

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

fd935d10451b860e912264c037858448452b693f94388908e29877e6bbbf5

**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
ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ
ИНФОРМАЦИИ**

Направление подготовки
10.03.01 «Информационная безопасность»

Профиль
Безопасность компьютерных систем

Квалификация выпускника: бакалавр

Для всех
форм обучения

Симферополь, 2026 г.

1. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

Средства оценивания в ходе текущего контроля:

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

Код компетенции	Результаты освоения ОПОП (содержание компетенций)	Планируемые результаты освоения дисциплины
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.1. Выбирает принципы формирования политики информационной безопасности в информационных системах ОПК-10.2. Подбирает и конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности

1.1 Вопросы к текущему контролю

1. Классификация программно-аппаратных средств защиты информации (ПАЗИ). Различие между средствами общего назначения со встроенными функциями защиты и специализированными СЗИ.
2. Концепция доверенной вычислительной базы (*TCB* — *Trusted Computing Base*). Основные требования к компонентам *TCB*.
3. Монитор обращений (референс-монитор): определение, три фундаментальных свойства (необходимость, полнота, изолированность) и способы его реализации в современных ОС.
4. Уровни привилегий процессора (кольца защиты архитектуры x86: Ring 0–Ring 3). Механизмы перехода между кольцами (шлюзы вызовов).
5. Понятие «задней двери» (*backdoor*) и руткитов уровня ядра (*kernel-mode rootkits*). Методы скрытого перехвата системных функций (*SSDT/IAT hooking*).
6. Доверенная загрузка компьютера: цели, этапы (загрузчик MBR/UEFI -> ядро ОС -> службы) и механизмы контроля целостности на каждом этапе.
7. Аппаратный корень доверия (*Hardware Root of Trust*). Роль модулей TPM (*Trusted Platform Module*) и Intel Boot Guard / AMD Hardware Validated Boot в обеспечении безопасной загрузки.
8. Специализированные защищенные компьютеры и сети: понятие физического разрыва (*air gap*), однонаправленные шлюзы (*data diodes*).
9. Программно-определяемые периметры (*SDP*) и микросегментация как методы защиты облачных инфраструктур и ЦОД.
10. Средства доверенного времени: аппаратные источники точного времени и их роль в разборе инцидентов информационной безопасности (логирование, метки Kerberos).
11. Факторы аутентификации («что вы знаете», «что у вас есть», «кем вы являетесь»). Многофакторная аутентификация (*MFA*) и ее устойчивость к атакам типа *Man-in-the-Middle*.

12. Технологии биометрической идентификации. Понятия *FAR* (False Acceptance Rate) и *FRR* (False Rejection Rate). Хранение биометрических шаблонов вместо исходных данных.
13. Модель Харрисона — Руззо — Ульмана (*HRU*): формальное описание матрицы доступа, примитивные операторы и доказательство разрешимости задачи безопасности.
14. Мандатное управление доступом (*MAC*, например, модель Белла — Лападулы). Субъектные и объектные метки конфиденциальности. Свойства Simple Security (*no read up*) и - (*no write down*).
15. Избирательное (дискреционное) управление доступом (*DAC*) в файловых системах (биты прав *rwX* в Linux, списки *ACL* в Windows NTFS).
16. Ролевое управление доступом (*RBAC*) и атрибутивное управление доступом (*ABAC*). Сравнение гибкости настройки политик для крупных корпоративных систем.
17. Технология виртуализации ввода-вывода (*SR-IOV*, *GPU Passthrough*) и риски утечки данных через побочные каналы между виртуальными машинами.
18. Механизмы изоляции адресного пространства процессов. Таблицы страниц, трансляция адресов (*MMU*) и защита от переполнения буфера на уровне оборудования (*DEP/NX-bit*).
19. Технология *ASLR* (Address Space Layout Randomization). Принцип работы и методы обхода (утечка указателей, атаки типа *ROP* — Return-Oriented Programming).
20. Песочницы (*sandboxes*) и контейнеризация (*Docker*, *LXC*, *gVisor*). Различия в механизмах изоляции (*namespaces*, *cgroups* в Linux; гипервизорные песочницы).
21. Ядра безопасности повышенной надежности (*Security-Enhanced Linux* — *SELinux*, *AppArmor*). Типовая и мандатная модели доступа внутри одной ОС.
22. Обеспечение безопасного удаления информации с магнитных и твердотельных накопителей (*SSD*). Проблемы команды *TRIM*, *wear leveling* и остаточной намагниченности.
23. Аппаратная виртуализация (*Intel VT-x*, *AMD-V*). Кольцо -1: архитектура мониторов виртуальных машин (*Hypervisor Type 1 vs Type 2*) и атака «голубой пилюлей» (*Blue Pill*).
24. Смарт-карты и USB-токены (Рутокен, JaCarta). Архитектура микропроцессорной карты: чиплет, собственная ОС, файловая система, апплеты.
25. Апплетно-модульная архитектура (*Java Card*). Принципы выполнения кода внутри защищенного элемента (*Secure Element*).
26. Аппаратные модули безопасности (*HSM* — Hardware Security Modules). Требования стандарта FIPS 140-2/3 уровней безопасности. Применение в банковских системах (*PIN-блоки*) и PKI.
27. Технология исполнения кода в доверенной среде (*TEE* — Trusted Execution Environment, пример: ARM TrustZone). Разделение ресурсов процессора на «нормальный» и «защищенный» миры.
28. Защита от побочных каналов (*side-channel attacks*): анализ энергопотребления (*SPA/DPA*) и временных задержек при выполнении криптографических операций.
29. Аппаратная проверка подлинности компонентов (*Hardware Attestation*). Удаленное подтверждение конфигурации устройства перед предоставлением доступа к ресурсам.
30. Российские нормативные требования к программно-аппаратным СЗИ. Сертификация ФСТЭК России по требованиям к уровням отсутствия недекларированных возможностей (НДВ) и по профилям защиты межсетевых экранов.

