

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Узунов Федор Владимирович

Должность: Ректор

Дата подписания: 30.09.2026 08:34:43

Уникальный программный ключ:

fd935d10451b860e912264c0378b5448452b603f94388008a39877a6bcb6f5

**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

*[Signature]* / Г.П. Узунова

«02» февраля 2026 г.

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ  
ЗАЩИТА ОПЕРАЦИОННЫХ СИСТЕМ СЕТЕВЫХ УСТРОЙСТВ**

Направление подготовки  
**09.03.01 «Информатика и вычислительная техника»**  
Профиль  
**Специалист по информационным системам**

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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ПК-1             | Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации | <p>ПК-1.1. Знает современные виды информационного взаимодействия и обслуживания, принципы и методы противодействия несанкционированному информационному воздействию на вычислительные сети и системы передачи информации, основные задачи и понятия криптографии, требования к шифрам и основные характеристики шифров, модели шифров и математические методы их исследования, принципы построения криптографических алгоритмов.</p> <p>ПК-1.2. Умеет использовать и настраивать программно-аппаратные средства защиты информации, проводить анализ показателей качества сетей и систем связи</p> <p>ПК-1.3. Владеет навыками по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации</p> |

### 1.1 Вопросы к текущему контролю

1. Концепция доверенной вычислительной базы (TCB — Trusted Computing Base) в сетевых ОС. Какие компоненты (ядро, стек протоколов, конфигуратор) входят в TCB маршрутизатора и почему компрометация любого из них ведет к полной потере контроля над устройством?
2. Модель «Запрос-Ответ» (Reference Monitor). Как в сетевой ОС реализуется принцип обязательной проверки каждого обращения субъекта (администратора или процесса) к объекту (таблице маршрутизации, интерфейсу) и почему монитор обращений должен быть защищен от модификации?
3. Кольца защиты процессора в сетевом оборудовании. Объясните, как разделение на уровни привилегий (например, User Mode для процессов мониторинга и Kernel Mode для пересылки пакетов) защищает критический трафик от влияния пользовательских скриптов.
4. Архитектура сетевой ОС (монолитная vs микроядерная). Сравните подходы Cisco IOS (монолитная) и современных SDN-контроллеров (микросервисы) с точки зрения поверхности атаки и отказоустойчивости.
5. Протокол TACACS+ против RADIUS. Сравните эти протоколы централизованного управления доступом (AAA) с точки зрения разделения функций аутентификации, авторизации и учета, а также безопасности передачи паролей.

6. Ролевое управление доступом (RBAC) в сетевых ОС. Разработайте матрицу прав для ролей «Администратор», «Оператор» и «Аудитор» на коммутаторе, ограничив доступ к изменению конфигурации VLAN для роли «Оператор».
7. Безопасность протоколов удаленного управления (SSH vs Telnet). Опишите процесс установления защищенного соединения в SSHv2 (обмен ключами, выбор алгоритма шифрования) и объясните, почему использование Telnet недопустимо в современных сетях.
8. Локальная и удаленная аутентификация. В чем заключается риск использования только локальной базы пользователей на устройстве? Опишите сценарий атаки «Fallback Authentication», когда при недоступности RADIUS-сервера устройство разрешает вход по статическому паролю.
9. Безопасность протокола SNMP (v1, v2c, v3). Почему community string в SNMPv1/v2c считается небезопасным, и какие механизмы (Authentication/Privacy protocols) предлагает SNMPv3 для защиты от перехвата и подмены команд?
10. Защита протокола NTP (Network Time Protocol). К чему может привести компрометация службы времени на сетевом устройстве (атака на аутентификацию по сертификатам, сбой логирования) и как работает симметричное/асимметричное шифрование в NTP?
11. Безопасность протоколов управления (NETCONF/RESTCONF). Как использование транспорта SSH (для NETCONF) или HTTPS (для RESTCONF) защищает конфигурацию устройства от несанкционированного чтения и модификации в процессе передачи?
12. Протоколы динамической маршрутизации (OSPF, BGP). Опишите механизмы защиты: использование аутентификации (MD5/SHA) в OSPF и расширение RPKI (Resource Public Key Infrastructure) для предотвращения BGP Hijacking.
13. Безопасная загрузка (Secure Boot) и доверенная загрузка (Trusted Boot). Как процесс проверки цифровой подписи образа ОС (UEFI Secure Boot / Boot Guard) предотвращает запуск вредоносного ПО на этапе старта сетевого устройства?
14. Управление обновлениями (Patch Management). Опишите риски использования ПО, достигшего End-of-Life (EOL). Какова процедура безопасной установки патча на критически важный маршрутизатор (стратегия ISSU — In-Service Software Upgrade)?
15. Защита конфигурационных файлов. Почему хранение конфигураций в открытом виде (например, в TFTP без ACL или в Git-репозитории без шифрования) является критической уязвимостью? Как правильно организовать резервное копирование (Backup) с шифрованием?
16. Изоляция процессов и контроль ресурсов (Control Plane Policing — CoPP). Как механизм CoPP защищает процесс управления (CPU) сетевого устройства от перегрузки (DoS-атаки) служебным трафиком (ICMP, ARP, Routing updates)?
17. Атаки на встроенное ПО (Firmware Attacks). Что такое «Firmware Rootkit»? Почему обнаружение вредоносного кода на уровне прошивки сетевого устройства значительно сложнее, чем на обычном ПК?
18. Анализ поверхности атаки (Attack Surface) сетевой ОС. Перечислите типичные сервисы, включенные по умолчанию, которые следует отключить (например, HTTP-сервер, Finger, BOOTP) для минимизации векторов атаки.
19. Логирование и аудит (Syslog). Какие критические события (изменение конфигурации, неудачные попытки входа, падение интерфейсов) должны централизованно собираться в SIEM-систему для своевременного обнаружения компрометации?
20. Безопасность SDN (Software Defined Networking). В чем заключаются уникальные риски безопасности контроллера SDN (например, OpenDaylight)? Как компрометация единственного контроллера влияет на всю сетевую инфраструктуру?

