

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Узунов Федор Владимирович

Должность: Ректор

Дата подписания: 30.09.2026 08:54:44

Уникальный программный ключ:

fd935d10451b860e912264c037878448452bfdb603f94388008e29877a6bcbf5

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

«УНИВЕРСИТЕТ ЭКОНОМИКИ И УПРАВЛЕНИЯ»

Факультет экономики, управления и юриспруденции

Кафедра управления и бизнес-информатики



УТВЕРЖДАЮ

Проректор по учебно-методической работе

Г.П. Узунова / Г.П. Узунова

«02» февраля 2026 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

Направление подготовки

10.03.01 «Информационная безопасность»

Профиль

Безопасность компьютерных систем

Квалификация выпускника: бакалавр

Для всех
форм обучения

Симферополь, 2026 г.

1. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

Средства оценивания в ходе текущего контроля:

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

Коды компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения по дисциплине
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности соответствующих проектных решений	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. Определение криптографического протокола. Основные отличия от простых алгоритмов шифрования (роль участников, последовательность шагов, цели).
2. Свойства безопасности криптографических протоколов: аутентификация, конфиденциальность, целостность, неотказуемость, свежесть (*freshness*) и живучесть (*liveness*).
3. Понятие противника в формальных моделях (*Dolev-Yao*, вычислительная модель). Возможности злоумышленника по перехвату, модификации и подмене сообщений.
4. Атаки на протоколы повторного использования (*replay attacks*). Механизмы обеспечения «свежести» сообщений: временные метки, случайные числа (*nonces*), счетчики вызовов.
5. Протокол «Широковещательная передача с отказом от авторства» (*Broadcast with non-repudiation*): проблема отсутствия доверия между участниками и пути ее решения.
6. Различие между криптографической примитивой (например, AES) и протоколом (например, TLS). Примеры их взаимодействия.
7. Понятие доказуемой безопасности (*provable security*) в теории протоколов. Редукция к сложной математической задаче.
8. Формальная верификация протоколов: роль инструментов типа ProVerif или Tamarin для поиска логических ошибок до реализации.
9. Протокол Диффи — Хеллмана (*Diffie-Hellman*, DH) в конечном поле: алгоритм вычисления общего секрета, уязвимость к атаке «человек посередине» (*MitM*).
10. Протокол MQV (Menezes–Qu–Vanstone) и его модификация HMQV: методы встраивания неявной аутентификации в обмен ключами Диффи — Хеллмана.
11. Схема интегрированного шифрования (*IES* — Integrated Encryption Scheme) и ECIES: объединение асимметричного согласования ключей и симметричного шифрования данных.

12. Протокол квантового распределения ключей BB84: принципы кодирования кубитов, обнаружение перехвата через возмущение состояния частиц.
13. Проблемы практической реализации квантовых сетей: доверенные промежуточные узлы (*trusted repeaters*) и ограничение дальности передачи фотонов.
14. Использование протокола Нидхема — Шрёдера как основы для построения аутентифицированных сеансов связи. Уязвимость оригинального варианта и исправление Деннинга — Сакко.
15. Протокол «Запрос-Ответ» (*Challenge-Response*) на основе симметричных алгоритмов. Проблема синхронизации состояний сторон.
16. Протокол Нидхема — Шрёдера для симметричных ключей: пошаговый разбор, использование сервера доверенных ключей (*KDC*).
17. Протокол Kerberos (версия 5): архитектура (AS, TGS, Client, Server), структура билетов (*tickets*) и аутентификаторов. Защита от атак повторного воспроизведения.
18. Протоколы аутентификации на основе паролей (*PAKE* — Password Authenticated Key Exchange): SPEKE, J-PAKE. Отличие от обычной передачи хеша пароля.
19. Взаимная аутентификация на основе асимметричной криптографии (протокол ISO/IEC 9798-3). Роль цифровых подписей в подтверждении владения закрытым ключом.
20. Протокол SIGMA (SIGn-and-MAC) как концептуальная основа для фазы рукопожатия (*Handshake*) в протоколах IPsec IKEv2 и TLS 1.3.
21. Эволюция протокола SSL 3.0 к TLS. Критические уязвимости SSL 3.0 (POODLE) и ранних версий TLS (BEAST, CRIME, Heartbleed).
22. Структура полного цикла установления соединения в TLS 1.3: переход к режиму (EC)DH(1-RTT), обязательное использование PFS (*Perfect Forward Secrecy*).
23. Обеспечение совершенной прямой секретности (*PFS*) в протоколах. Почему статический RSA в TLS 1.2 считается небезопасным при компрометации долгосрочного ключа сервера.
24. Протокол SSH версии 2: механизм обмена ключами (*Diffie-Hellman Group Exchange*), проверка подлинности хоста (*Host Keys*) и защита от внедрения вредоносных серверов.
25. Атака понижения версии (*downgrade attack*) в TLS (Logjam, FREAK). Методы защиты через жесткие политики выбора наборов шифров (*cipher suites*).
26. Протокол DTLS (*Datagram Transport Layer Security*): адаптация механизмов надежности TLS для работы поверх ненадежного транспорта UDP.
27. Протоколы безопасного многостороннего вычисления (*MPC* — Secure Multi-party Computation). Задача «Миллионеров Яо» как классический пример сравнения данных без их раскрытия.
28. Доказательства с нулевым разглашением (*Zero-Knowledge Proofs*, ZKP). Свойства полноты, корректности и нулевого разглашения. Пример протокола доказательства знания гамильтонова цикла.
29. Инфраструктура открытых ключей (*PKI*) как поддерживающая среда для протоколов. Цепочки сертификатов, кросс-сертификация и протокол проверки статуса сертификата OCSP.
30. Протоколы анонимизации трафика (*Onion Routing*, Tor): принцип многослойного («луковичного») шифрования, роль входных, промежуточных и выходных узлов, угрозы деанонимизации.