1.2 Темы рефератов:

1. Концепция монитора обращений (референс-монитора) в современных операционных системах: теоретические требования, практические реализации в ядрах Linux и Windows NT, уязвимости обхода.

2. Архитектура доверенной вычислительной базы (TCB): минимизация TCB, проблема «раздувания» кода ядра и переход к микроядерным архитектурам (на примере seL4 или QNX).
3. Кольца защиты процессора (*Ring 0–3*) и механизмы перехода между уровнями привилегий: эволюция от архитектуры x86 к современным механизмам изоляции системного кода.
4. Формальные модели управления доступом: сравнительный анализ моделей Харрисона — Руззо — Ульмана (HRU) и Сазерленда для верификации политик безопасности.
5. Проблема скрытых каналов передачи информации (*covert channels*) в защищенных системах: классификация (память vs время), методы обнаружения и противодействия на уровне гипервизоров.
6. Технология UEFI Secure Boot: принципы работы криптографической цепочки доверия, управление ключами PK/KEK/db и атака «буткит».
7. Аппаратный корень доверия (*Hardware Root of Trust*): роль модулей TPM 2.0 и Intel Boot Guard в обеспечении неизменности программного обеспечения при старте платформы.
8. Системы доверенной загрузки отечественного производства: архитектура и особенности функционирования ПАК «Соболь», ViPNet SafeBoot и Аккорд-АМДЗ.
9. Атаки типа *Return-Oriented Programming (ROP)*: программно-аппаратные методы противодействия эксплуатации уязвимостей переполнения буфера (DEP, ASLR, Shadow Stack).
10. Изоляция адресного пространства процессов: реализация механизмов ASLR и DEP/NX-bit на уровне компилятора и операционной системы.
11. Аппаратные модули безопасности (HSM): архитектура, уровни безопасности по стандарту FIPS 140-3 и применение в платежных системах (банковские HSM).
12. Технология ARM TrustZone: разделение ресурсов процессора на «нормальный» (*Normal World*) и «защищенный» (*Secure World*) миры, сценарии использования в мобильных устройствах.
13. Смарт-карты и защищенные элементы (*Secure Element*): микропроцессорная архитектура, протоколы обмена данными (APDU) и использование в биометрических паспортах РФ.
14. USB-токены и смарт-карты российской разработки (Рутокен, JaCarta): функциональные возможности, встроенные апплеты электронной подписи и поддержка отечественных стандартов ГОСТ.
15. Анализ побочных каналов (*Side-Channel Attacks*): атаки по времени выполнения (*timing attacks*) и энергопотреблению (DPA/SPA) на реализацию алгоритмов AES и RSA.
16. Безопасность гипервизоров первого типа: архитектура изоляции виртуальных машин, уязвимости класса VM Escape и технология вложенной виртуализации.
17. Программно-определяемые периметры (SDP) и микросегментация: замена традиционных межсетевых экранов в облачных инфраструктурах и ЦОД.
18. Специализированные устройства предотвращения вторжений (IPS/IDS): работа сетевых сенсоров в прозрачном режиме, аппаратное ускорение анализа трафика на базе FPGA.
19. Информационная безопасность периферийных устройств ввода-вывода: атаки через интерфейсы USB, Thunderbolt и DMA (Direct Memory Access), технологии IOMMU для защиты памяти.
20. Однонаправленные шлюзы (*Data Diodes*): физическая невозможность обратной связи, применение в АСУ ТП критической инфраструктуры и оборонном секторе.

