвимости и предложить переход на алгоритмы семейства Argon2 или bcrypt.

Задание №11 Инженер подключил ноутбук отдела разработок напрямую в сеть завода, соединив офисный сегмент и технологический сегмент АСУ ТП одним патч-кордом.

- **Вопрос:** Какая концепция сегментации сети была нарушена? Чем грозит наличие моста между ИТ и ОТ сетями?
- **Требования к анализу:** Настроить демилитаризованную зону (*DMZ*) и однонаправленные шлюзы (*дата-диоды*).

Задание №12 Компания использует симметричный алгоритм ГОСТ 28147-89 в режиме простой замены (*ECB*) для шифрования изображений.

- **Вопрос:** Почему на зашифрованном изображении будут отчетливо видны контуры исходного рисунка?
- **Требования к анализу:** Перевести систему на режим гаммирования с обратной связью (*CFB*) или сцепления блоков (*CBC*).

Задание №13 Удостоверяющий центр (CA) подписал пользовательский сертификат, используя алгоритм хэширования SHA-1.

- **Вопрос:** Почему современные браузеры пометят такой сайт как небезопасный («Not Secure»)?
- **Требования к анализу:** Описать процесс практической генерации коллизии для SHA-1 и её последствия для подделки сертификатов.

Задание №14 Оператор связи передает трафик клиента в открытом виде между городами по своей магистральной сети, считая внутреннюю сеть «доверенной зоной».

- **Вопрос:** Кто может осуществить перехват легитимно с точки зрения оператора и нелегитимно со стороны хакера?
- **Требования к анализу:** Обосновать необходимость применения MACsec или IPsec для шифрования каналов связи.

Задание №15 Пользователь заходит в корпоративный Wi-Fi с личным смартфоном, вводя свой доменный пароль от почты.

- **Вопрос:** Какой протокол аутентификации должен использоваться в корпоративных сетях вместо передачи пароля в открытом или слабо защищенном виде?
- **Требования к анализу:** Сравнить безопасность протоколов WPA2-PSK и WPA2-Enterprise (IEEE 802.1X).

Задание №16 В мобильном приложении банка функция jailbreak/root detection отключена. Пользователь имеет права суперпользователя на телефоне.

- **Вопрос:** Почему среда считается недоверенной и какие данные приложения (ключи, токены) становятся доступны злоумышленнику?
- **Требования к анализу:** Использование белой-бох криптографии или вынос операций на сторону сервера (*HSM*).

Задание №17 Срок действия ключевого материала для подписи платежных поручений составляет 10 лет без процедуры смены ключа.

- **Вопрос:** В чем опасность компрометации ключа с таким сроком жизни? Как часто рекомендуется менять сессионные ключи?
- **Требования к анализу:** Разработать регламент плановой ротации ключей согласно требованиям ФСБ/НЛЦ.

Задание №18 Система дистанционного банковского обслуживания (ДБО) отправляет клиенту SMS-код подтверждения операции, но не привязывает этот код к конкретной сумме и получателю платежа.

- **Вопрос:** Как называется атака, при которой злоумышленник инициирует перевод, перехватывает SMS и заставляет жертву продиктовать код?
- **Требования к анализу:** Текст SMS-сообщения должен содержать детали транзакции (сумма, последние цифры карты).

Задание №19 Для защиты канала VPN используется устаревший протокол PPTP с аутентификацией MS-CHAPv2.

- **Вопрос:** Почему данный стек протоколов считается абсолютно небезопасным сегодня?
- **Требования к анализу:** Миграция на L2TP/IPsec или современный TLS-based VPN (OpenVPN, WireGuard).

Задание №20 Криптопровайдер (СКЗИ) установлен на виртуальной машине, которая регулярно мигрирует между физическими хостами в облаке.

- **Вопрос:** В чем специфическая сложность обеспечения защиты ключей в виртуализированной среде по сравнению с физическим сервером?
- **Требования к анализу:** Риски дампа оперативной памяти (*memory dump*) и необходимость использования vTPM.

Задание №21 Установите соответствие между атакой и методом защиты: А) Brute-force — ... Б) SQL Injection — ... В) XSS — ... Г) DDoS — ...

1. Параметризованные запросы.
2. Экранирование вывода.
3. Rate Limiting / CAPTCHA.

4. Гео-балансировка трафика. (Ответ: А-3, Б-1, В-2, Г-4)

Задание №22 Расположите этапы протокола Handshake TLS 1.2 в правильном порядке: А) Проверка цепочки доверия сертификата. Б) Выбор Cipher Suite. В) Вычисление мастер-секрета. Г) Change Cipher Spec. (Ответ: Б, А, В, Г)

Задание №23 Вычислите количество возможных вариантов ключа для алгоритма AES-256. Во сколько раз пространство ключей больше, чем у AES-128? (Ответ: 2^{256} ; в 2^{128} раз больше).

Задание №24 Рассчитайте размер цифровой подписи RSA-2048 в байтах. (Ответ: 256 байт, так как $2048 \text{ бит} / 8 = 256$).

Задание №25 Определите минимальную рекомендуемую длину модуля n для RSA, обеспечивающую стойкость до 2030 года согласно актуальным рекомендациям NIST. (Ответ: 3072 бита).

Задание №26 Как изменится длина хэш-значения (в битах), если перейти от алгоритма SHA-256 к SHA-512? (Ответ: Увеличится с 256 до 512 бит).

Задание №27 Сколько раундов преобразования выполняет алгоритм AES при использовании ключа длиной 192 бита? (Ответ: 12 раундов).

Задание №28 Какой длины будет имитовставка (MAC), вычисленная по алгоритму HMAC-SHA1? (Ответ: 160 бит / 20 байт, равна длине блока хэша SHA-1).

Задание №29 Если вероятность взлома (P) равна 0.05, а ущерб (L) составляет 10 млн рублей, какова величина среднегодового ущерба (ALE — *Annual Loss Expectancy*)? (Ответ: $ALE = P \times L = 500,000$ рублей).

Задание №30 В асимметричной системе у Алисы есть пара $(Pub_A, Priv_A)$, у Боба — $(Pub_B, Priv_B)$. Чтобы отправить Бобу конфиденциальное сообщение, чьим ключом Алиса должна зашифровать текст, а чьим — подписать его? (Ответ: Зашифровать открытым ключом Боба (Pub_B), подписать закрытым ключом Алисы ($Priv_A$)).

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

Разработчик

Инжиева Д.М.

Согласовано

Заведующий кафедрой

_____ Моторина Д.В.