1.2 Темы рефератов:

1. Протокол Нидхема — Шрёдера: история создания, логическая структура и критический анализ уязвимостей (атака Деннинга — Сакко).

2. Протокол Kerberos v5: архитектура доверенной третьей стороны, жизненный цикл билетов (*TGT*, сервисные билеты) и защита от атак повторного воспроизведения в корпоративных сетях.
3. Сравнительный анализ протоколов «Запрос-Ответ» (*Challenge-Response*): реализация на основе симметричных MAC-кодов против асимметричных цифровых подписей.
4. Протокол Диффи — Хеллмана (*DH*) над эллиптическими кривыми (*ECDH*): математические основы, преимущества в производительности и роль в современных стандартах связи.
5. Интегрированные схемы шифрования (*IES/ECIES*): гибридный подход к передаче данных, объединяющий *ECC* для согласования ключей и блочные шифры для защиты полезной нагрузки.
6. Анализ атаки «человек посередине» (*Man-in-the-Middle*) на неаутентифицированный обмен ключами и методы ее предотвращения через предварительно распределенные секреты (*PPK*).
7. Эволюция протокола TLS: от SSL 3.0 до TLS 1.3. Устранение уязвимостей (*POODLE*, *BEAST*, *Logjam*) и переход к архитектуре с минимизацией задержек (*Zero-RTT*).
8. Обеспечение совершенной прямой секретности (*PFS*) в интернет-протоколах: сравнение механизмов обмена ключами *RSA vs (EC)DHE* и их влияние на долгосрочную безопасность переписки.
9. Протокол *IKEv2/IPsec*: механизмы взаимной аутентификации сторон, создание защищенных ассоциаций (*SA*) и применение в технологиях построения корпоративных *VPN*.
10. Архитектура безопасности протокола *SSH* версии 2: алгоритм обмена ключами *Diffie-Hellman Group Exchange*, проверка подлинности хоста и защита от подмены серверных ключей.
11. Протокол *DTLS (Datagram Transport Layer Security)*: проблемы обеспечения надежности при работе поверх *UDP* и механизмы защиты от *DoS*-атак на этапе рукопожатия (*Cookie Extension*).
12. Анализ безопасности расширений TLS: риски использования расширения *SNI (Server Name Indication)* для утечки метаданных о посещаемых ресурсах и методы их сокрытия (*ESNI/ECH*).
13. Инфраструктура открытых ключей (*PKI*): протокол проверки статуса сертификатов *OCSF* и *OCSF Stapling*. Проблемы конфиденциальности и отказоустойчивости централизованных центров сертификации.
14. Протоколы аутентификации на основе паролей (*PAKE*): алгоритмы *SPEKE* и *J-PAKE*. Защита от офлайн-словарных атак при использовании слабых пользовательских паролей.
15. Беспарольная аутентификация с использованием протокола *FIDO2 (WebAuthn)*: роль открытого ключа как фактора доступа и архитектура взаимодействия клиента, сервера и аутентификатора.
16. Криптографические протоколы электронного голосования: требования анонимности, проверяемости и неотказуемости. Сравнение систем типа *Helios* и протоколов на основе слепых подписей.
17. Протоколы безопасного подбрасывания монеты (*Coin Tossing*) и генерации общих случайных битов по недоверенным каналам связи.
18. Доказательства с нулевым разглашением (*ZKP*): протокол доказательства знания гамильтонова цикла. Применение *zk-SNARKs* в криптовалютах (например, *Zcash*) для приватных транзакций.

19. Протоколы безопасного многостороннего вычисления (MPC): классическая задача «Миллионеров Яо» и современные практические применения (совместный анализ медицинских данных без их раскрытия).
20. Постквантовые криптографические протоколы: миграция ключевых этапов обмена (Key Encapsulation Mechanisms, например, Kyber) в существующие протоколы TLS и SSH для защиты от квантовых компьютеров.
21. Протоколы конфиденциального машинного обучения (Privacy-Preserving ML): использование гомоморфного шифрования и MPC для обработки нейросетями зашифрованных данных пользователей.
22. Атаки понижения версии (Downgrade Attacks) и несоответствия параметров (Cross-Protocol Attacks): ретроспективный анализ атак DROWN и SLOTH на согласование протоколов.
23. Протоколы анонимизации трафика (Onion Routing / Tor): механизм многослойного («луковичного») шифрования, угрозы деанонимизации через подтверждение трафика (traffic confirmation attacks).
24. Симметричное шифрование в протоколах поиска по зашифрованным данным (Searchable Encryption): модель злоумышленника HBC (Honest-but-Curious) и сохранение конфиденциальности поискового запроса.
25. Формальная верификация криптографических протоколов: использование методов ВАН-логики и инструментов автоматизированного анализа (ProVerif, Tamarin) для доказательства свойств безопасности перед внедрением.