1.3 Тестовые задания

1. Какое фундаментальное свойство монитора обращений (референс-монитора) гарантирует, что его невозможно обойти при любом обращении субъекта к объекту? а) Изолированность б) Полнота медиации (Always invoked) в) Минимизация сложности г) Верифицируемость *Правильный ответ: б*
2. В архитектуре x86 уровни привилегий 0–3 называются «кольцами защиты». Где выполняется код самой защищенной части операционной системы (ядра)? а) Ring 3 б) Ring 1 в) Ring 0 г) Ring -1 *Правильный ответ: в*
3. Какой механизм аппаратной защиты памяти предотвращает выполнение кода из областей, помеченных как данные (например, стек или куча)? а) ASLR (Address Space Layout Randomization) б) DEP / NX-бит (No-eXecute bit) в) Stack Canaries г) SSP (Stack Smashing Protector) *Правильный ответ: б*
4. Технология рандомизации адресного пространства (ASLR) предназначена для защиты от... а) Перехвата сетевого трафика б) Эксплуатации уязвимостей путем перехода на заранее подготовленный shell-код в памяти в) Несанкционированного копирования файлов г) Подмены системных библиотек на диске *Правильный ответ: б*
5. Что является основным назначением модуля TPM (Trusted Platform Module) при реализации доверенной загрузки? а) Ускорение расшифрования жесткого диска б) Хранение хеш-сумм компонентов ПО и ключей для проверки целостности цепочки загрузки в) Фильтрация вредоносного трафика до загрузки ОС г) Генерация паролей пользователя *Правильный ответ: б*
6. В модели Белла — Лападулы (мандатное управление доступом) какое правило запрещает субъекту с уровнем доступа «Конфиденциально» читать документ уровня «Совершенно секретно»? а) Simple Security Property (no read up) б) *-Property (no write down) в) Дискреционное правило ACL г) Свойство транзитивности *Правильный ответ: а*
7. Какая технология позволяет изолировать приложения друг от друга и от основной ОС, используя общее ядро хоста, но отдельное пространство процессов и имен? а) Полная виртуализация (Type 1 Hypervisor) б) Эмуляция оборудования в) Контейнеризация (Docker, LXC) г) Кольца защиты процессора *Правильный ответ: в*
8. Атака типа VM Escape («побег из виртуальной машины») означает... а) Выключение питания физического сервера б) Прорыв изоляции между гостевой ОС и хостовой системой через уязвимости гипервизора в) Удаленное отключение виртуальной машины администратором г) Копирование образа виртуального диска *Правильный ответ: б*
9. Для чего предназначен стандарт FIPS 140-3 в контексте программно-аппаратных СЗИ? а) Определение скорости шифрования алгоритма AES б) Установление требований к безопасности и уровням сертификации криптографических модулей (включая HSM) в) Регулирование правил использования биометрических данных г) Описание форматов электронных документов *Правильный ответ: б*
10. Основное отличие аппаратного модуля безопасности (HSM) от программного криптопровайдера заключается в том, что в HSM... а) Ключи генерируются быстрее б) Закрытые ключи никогда не покидают защищенную физическую среду устройства в) Поддерживается больше алгоритмов шифрования г) Интерфейс взаимодействия проще для программиста *Правильный ответ: б*
11. Как называется атака, позволяющая злоумышленнику определить криптографический ключ, измеряя время выполнения операций или потребление энергии устройством? а) Прямой перебор (Brute force) б) Атака по побочным каналам (Side-channel attack) в) Дифференциальный криптоанализ г) Социальная инженерия *Правильный ответ: б*
12. Технология ARM TrustZone разделяет ресурсы процессора на два мира. Как они называются? а) Kernel Mode и User Mode б) Normal World и Secure World в) Master и Slave г) Active и Standby *Правильный ответ: б*

13. Какую функцию выполняет IOMMU (Input-Output Memory Management Unit), например Intel VT-d? а) Ускоряет работу видеокарты в играх б) Ограничивает прямой доступ периферийных устройств (DMA) к произвольным областям оперативной памяти в) Шифрует трафик шины PCI Express г) Проверяет цифровую подпись драйверов
Правильный ответ: б