1.3 Тестовые задания

1. **В чем заключается принципиальное отличие криптографического протокола от одиночного алгоритма шифрования (например, AES)?** а) Протокол всегда работает быстрее алгоритма. б) Протокол описывает последовательность действий и обмен сообщениями между двумя и более сторонами для достижения общей цели безопасности. в) Алгоритм требует наличия секретного ключа, а протокол — нет. г) Протоколы используются только в квантовой криптографии. *Правильный ответ: б*
2. **Какова основная цель использования случайных чисел (nonces) или временных меток в криптографических протоколах?** а) Увеличение скорости вычисления общего ключа. б) Обеспечение «свежести» сообщения и защита от атак повторного воспроизведения (replay attacks). в) Замена асимметричного шифрования симметричным. г) Соккрытие IP-адреса отправителя. *Правильный ответ: б*
3. **Протокол Диффи — Хеллмана (DH) без дополнительных механизмов аутентификации уязвим к атаке...** а) Полного перебора (brute force) б) Атаки по словарю в) «Человек посередине» (Man-in-the-Middle) г) Атаки на коллизии хеш-функции *Правильный ответ: в*
4. **В архитектуре протокола Kerberos 5 доверенная третья сторона, выдающая билеты пользователю для получения доступа к конкретным сервисам, называется...** а) AS (Authentication Server) б) TGS (Ticket Granting Server) в) KDC (Key Distribution Center) г) CA (Certificate Authority) *Правильный ответ: б (Примечание: KDC — это общее название всей системы, состоящей из AS и TGS, но именно TGS выдает сервисные билеты).*
5. **Что обеспечивает свойство совершенной прямой секретности (Perfect Forward Secrecy, PFS) в протоколе TLS?** а) Невозможность расшифровать записанный ранее трафик при компрометации долгосрочного закрытого ключа сервера. б) Защиту от изменения данных злоумышленником во время передачи. в) Ускорение процесса установки соединения за счет отсутствия проверки сертификатов. г) Возможность восстановления сессии после обрыва связи без нового рукопожатия. *Правильный ответ: а*
6. **Какой механизм обмена ключами в TLS 1.3 гарантирует наличие PFS по умолчанию, в отличие от классического обмена на основе RSA в TLS 1.2?** а)

Статический RSA б) Анонимный Diffie-Hellman в) (EC)DHE (Diffie-Hellman Ephemeral) г) Pre-Shared Keys (PSK) без DH *Правильный ответ: в*

7. Атака Logjam была направлена на принудительное снижение версии протокола до «экспортного» уровня стойкости. Как называется этот класс атак? а) Side-channel attack б) Downgrade attack (атака понижения версии) в) Padding oracle attack г) Birthday attack *Правильный ответ: б*

8. В протоколе безопасного удаленного входа SSH проверка подлинности сервера (Host Authentication) критически важна для предотвращения... а) Перегрузки процессора сервера б) Внедрения злоумышленника под видом легитимного сервера с целью перехвата паролей пользователя в) Истечения срока действия пользовательского сертификата г) Снижения скорости интернет-соединения *Правильный ответ: б*

9. Какую фундаментальную проблему решает инфраструктура открытых ключей (PKI) в контексте протоколов? а) Распределение симметричных ключей между всеми пользователями сети. б) Проблема аутентификации открытого ключа субъекта (связь ключа с реальной личностью/доменом). в) Вычисление дискретного логарифма за полиномиальное время. г) Шифрование больших объемов данных без использования сессионных ключей. *Правильный ответ: б*

10. Чем протокол DTLS (Datagram Transport Layer Security) принципиально отличается от TLS при работе поверх UDP? а) Он не использует шифрование. б) Он добавляет порядковые номера сообщений для защиты от потери пакетов, дубликатов и переупорядочивания. в) Он передает ключи в открытом виде для ускорения работы. г) Он поддерживает только алгоритм ГОСТ 28147-89. *Правильный ответ: б*

11. В BAN-логике (формальной модели анализа протоколов) символ $\$P \equiv X\$$ означает... а) Субъект $\$P\$$ обладает полномочиями на чтение $\$X\$$. б) Субъект $\$P\$$ верит (убежден), что высказывание $\$X\$$ истинно. в) Сообщение $\$X\$$ зашифровано ключом $\$P\$$. г) Формула $\$X\$$ является математическим тождеством. *Правильный ответ: б*

12. Основная особенность протоколов PAKE (Password Authenticated Key Exchange), таких как SPEKE или J-PAKE, заключается в том, что они... а) Позволяют использовать короткие пароли, защищаясь при этом от офлайн-словарных атак. б) Требуют обязательной биометрической идентификации перед началом обмена. в) Работают исключительно в квантовых сетях. г) Не используют никаких математических преобразований над паролем. *Правильный ответ: а*