14. Что проверяет АМДЗ (Аппаратный модуль доверенной загрузки), например «Аккорд», перед стартом операционной системы? а) Наличие свободного места на жестком диске б) Целостность BIOS/UEFI, загрузчика и критических файлов ядра до передачи им управления в) Скорость вращения вентиляторов охлаждения г) Срок действия лицензии антивируса
Правильный ответ: б

15. В чем принципиальное отличие однонаправленного шлюза (Data Diode) от традиционного межсетевого экрана? а) Он работает только с зашифрованными данными б) Физическая невозможность передачи данных в обратном направлении на физическом уровне в) Он фильтрует только почтовый трафик г) Он требует установки двух кабелей вместо одного
Правильный ответ: б

16. Какова основная цель технологии UEFI Secure Boot? а) Защита от подбора пароля пользователя при входе в систему б) Запрет запуска исполняемых файлов, если их цифровая подпись не входит в список доверенных производителем в) Автоматическое обновление прошивки материнской платы г) Блокировка USB-портов
Правильный ответ: б

17. Какой российский регулятор осуществляет сертификацию программно-аппаратных средств защиты информации по требованиям отсутствия недекларированных возможностей (НДВ)? а) Роскомнадзор б) Министерство цифрового развития в) ФСТЭК России г) Центральный банк РФ
Правильный ответ: в

18. Стековые канарейки (Stack Canaries) — это защитный механизм, который... а) Резервирует дополнительную память под переменные б) Размещает специальное случайное значение перед адресом возврата для обнаружения факта переполнения буфера в) Шифрует содержимое стека при передаче по сети г) Очищает оперативную память после завершения программы
Правильный ответ: б

19. При использовании смарт-карт стандарта Java Card апплеты выполняются внутри... а) Операционной системы Windows компьютера, к которому подключен считыватель б) Процессора самого микропроцессора карты в изолированной среде в) Браузера пользователя г) Драйвера USB-порта
Правильный ответ: б

20. Технология микросегментации в современных ЦОД направлена на... а) Увеличение объема дискового хранилища б) Изоляцию потоков трафика между отдельными рабочими нагрузками (приложениями/контейнерами) внутри одной физической сети в) Объединение всех серверов в один широковеб-домен г) Снижение стоимости электроэнергии
Правильный ответ: б

Ключи: 1-б, 2-в, 3-б, 4-б, 5-б, 6-а, 7-в, 8-б, 9-б, 10-б, 11-б, 12-б, 13-б, 14-б, 15-б, 16-б, 17-в, 18-б, 19-б, 20-б.

21. Фундаментальным свойством монитора обращений (референс-монитора), гарантирующим, что он вызывается при каждом обращении субъекта к объекту и его невозможно обойти, является свойство _____. (Правильный ответ: полноты или полноты медиации)

22. В архитектуре x86 аппаратный механизм защиты памяти, который помечает определенные страницы как «неисполняемые» (No-eXecute) и предотвращает выполнение кода из областей данных (например, стека), называется технологией _____ или устанавливается _____-бит. (Правильные ответы: DEP; NX)

23. Аппаратный корень доверия в современных компьютерах реализуется с помощью специализированного микрочипа на материнской плате — модуля _____. Он используется для безопасного хранения криптографических ключей, хеш-сумм компонентов BIOS/UEFI и обеспечения целостности цепочки загрузки. (Правильный ответ: TPM / Trusted Platform Module)

24. Согласно модели мандатного управления доступом Белла — Лападулы, правило *Simple Security Property* («простое свойство безопасности»), запрещающее субъекту читать данные более высокого уровня секретности, кратко формулируется как «по _____». (Правильный ответ: *read up* / чтение вверх)

25. Специализированное физическое устройство, предназначенное для выполнения криптографических операций в защищенной среде, где закрытые ключи никогда не покидают пределы устройства в открытом виде, называется аппаратным модулем безопасности, или сокращенно _____. (Правильный ответ: HSM / Hardware Security Module)

26. Задание 1. Установите соответствие между технологией защиты и ее основным назначением

Технология	Назначение
1. ASLR (Address Space Layout Randomization)	А. Предотвращение выполнения кода из областей памяти, помеченных как данные (стек, куча).
2. DEP / NX-бит	Б. Рандомизация базовых адресов загрузки модулей для затруднения эксплуатации уязвимостей.
3. Stack Canaries	В. Разделение процессора на «нормальный» и «защищенный» миры исполнения.
4. ARM TrustZone	Г. Размещение случайного значения перед адресом возврата для обнаружения переполнения буфера.

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

27. Установите соответствие между аппаратным средством и его ключевой функцией

Средство	Функция
1. TPM (Trusted Platform Module)	А. Хранение закрытых ключей электронной подписи и выполнение криптографических операций в корпусе, защищенном от вскрытия.
2. HSM (Hardware Security Module)	Б. Аппаратный контроль целостности BIOS/UEFI и загрузчика до передачи управления операционной системе.
3. Смарт-карта / USB-токен	В. Хранение хеш-сумм критических компонентов ПО и привязка криптографических ключей к конкретной платформе («привязка железа»).
4. АМДЗ (Аппаратный модуль доверенной загрузки)	Г. Масштабируемое решение для центров обработки данных по управлению тысячами ключей и ускорению SSL/TLS-шифрования.

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

28. Установите соответствие между моделью безопасности и правилом доступа

Модель	Правило
1. Белла — Лападулы (Bell-LaPadula)	А. Запрет записи информации с более высокого уровня секретности на более низкий (<i>no write down</i>).
2. Бибы (Biba)	Б. Запрет чтения информации с более высокого уровня секретности при низком уровне допуска (<i>no read up</i>).
3. Кларка — Вилсона (Clark-Wilson)	В. Запрет записи данных с низкого уровня целостности на высокий (<i>no write up</i>) для предотвращения порчи надежных данных.
4. Харрисона — Руззо — Ульмана (HRU)	Г. Формальная модель матрицы доступа, анализирующая разрешимость вопроса о возникновении права «владеть» за конечное число шагов.

Правильные ответы: 1–Б (и А), 2–В (и А), 3–В (акцент на транзакции), 4–Г. (Примечание: Для моделей Белла — Лападулы и Бибы характерны оба правила, но в тестах их часто разделяют: 1–Б — классический признак конфиденциальности, 2–В — классический признак целостности).

29. Установите соответствие между типом атаки и принципом ее реализации

Атака	Принцип реализации
1. VM Escape (Побег из виртуальной машины)	А. Использование остаточных данных в оперативной памяти или регистрах процессора после завершения операции.
2. Cold Boot Attack	Б. Прорыв изоляции гостевой ОС через эксплуатацию уязвимостей в коде гипервизора (например, в эмуляторе сетевой карты).
3. Side-channel attack (по времени)	В. Мгновенное охлаждение модуля памяти жидким азотом для переноса микросхем на другое устройство и считывания ключей шифрования диска.
4. DMA-атака (через FireWire/Thunderbolt)	Г. Прямой высокоскоростной доступ периферийного устройства к физической оперативной памяти в обход центрального процессора.

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

30. Установите соответствие между российским регулятором и областью его полномочий в сфере ПАЗИ

Регулятор	Область полномочий
1. ФСТЭК России	А. Выработка государственной политики и нормативно-правовое регулирование в области разработки и производства СКЗИ.
2. ФСБ России	Б. Сертификация средств технической защиты информации от несанкционированного доступа (НСД) и отсутствие недеklarированных возможностей (НДВ).
3. Минцифры России	В. Аккредитация удостоверяющих центров и надзор за соблюдением требований к использованию электронных подписей.
4. Банк России	Г. Выпуск стандартов безопасности (ГОСТ Р 57580) и обязательное

Регулятор (ЦБ РФ)	Область полномочий требование применения сертифицированных СЗИ в платежных системах.
-----------------------------	--

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

1.4 Практические задания

Задание 1. Сформулируйте три обязательных свойства референс-монитора (монитора обращений). Объясните, почему полная медиация критически важна для безопасности ядра ОС.

Задание 2. Постройте формальную модель матрицы доступа HRU для системы из двух субъектов (S1, S2) и двух объектов (O1, O2). Опишите последовательность примитивных операторов для передачи права «запись» от S1 к S2 относительно объекта O1.

Задание 3. Сравните модели Белла — Лападулы и Биба. Приведите по одному практическому примеру применения каждой модели (например, в военных системах или банковских транзакциях).

Задание 4. Опишите принцип работы механизма ASLR (рандомизация адресного пространства). Предложите два различных метода обхода (*bypass*) ASLR при наличии уязвимости типа Use-After-Free.

Задание 5. В системе реализовано мандатное управление доступом (MAC). Субъект имеет уровень «Конфиденциально», объект — «Секретно». Разрешит ли система операцию чтения? Изменится ли решение, если операция будет «запись»? Обоснуйте ответ правилами соответствующих моделей.

Задание 6. Разработайте алгоритм проверки целостности критических системных файлов Windows с использованием встроенного механизма WDAC (Windows Defender Application Control) и политики принудительного подписания драйверов (*Driver Signing Enforcement*).