13. Суть атаки Bleichenbacher на SSL/TLS заключалась в эксплуатации некорректной обработки ошибок заполнения (padding) в режиме PKCS#1 v1.5, что позволяло проводить... а) Отказ в обслуживании (DoS) б) Оракульную атаку для постепенного восстановления закрытого ключа RSA в) Подмену DNS-записей г) Заражение сервера вредоносным кодом через картинку *Правильный ответ: б*

14. Какое расширение TLS отвечает за передачу доменного имени сервера в процессе установления соединения и часто становится источником утечки метаданных? а) ALPN б) SNI (Server Name Indication) в) Heartbeat г) Session Ticket *Правильный ответ: б*

15. В протоколах конфиденциального машинного обучения (Privacy-Preserving ML) использование гомоморфного шифрования позволяет... а) Обучать нейросеть без использования размеченных данных. б) Выполнять вычисления непосредственно над зашифрованными данными без их предварительного расшифрования. в) Уменьшить размер обучающей выборки в 10 раз. г) Гарантировать 100% точность предсказания модели. *Правильный ответ: б*

16. Для защиты криптографического протокола от атак повторного воспроизведения (replay attacks) каждое новое сообщение должно содержать уникальный одноразовый параметр, называемый _____ (случайное число) или временную метку. *(Правильный ответ: нонс / nonce)*

17. В протоколе Kerberos 5 сервер аутентификации (AS) выдает пользователю специальный билет для получения доступа к другим сервисам, который называется _____ (аббревиатура TGT). *(Правильный ответ: Ticket-Granting Ticket / Билет на получение билетов)*
18. Протокол Диффи — Хеллмана без использования дополнительных механизмов цифровой подписи или обмена сертификатами уязвим к классической атаке «_____ посередине». *(Правильный ответ: человек / man)*
19. Свойство протокола TLS, гарантирующее, что компрометация долгосрочного закрытого ключа сервера не позволит расшифровать ранее записанный сетевой трафик, называется совершенной _____ секретностью (PFS). *(Правильный ответ: прямой / forward)*
20. В отличие от классического RSA, современные безопасные обмены ключами в TLS 1.3 используют эфемерные параметры Диффи — Хеллмана (обозначаются буквой ____ в аббревиатуре DHE/ECDHE), которые удаляются из памяти сразу после завершения сессии. *(Правильный ответ: E / Ephemeral / эфемерный)*
21. Инфраструктура открытых ключей (PKI) решает проблему доверия к открытому ключу с помощью цифровых сертификатов стандарта X.509, которые выдаются и подписываются доверенной третьей стороной — Центром _____. *(Правильный ответ: сертификации / CA)*
22. В формальной логике BAN (Burrows-Abadi-Needham), используемой для верификации протоколов, символ $\$ \equiv \$$ читается как «_____» (например, $\$P \equiv X\$$ означает, что субъект P верит в истинность X). *(Правильный ответ: верит / believes)*
23. Протокол безопасного удаленного доступа SSH использует механизм Host Keys для предотвращения подмены сервера. При первом подключении пользователь проверяет отпечаток (_____) ключа сервера вручную. *(Правильный ответ: fingerprint / отпечаток)*
24. Протоколы класса PAKE (Password Authenticated Key Exchange), такие как SPEKE, позволяют сторонам доказать знание общего пароля и выработать общий ключ, при этом защищаясь от _____ словарных атак злоумышленника. *(Правильный ответ: офлайн / offline)*
25. Технология доказательства с нулевым разглашением (Zero-Knowledge Proof, ZKP) позволяет одной стороне подтвердить истинность утверждения другой стороне, не передавая ей никакой информации, кроме самого факта _____. *(Правильный ответ: истинности / знания)*
26. **Установите соответствие между криптографическим протоколом и его основной целью**

Протокол	Основная цель
1. Diffie-Hellman (DH / ECDH)	А. Получение доступа к сетевым ресурсам через доверенную третью сторону с использованием «билетов».
2. Kerberos	Б. Согласование общего секретного ключа по незащищенному каналу без его прямой передачи.
3. TLS Handshake	В. Обеспечение анонимности пользователя и защита трафика от анализа на уровне сети Интернет.
4. Tor (Onion Routing)	Г. Создание защищенного канала связи поверх транспортного протокола (TCP/TLS Record Layer).

27. **Установите соответствие между уязвимостью/атакой и затронутым протоколом или механизмом**

Уязвимость / Атака	Затронутый протокол / Механизм
1. POODLE	А. Протокол SSH; компрометация сервера путем внедрения вредоносного кода в библиотеку сжатия памяти (<i>memory corruption</i>).
2. Heartbleed	Б. Протокол SSL 3.0; атака типа <i>padding oracle</i> , позволяющая извлекать данные из зашифрованных куки.
3. Logjam	В. Библиотека OpenSSL; утечка оперативной памяти сервера через некорректную реализацию расширения Heartbeat.
4. Terrapin	Г. Протоколы семейства Диффи — Хеллмана; принудительное снижение стойкости до «экспортной» (512 бит) для взлома $g^a \bmod p$.

Правильные ответы: 1–Б, 2–В, 3–Г, 4–А. (Примечание: Террапин — это атака на канал управления SSHv2 через манипуляции с порядком пакетов при рукопожатии).