Задание 7. Опишите механизм реализации атаки класса Kernel-Mode Rootkit через подмену таблицы SSDT (System Service Dispatch Table) в legacy-системах Windows. Каким образом современные механизмы *Kernel Patch Protection* (PatchGuard) препятствуют этой атаке?

Задирование 8. Настройте базовую политику SELinux для веб-сервера Apache. Опишите контекст безопасности (`httpd_sys_content_t`), который должен быть назначен для каталога `/var/www/html`, чтобы сервер мог читать файлы, но не имел права создавать сетевые соединения.

Задание 9. Проанализируйте риски использования технологии вложенной виртуализации (Nested Virtualization). Какие новые векторы атак появляются у злоумышленника, получившего контроль над гостевой ОС первого уровня (L1)?

Задание 10. Объясните разницу между изоляцией на уровне контейнеров (Docker/LXC) и полной аппаратной виртуализацией (KVM/Hyper-V) с точки зрения поверхности атаки и механизмов разграничения ресурсов (Namespaces/Cgroups vs Rings -1).

Задание 11. Смоделируйте процесс удаленной аттестации (Remote Attestation) с использованием модуля TPM 2.0. Опишите, какие значения регистров PCR (Platform Configuration Registers) отправляются серверу и как проверяющая сторона убеждается в неизменности загрузчика.

Задание 12. Опишите архитектуру микропроцессорной смарт-карты. Перечислите основные компоненты чипа (CPU, ROM, RAM, Crypto Co-processor, File System) и их роль в выполнении апплета электронной подписи стандарта Java Card.

Задание 13. Рассчитайте теоретическую производительность HSM-модуля, если он выполняет операции RSA-2048 (расшифрование) со скоростью 5000 операций в секунду, а приложению требуется обрабатывать поток из 10 000 TLS-рукопожатий в секунду. Сколько модулей необходимо установить?

Задание 14. Охарактеризуйте атаку по побочным каналам (Side-Channel Attack) методом дифференциального анализа питания (DPA). Почему программная реализация AES без маскирования данных уязвима к этому типу атак?

Задание 15. Раскройте концепцию ARM TrustZone. Опишите сценарий безопасного хранения биометрических шаблонов отпечатков пальцев в смартфоне, используя разделение на Normal World и Secure World.

Задание 16. Объясните назначение технологии IOMMU (VT-d / AMD-Vi). Составьте схему взаимодействия устройства с поддержкой DMA (например, видеокарты или сетевого адаптера) с оперативной памятью до и после включения IOMMU.

Задание 17. Спроектируйте сегмент сети промышленного предприятия с использованием однонаправленного шлюза (Data Diode) для передачи телеметрии из технологического сегмента в офисный. Докажите невозможность обратного управления контроллерами через это устройство.

Задание 18. Опишите работу АМДЗ (Аппаратного модуля доверенной загрузки), например «Аккорд-АМДЗ». Перечислите этапы контроля целостности, выполняемые устройством до момента монтирования файловой системы операционной системы.

Задание 19. Согласно требованиям ФСТЭК России (Приказ №18 для КИИ), определите необходимость применения сертифицированных МЭ (межсетевых экранов) уровня физической среды для информационной системы 1-го класса защищенности. Укажите конкретный тип межсетевого экрана из реестра.

Задание 20. Проведите сравнительный анализ программного VPN-клиента (OpenVPN) и специализированного криптошлюза (ПАК ViPNet Coordinator HW). Заполните таблицу сравнения по критериям: производительность шифрования, место хранения закрытых ключей, устойчивость к компрометации ОС.

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.

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

ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.1. Выбирает принципы формирования политики информационной безопасности в информационных системах ОПК-10.2. Подбирает и конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности
--------	--	--

3.1. Вопросы к зачету

1. Классификация программно-аппаратных средств защиты информации (ПАЗИ). Различие между средствами общего назначения со встроенными функциями защиты и специализированными СЗИ.
2. Концепция доверенной вычислительной базы (*TCB* — *Trusted Computing Base*). Основные требования к компонентам *TCB*.
3. Монитор обращений (референс-монитор): определение, три фундаментальных свойства (необходимость, полнота, изолированность) и способы его реализации в современных ОС.
4. Уровни привилегий процессора (кольца защиты архитектуры x86: Ring 0–Ring 3). Механизмы перехода между кольцами (шлюзы вызовов).
5. Понятие «задней двери» (*backdoor*) и руткитов уровня ядра (*kernel-mode rootkits*). Методы скрытого перехвата системных функций (*SSDT/IAT hooking*).
6. Доверенная загрузка компьютера: цели, этапы (загрузчик MBR/UEFI -> ядро ОС -> службы) и механизмы контроля целостности на каждом этапе.
7. Аппаратный корень доверия (*Hardware Root of Trust*). Роль модулей TPM (*Trusted Platform Module*) и Intel Boot Guard / AMD Hardware Validated Boot в обеспечении безопасной загрузки.
8. Специализированные защищенные компьютеры и сети: понятие физического разрыва (*air gap*), однонаправленные шлюзы (*data diodes*).
9. Программно-определяемые периметры (*SDP*) и микросегментация как методы защиты облачных инфраструктур и ЦОД.
10. Средства доверенного времени: аппаратные источники точного времени и их роль в разборе инцидентов информационной безопасности (логирование, метки Kerberos).
11. Факторы аутентификации («что вы знаете», «что у вас есть», «кем вы являетесь»). Многофакторная аутентификация (*MFA*) и ее устойчивость к атакам типа *Man-in-the-Middle*.
12. Технологии биометрической идентификации. Понятия *FAR* (*False Acceptance Rate*) и *FRR* (*False Rejection Rate*). Хранение биометрических шаблонов вместо исходных данных.
13. Модель Харрисона — Руззо — Ульмана (*HRU*): формальное описание матрицы доступа, примитивные операторы и доказательство разрешимости задачи безопасности.
14. Мандатное управление доступом (*MAC*, например, модель Белла — Лападулы). Субъектные и объектные метки конфиденциальности. Свойства Simple Security (*no read up*) и - (*no write down*).
15. Избирательное (дискреционное) управление доступом (*DAC*) в файловых системах (биты прав *rwX* в Linux, списки *ACL* в Windows NTFS).
16. Ролевое управление доступом (*RBAC*) и атрибутивное управление доступом (*ABAC*). Сравнение гибкости настройки политик для крупных корпоративных систем.

17. Технология виртуализации ввода-вывода (SR-IOV, GPU Passthrough) и риски утечки данных через побочные каналы между виртуальными машинами.
18. Механизмы изоляции адресного пространства процессов. Таблицы страниц, трансляция адресов (MMU) и защита от переполнения буфера на уровне оборудования (DEP/NX-bit).
19. Технология ASLR (Address Space Layout Randomization). Принцип работы и методы обхода (утечка указателей, атаки типа ROP — Return-Oriented Programming).
20. Песочницы (sandboxes) и контейнеризация (Docker, LXC, gVisor). Различия в механизмах изоляции (namespaces, cgroups в Linux; гипервизорные песочницы).
21. Ядра безопасности повышенной надежности (Security-Enhanced Linux — SELinux, AppArmor). Типовая и мандатная модели доступа внутри одной ОС.
22. Обеспечение безопасного удаления информации с магнитных и твердотельных накопителей (SSD). Проблемы команды TRIM, wear leveling и остаточной намагниченности.
23. Аппаратная виртуализация (Intel VT-x, AMD-V). Кольцо -1: архитектура мониторов виртуальных машин (Hypervisor Type 1 vs Type 2) и атака «голубой пилюлей» (Blue Pill).
24. Смарт-карты и USB-токены (Рутокен, JaCarta). Архитектура микропроцессорной карты: чиплет, собственная ОС, файловая система, апплеты.
25. Апплетно-модульная архитектура (Java Card). Принципы выполнения кода внутри защищенного элемента (Secure Element).
26. Аппаратные модули безопасности (HSM — Hardware Security Modules). Требования стандарта FIPS 140-2/3 уровней безопасности. Применение в банковских системах (PIN-блоки) и PKI.
27. Технология исполнения кода в доверенной среде (TEE — Trusted Execution Environment, пример: ARM TrustZone). Разделение ресурсов процессора на «нормальный» и «защищенный» миры.
28. Защита от побочных каналов (side-channel attacks): анализ энергопотребления (SPA/DPA) и временных задержек при выполнении криптографических операций.
29. Аппаратная проверка подлинности компонентов (Hardware Attestation). Удаленное подтверждение конфигурации устройства перед предоставлением доступа к ресурсам.
30. Российские нормативные требования к программно-аппаратным СЗИ. Сертификация ФСТЭК России по требованиям к уровням отсутствия недекларированных возможностей (НДВ) и по профилям защиты межсетевых экранов.

3.2. Задания для зачета:

Задание 1. Сформулируйте три обязательных свойства референс-монитора (монитора обращений). Объясните, почему полная медиация критически важна для безопасности ядра ОС.

Задание 2. Постройте формальную модель матрицы доступа HRU для системы из двух субъектов (S1, S2) и двух объектов (O1, O2). Опишите последовательность примитивных операторов для передачи права «запись» от S1 к S2 относительно объекта O1.