28. Задание 3. Установите соответствие между компонентом инфраструктуры PKI и его описанием

Компонент	Описание
1. CA (Certificate Authority)	А. Локальное хранилище компьютера, содержащее корневые сертификаты организаций, которым безусловно доверяет система.
2. RA (Registration Authority)	Б. Удостоверяющий центр, который проверяет личность заявителя и ставит свою цифровую подпись на выпущенный сертификат.
3. Trust Store	В. Сетевой протокол для проверки статуса отзыва цифрового сертификата в режиме реального времени.
4. OCSP	Г. Регистрационный орган, принимающий заявки на выпуск сертификатов и проводящий первичную идентификацию пользователей перед передачей запроса в ЦС.

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

29. Установите соответствие между формальной нотацией BAN-логики и ее смыслом

Нотация	Смысл
1. $SP \equiv X$	А. Субъект SP обладает сообщением X (видел его, может читать, если оно не зашифровано, или расшифровал).
2. $SP \rightarrow X$	Б. Сообщение X является свежим (не является повтором старого сообщения).
3. $SP \triangleleft X$	В. Субъект SP верит (убежден), что утверждение X истинно.
4. $\sharp(X)$	Г. Субъект SP имеет юрисдикцию (полномочия) над утверждением X и ему можно доверять в этом вопросе.

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

30. Установите соответствие между типом протокола аутентификации и используемым фактором/секретом

Тип протокола	Используемый фактор / Секрет
1. PAKE (SPEKE, J-	А. Асимметричная пара ключей; подтверждение владения

Тип протокола	Используемый фактор / Секрет
PAKE)	закрытым ключом через цифровую подпись challenge-ответа.
2. FIDO2 / WebAuthn	Б. Низкоэнтропийный человеческий пароль, преобразуемый в точку эллиптической кривой или базу для обмена DH.
3. ISO/IEC 9798-3	В. Специализированный аппаратный токен (USB/NFC), требующий физического присутствия пользователя.
4. NTLM / Kerberos (классический)	Г. Симметричный секрет (хеш пароля), разделяемый пользователем и контроллером домена (KDC).

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

1.4 Практические задания

Задание 1. Дайте определение криптографического протокола. Перечислите не менее пяти целей безопасности (свойств), которые протокол должен обеспечивать одновременно.

Задание 2. Опишите модель противника Долева — Яо (*Dolev-Yao*). Какие три основные операции злоумышленник может выполнять с сообщениями в канале связи?

Задание 3. В чем заключается атака повторного воспроизведения (*replay attack*)? Предложите два различных механизма обеспечения «свежести» (*freshness*) сообщений для защиты от нее.

Задание 4. Сравните синхронные и асинхронные протоколы аутентификации. Какая проблема возникает в чисто симметричных синхронных системах при рассинхронизации счетчиков вызовов?

Задание 5. Что такое оракульная атака (*oracle attack*)? Приведите пример атаки *padding oracle*, объяснив, какую информацию о закрытом тексте выдает «оракул».

Задание 6. Изобразите диаграмму сообщений классического протокола Диффи — Хеллмана (DH). Покажите математически, как вычисляется общий секрет Z , если известны открытые параметры (p, g) и закрытые экспоненты (a, b) .

Задание 7. Объясните уязвимость базового протокола DH к атаке «человек посередине». Каким образом использование цифровых подписей или протокола STS (Station-to-Station) устраняет эту угрозу?

Задание 8. Опишите алгоритм работы сервера распределения ключей Керберос (*Kerberos KDC*). В чем разница между билетом на получение билетов (*TGT*) и сервисным билетом?

Задание 9. Проведите сравнительный анализ протоколов Нидхема — Шрёдера (симметричный вариант) и Отвея — Риса. Укажите на критическую ошибку в сообщении №4 оригинального протокола Нидхема — Шрёдера.

Задание 10. Квантовое распределение ключей (*QKD*): опишите принцип кодирования информации в поляризации фотонов по протоколу BB84. Почему сам факт измерения кубита злоумышленником приводит к обнаружению слежки?

Задание 11. Постройте пошаговую схему полного цикла установления соединения (*Full Handshake*) в TLS 1.3. Выделите этапы, обеспечивающие совершенную прямую секретность (*PFS*).

Задание 12. Объясните, почему использование статического ключа RSA для обмена сессионными ключами в TLS 1.2 нарушает свойство PFS. Какой механизм пришел ему на смену в TLS 1.3?

Задание 13. Атака Logjam основана на принудительном снижении параметров группы Диффи — Хеллмана до экспортной стойкости (512 бит). Опишите процесс «предвычисления», который позволяет злоумышленнику взломать такой обмен за короткое время.

Задание 14. Сравните архитектуру защищенного канала в IPsec/IKEv2 и TLS. На каком сетевом уровне работает каждый из них и как это влияет на прозрачность приложений?

Задание 15. Протокол SSH версии 2 использует два независимых этапа: проверка подлинности сервера (*Host Authentication*) и проверка подлинности пользователя. Чем опасен пропуск первого этапа (принятие нового неизвестного ключа хоста)?

Задание 16. Опишите работу расширения *SNI* (*Server Name Indication*) в TLS. Какие риски приватности оно несет и какие технологии (*ECH*) призваны их решить?

Задание 17. Инфраструктура открытых ключей (*PKI*): постройте цепочку доверия от конечного сертификата веб-сайта до корневого удостоверяющего центра (*Root CA*). Что произойдет, если промежуточный *CA* будет скомпрометирован?

Задание 18. Опишите протокол проверки статуса сертификата *OCSP*. В чем его недостаток с точки зрения приватности и как расширение *OCSP Stapling* решает эту проблему?

Задание 19. Протоколы *PAKE* (*Password Authenticated Key Exchange*): объясните принцип работы *SPAKE*. Как именно слабый пароль преобразуется в элемент группы для выполнения обмена *DH*?

Задание 20. Беспарольная аутентификация *FIDO2/WebAuthn*: опишите роль «Апплета-аутентификатора» (например, *USB-токена*) в процессе генерации пары ключей для конкретного домена сайта.

Задание 21. Электронное голосование: сформулируйте противоречие между свойствами анонимности избирателя и проверяемости (верифицируемости) результата. Как протоколы на основе слепых подписей решают задачу тайного голосования?

Задание 22. Доказательства с нулевым разглашением (*ZKP*): приведите классический пример задачи «Миллионеры Яо». Как один миллионер может доказать другому, что он богаче, не называя точную сумму своего состояния?

Задание 23. Безопасное многостороннее вычисление (*MPC*): объясните концепцию разделения секрета (*Secret Sharing*) на примере сложения чисел трех участников без раскрытия исходных значений каждому из них.

Задание 24. BAN-логика: расшифруйте нотацию
$$\frac{P \equiv P \stackrel{K}{\leftrightarrow} Q, P \triangleleft \{X\}_K}{P \equiv Q \sim X}$$
 словами. Какое логическое умозаключение делает субъект *P*?

Задание 25. Атака *Bleichenbacher'98* на *SSL/TLS* (ошибка заполнения *PKCS#1 v1.5*). Как злоумышленник, выступая в роли оракула, может восстановить зашифрованный сеансовый ключ, просто получая ответы сервера «да/нет» на корректность *padding*?

Задание 26. Формальная верификация: в чем преимущество инструментов типа *ProVerif* перед ручной проверкой кода протокола? Какую типичную логическую ошибку («атаку отражения») они находят автоматически?

Задание 27. Протокол *Signal* (*Double Ratchet*): объясните концепцию «плавающего» корня доверия и двойного храповика (*ratchet*). Почему этот протокол обеспечивает высокую степень прямой секретности даже при длительном компрометации устройства?

Задание 28. Постквантовые протоколы: опишите идею алгоритма согласования ключей *Kyber*. На какой сложной математической задаче (в решетках) строится его стойкость против квантовых компьютеров?

Задание 29. Составьте таблицу сравнения режимов рукопожатия (*Handshake Modes*) в *TLS 1.3*:

- Full 1-RTT;
- Resumption via *PSK* (*Session Ticket*);
- Zero Round-Trip (0-RTT). Укажите главный риск использования режима 0-RTT.

Задание 30. Разработайте упрощенный протокол аутентификации для системы «Умный дом» (датчик температуры -> контроллер), где датчик имеет крайне ограниченные вычислительные ресурсы и питание от батарейки. Обоснуйте выбор симметричных *MAC*-кодов вместо асимметричной подписи.

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 и аудиторных работ, 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 практических и 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	отлично

	объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы. 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 зачета;
- тестовые задания к зачету.

Коды компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения по дисциплине
------------------	--------------------------	---

ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности соответствующих проектных решений	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 зачету

1. Определение криптографического протокола. Основные отличия от простых алгоритмов шифрования (роль участников, последовательность шагов, цели).
2. Свойства безопасности криптографических протоколов: аутентификация, конфиденциальность, целостность, неотказуемость, свежесть (*freshness*) и живучесть (*liveness*).
3. Понятие противника в формальных моделях (*Dolev-Yao*, вычислительная модель). Возможности злоумышленника по перехвату, модификации и подмене сообщений.
4. Атаки на протоколы повторного использования (*replay attacks*). Механизмы обеспечения «свежести» сообщений: временные метки, случайные числа (*nonces*), счетчики вызовов.
5. Протокол «Широковещательная передача с отказом от авторства» (*Broadcast with non-repudiation*): проблема отсутствия доверия между участниками и пути ее решения.
6. Различие между криптографической примитивой (например, AES) и протоколом (например, TLS). Примеры их взаимодействия.
7. Понятие доказуемой безопасности (*provable security*) в теории протоколов. Редукция к сложной математической задаче.
8. Формальная верификация протоколов: роль инструментов типа ProVerif или Tamarin для поиска логических ошибок до реализации.
9. Протокол Диффи — Хеллмана (*Diffie-Hellman*, DH) в конечном поле: алгоритм вычисления общего секрета, уязвимость к атаке «человек посередине» (*MitM*).
10. Протокол MQV (Menezes–Qu–Vanstone) и его модификация HMQV: методы встраивания неявной аутентификации в обмен ключами Диффи — Хеллмана.
11. Схема интегрированного шифрования (*IES* — Integrated Encryption Scheme) и ECIES: объединение асимметричного согласования ключей и симметричного шифрования данных.
12. Протокол квантового распределения ключей BB84: принципы кодирования кубитов, обнаружение перехвата через возмущение состояния частиц.
13. Проблемы практической реализации квантовых сетей: доверенные промежуточные узлы (*trusted repeaters*) и ограничение дальности передачи фотонов.
14. Использование протокола Нидхем — Шрёдера как основы для построения аутентифицированных сеансов связи. Уязвимость оригинального варианта и исправление Деннинга — Сакко.
15. Протокол «Запрос-Ответ» (*Challenge-Response*) на основе симметричных алгоритмов. Проблема синхронизации состояний сторон.
16. Протокол Нидхем — Шрёдера для симметричных ключей: пошаговый разбор, использование сервера доверенных ключей (*KDC*).
17. Протокол Kerberos (версия 5): архитектура (AS, TGS, Client, Server), структура билетов (*tickets*) и аутентификаторов. Защита от атак повторного воспроизведения.