Задание 3. Сравните модели Белла — Лападулы и Биба. Приведите по одному практическому примеру применения каждой модели (например, в военных системах или банковских транзакциях).

Задание 4. Опишите принцип работы механизма ASLR (рандомизация адресного пространства). Предложите два различных метода обхода (bypass) ASLR при наличии уязвимости типа Use-After-Free.

Задание 5. В системе реализовано мандатное управление доступом (MAC). Субъект имеет уровень «Конфиденциально», объект — «Секретно». Разрешит ли система операцию чтения? Изменится ли решение, если операция будет «запись»? Обоснуйте ответ правилами соответствующих моделей.

Задание 6. Разработайте алгоритм проверки целостности критических системных файлов Windows с использованием встроенного механизма WDAC (Windows Defender Application Control) и политики принудительного подписания драйверов (*Driver Signing Enforcement*).

Задание 7. Опишите механизм реализации атаки класса Kernel-Mode Rootkit через подмену таблицы SSDT (System Service Dispatch Table) в legacy-системах Windows. Каким образом современные механизмы *Kernel Patch Protection* (PatchGuard) препятствуют этой атаке?

Задание 8. Настройте базовую политику SELinux для веб-сервера Apache. Опишите контекст безопасности (`httpd_sys_content_t`), который должен быть назначен для каталога `/var/www/html`, чтобы сервер мог читать файлы, но не имел права создавать сетевые соединения.

Задание 9. Проанализируйте риски использования технологии вложенной виртуализации (Nested Virtualization). Какие новые векторы атак появляются у злоумышленника, получившего контроль над гостевой ОС первого уровня (L1)?

Задание 10. Объясните разницу между изоляцией на уровне контейнеров (Docker/LXC) и полной аппаратной виртуализацией (KVM/Hyper-V) с точки зрения поверхности атаки и механизмов разграничения ресурсов (Namespaces/Cgroups vs Rings -1).

Задание 11. Смоделируйте процесс удаленной аттестации (Remote Attestation) с использованием модуля TPM 2.0. Опишите, какие значения регистров PCR (Platform Configuration Registers) отправляются серверу и как проверяющая сторона убеждается в неизменности загрузчика.

Задание 12. Опишите архитектуру микропроцессорной смарт-карты. Перечислите основные компоненты чипа (CPU, ROM, RAM, Crypto Co-processor, File System) и их роль в выполнении апплета электронной подписи стандарта Java Card.

Задание 13. Рассчитайте теоретическую производительность HSM-модуля, если он выполняет операции RSA-2048 (расшифрование) со скоростью 5000 операций в секунду, а приложению требуется обрабатывать поток из 10 000 TLS-рукопожатий в секунду. Сколько модулей необходимо установить?

Задание 14. Охарактеризуйте атаку по побочным каналам (Side-Channel Attack) методом дифференциального анализа питания (DPA). Почему программная реализация AES без маскирования данных уязвима к этому типу атак?

Задание 15. Раскройте концепцию ARM TrustZone. Опишите сценарий безопасного хранения биометрических шаблонов отпечатков пальцев в смартфоне, используя разделение на Normal World и Secure World.

Задание 16. Объясните назначение технологии IOMMU (VT-d / AMD-Vi). Составьте схему взаимодействия устройства с поддержкой DMA (например, видеокарты или сетевого адаптера) с оперативной памятью до и после включения IOMMU.

Задание 17. Спроектируйте сегмент сети промышленного предприятия с использованием однонаправленного шлюза (Data Diode) для передачи телеметрии из технологического сегмента в офисный. Докажите невозможность обратного управления контроллерами через это устройство.

Задание 18. Опишите работу АМДЗ (Аппаратного модуля доверенной загрузки), например «Аккорд-АМДЗ». Перечислите этапы контроля целостности, выполняемые устройством до момента монтирования файловой системы операционной системы.

Задание 19. Согласно требованиям ФСТЭК России (Приказ №18 для КИИ), определите необходимость применения сертифицированных МЭ (межсетевых экранов) уровня физической среды для информационной системы 1-го класса защищенности. Укажите конкретный тип межсетевого экрана из реестра.

Задание 20. Проведите сравнительный анализ программного VPN-клиента (OpenVPN) и специализированного криптошлюза (ПАК ViPNet Coordinator HW). Заполните таблицу сравнения по критериям: производительность шифрования, место хранения закрытых ключей, устойчивость к компрометации ОС.

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 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 – зачет с оценкой.

Форма проведения промежуточной аттестации – письменный зачет.