18. Протоколы аутентификации на основе паролей (*PAKE* — Password Authenticated Key Exchange): *SPEKE*, *J-PAKE*. Отличие от обычной передачи хеша пароля.
19. Взаимная аутентификация на основе асимметричной криптографии (протокол *ISO/IEC 9798-3*). Роль цифровых подписей в подтверждении владения закрытым ключом.
20. Протокол *SIGMA* (*SIGn-and-MAC*) как концептуальная основа для фазы рукопожатия (*Handshake*) в протоколах *IPsec IKEv2* и *TLS 1.3*.
21. Эволюция протокола *SSL 3.0* к *TLS*. Критические уязвимости *SSL 3.0* (*POODLE*) и ранних версий *TLS* (*BEAST*, *CRIME*, *Heartbleed*).
22. Структура полного цикла установления соединения в *TLS 1.3*: переход к режиму (*EC*)*DH*(1-*RTT*), обязательное использование *PFS* (*Perfect Forward Secrecy*).
23. Обеспечение совершенной прямой секретности (*PFS*) в протоколах. Почему статический *RSA* в *TLS 1.2* считается небезопасным при компрометации долгосрочного ключа сервера.
24. Протокол *SSH* версии 2: механизм обмена ключами (*Diffie-Hellman Group Exchange*), проверка подлинности хоста (*Host Keys*) и защита от внедрения вредоносных серверов.
25. Атака понижения версии (*downgrade attack*) в *TLS* (*Logjam*, *FREAK*). Методы защиты через жесткие политики выбора наборов шифров (*cipher suites*).
26. Протокол *DTLS* (*Datagram Transport Layer Security*): адаптация механизмов надежности *TLS* для работы поверх ненадежного транспорта *UDP*.
27. Протоколы безопасного многостороннего вычисления (*MPC* — Secure Multi-party Computation). Задача «Миллионеров Йо» как классический пример сравнения данных без их раскрытия.
28. Доказательства с нулевым разглашением (*Zero-Knowledge Proofs*, *ZKP*). Свойства полноты, корректности и нулевого разглашения. Пример протокола доказательства знания гамильтонова цикла.
29. Инфраструктура открытых ключей (*PKI*) как поддерживающая среда для протоколов. Цепочки сертификатов, кросс-сертификация и протокол проверки статуса сертификата *OCSP*.
30. Протоколы анонимизации трафика (*Onion Routing*, *Tor*): принцип многослойного («луковичного») шифрования, роль входных, промежуточных и выходных узлов, угрозы деанонимизации.

3.2. Задания для зачета:

Задание 1. Дайте определение криптографического протокола. Перечислите не менее пяти целей безопасности (свойств), которые протокол должен обеспечивать одновременно.

Задание 2. Опишите модель противника Долева — Йо (*Dolev-Yao*). Какие три основные операции злоумышленник может выполнять с сообщениями в канале связи?

Задание 3. В чем заключается атака повторного воспроизведения (*replay attack*)? Предложите два различных механизма обеспечения «свежести» (*freshness*) сообщений для защиты от нее.

Задание 4. Сравните синхронные и асинхронные протоколы аутентификации. Какая проблема возникает в чисто симметричных синхронных системах при рассинхронизации счетчиков вызовов?

Задание 5. Что такое оракульная атака (*oracle attack*)? Приведите пример атаки *padding oracle*, объяснив, какую информацию о закрытом тексте выдает «оракул».

Задание 6. Изобразите диаграмму сообщений классического протокола Диффи — Хеллмана (*DH*). Покажите математически, как вычисляется общий секрет ZZ , если известны открытые параметры (p, g) и закрытые экспоненты (a, b) .

Задание 7. Объясните уязвимость базового протокола DH к атаке «человек посередине». Каким образом использование цифровых подписей или протокола STS (Station-to-Station) устраняет эту угрозу?

Задание 8. Опишите алгоритм работы сервера распределения ключей Керберос (*Kerberos KDC*). В чем разница между билетом на получение билетов (*TGT*) и сервисным билетом?

Задание 9. Проведите сравнительный анализ протоколов Нидхема — Шрёдера (симметричный вариант) и Отвея — Риса. Укажите на критическую ошибку в сообщении №4 оригинального протокола Нидхема — Шрёдера.

Задание 10. Квантовое распределение ключей (*QKD*): опишите принцип кодирования информации в поляризации фотонов по протоколу BB84. Почему сам факт измерения кубита злоумышленником приводит к обнаружению слежки?

Задание 11. Постройте пошаговую схему полного цикла установления соединения (*Full Handshake*) в TLS 1.3. Выделите этапы, обеспечивающие совершенную прямую секретность (*PFS*).

Задание 12. Объясните, почему использование статического ключа RSA для обмена сессионными ключами в TLS 1.2 нарушает свойство PFS. Какой механизм пришел ему на смену в TLS 1.3?

Задание 13. Атака Logjam основана на принудительном снижении параметров группы Диффи — Хеллмана до экспортной стойкости (512 бит). Опишите процесс «предвычисления», который позволяет злоумышленнику взломать такой обмен за короткое время.

Задание 14. Сравните архитектуру защищенного канала в IPsec/IKEv2 и TLS. На каком сетевом уровне работает каждый из них и как это влияет на прозрачность приложений?

Задание 15. Протокол SSH версии 2 использует два независимых этапа: проверка подлинности сервера (*Host Authentication*) и проверка подлинности пользователя. Чем опасен пропуск первого этапа (принятие нового неизвестного ключа хоста)?

Задание 16. Опишите работу расширения SNI (*Server Name Indication*) в TLS. Какие риски приватности оно несет и какие технологии (*ECH*) призваны их решить?

Задание 17. Инфраструктура открытых ключей (*PKI*): постройте цепочку доверия от конечного сертификата веб-сайта до корневого удостоверяющего центра (*Root CA*). Что произойдет, если промежуточный CA будет скомпрометирован?

Задание 18. Опишите протокол проверки статуса сертификата OCSP. В чем его недостаток с точки зрения приватности и как расширение OCSP Stapling решает эту проблему?

Задание 19. Протоколы PAKE (*Password Authenticated Key Exchange*): объясните принцип работы SPEKE. Как именно слабый пароль преобразуется в элемент группы для выполнения обмена DH?

Задание 20. Беспарольная аутентификация FIDO2/WebAuthn: опишите роль «Апплета-аутентификатора» (например, USB-токена) в процессе генерации пары ключей для конкретного домена сайта.

Задание 21. Электронное голосование: сформулируйте противоречие между свойствами анонимности избирателя и проверяемости (верифицируемости) результата. Как протоколы на основе слепых подписей решают задачу тайного голосования?

Задание 22. Доказательства с нулевым разглашением (*ZKP*): приведите классический пример задачи «Миллионеры Яо». Как один миллионер может доказать другому, что он богаче, не называя точную сумму своего состояния?

Задание 23. Безопасное многостороннее вычисление (*MPC*): объясните концепцию разделения секрета (*Secret Sharing*) на примере сложения чисел трех участников без раскрытия исходных значений каждому из них.

Задание 24. ВАН-логика: расшифруйте нотацию логическое умозаключение делает субъект P?

$$\frac{P \equiv P \stackrel{K}{\leftrightarrow} Q, P \triangleleft \{X\}_K}{P \equiv Q \sim X}$$

словами. Какое

Задание 25. Атака Bleichenbacher'98 на SSL/TLS (ошибка заполнения PKCS#1 v1.5). Как злоумышленник, выступая в роли оракула, может восстановить зашифрованный сеансовый ключ, просто получая ответы сервера «да/нет» на корректность *padding*?

Задание 26. Формальная верификация: в чем преимущество инструментов типа ProVerif перед ручной проверкой кода протокола? Какую типичную логическую ошибку («атаку отражения») они находят автоматически?

Задание 27. Протокол Signal (Double Ratchet): объясните концепцию «плавающего» корня доверия и двойного храповика (*ratchet*). Почему этот протокол обеспечивает высокую степень прямой секретности даже при длительном компрометации устройства?

Задание 28. Постквантовые протоколы: опишите идею алгоритма согласования ключей Kyber. На какой сложной математической задаче (в решетках) строится его стойкость против квантовых компьютеров?

Задание 29. Составьте таблицу сравнения режимов рукопожатия (*Handshake Modes*) в TLS 1.3:

- Full 1-RTT;
- Resumption via PSK (Session Ticket);
- Zero Round-Trip (0-RTT). Укажите главный риск использования режима 0-RTT.

Задание 30. Разработайте упрощенный протокол аутентификации для системы «Умный дом» (датчик температуры -> контроллер), где датчик имеет крайне ограниченные вычислительные ресурсы и питание от батарейки. Обоснуйте выбор симметричных MAC-кодов вместо асимметричной подписи.

4. ОСНОВНЫЕ КРИТЕРИИ ОЦЕНИВАНИЯ ПРИ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Шкала оценивания уровня сформированности универсальной компетенций (зачет с оценкой)

Формируемые уровни освоения компетенций	Критерии оценивания	Шкала оценивания
Высокий уровень	Изложено правильное понимание вопроса, четко и самостоятельно дан исчерпывающий ответ, содержание раскрыто полно, профессионально, грамотно. Обучающимся усвоена взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии. Отражает успешное и систематическое применение навыков и умений по данной дисциплине в соответствии с ФГОС.	отлично

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

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

Вид промежуточной аттестации – зачет с оценкой.

Форма проведения промежуточной аттестации – письменный зачет.