## 1.2 Темы рефератов:

1. Концепция доверенной вычислительной базы (TCB) в сетевых операционных системах. Анализ поверхности атаки на примере Cisco IOS и Juniper Junos.
2. Сравнение монолитной и модульной архитектуры сетевых ОС. Влияние архитектуры на устойчивость к сбоям и поверхность атаки (на примере монолитной IOS и модульной EOS).
3. Модель «Запрос-Ответ» (Reference Monitor) в сетевом оборудовании. Механизмы реализации контроля доступа к таблицам маршрутизации и конфигурационным файлам.
4. Безопасность микрокода и прошивок (Firmware). Анализ угроз внедрения вредоносного кода на уровне загрузчика (Bootkit) сетевых устройств.
5. Использование гипервизоров в сетевом оборудовании. Изоляция сетевых функций (NFV) и риски компрометации управляющего домена.
6. Протоколы централизованного управления доступом (AAA): сравнительный анализ TACACS+ и RADIUS. Оценка безопасности передачи данных и разделения полномочий.
7. Ролевое управление доступом (RBAC) в сетевых ОС. Проектирование матрицы доступа для операторов связи и администраторов корпоративных сетей.
8. Безопасность протокола SSHv2 на сетевых устройствах. Анализ алгоритмов обмена ключами (KEX) и методов защиты от атак типа «Downgrade».
9. Управление парольной политикой на сетевых устройствах. Проблемы хранения хешей паролей в конфигурациях и использование систем одноразовых паролей (OTP).
10. Анализ рисков «Fallback Authentication». Угрозы несанкционированного доступа при недоступности RADIUS-сервера и механизмы защиты.
11. Эволюция безопасности протокола SNMP: от community string (v1/v2c) к USM и VACM (v3). Проблемы шифрования и аутентификации в управлении сетями.
12. Защита службы времени (NTP) в критической инфраструктуре. Анализ уязвимостей NTP Amplification и методы безопасной синхронизации (NTP Autokey, PTP).
13. Безопасность протоколов RESTCONF и NETCONF. Использование TLS для защиты передачи конфигураций и сравнение с традиционными методами (TFTP, SCP).
14. Защита протоколов динамической маршрутизации (OSPF, BGP). Механизмы аутентификации соседей и роль RPKI в предотвращении перехвата маршрутов (BGP Hijacking).
15. Анализ безопасности протокола LLDP (Link Layer Discovery Protocol). Риски утечки топологии сети и методы сегментации (LLDP-MED).
16. Механизмы доверенной загрузки (Secure Boot / UEFI) в сетевых устройствах. Роль аппаратных модулей (TPM/Root of Trust) в проверке целостности образа ОС.
17. Стратегии безопасного обновления ПО (Patch Management). Сравнительный анализ процессов ISSU (In-Service Software Upgrade) и классического перезапуска сервисов.
18. Защита конфигурационных файлов. Методы шифрования (AES) и цифровое подписание конфигураций для предотвращения несанкционированных изменений.
19. Контроль плоскости управления (Control Plane Policing — CoPP). Защита ресурсов CPU сетевого устройства от DoS-атак служебным трафиком.
20. Безопасность протоколов резервирования шлюза (FHRP). Анализ уязвимостей HSRP, VRRP и GLBP (атаки перехвата роли Default Gateway) и методы защиты.

### 1.3 Тестовые задания

1. В чем заключается фундаментальное отличие протокола TACACS+ от RADIUS при управлении доступом к сетевому оборудованию? а) TACACS+ работает только по протоколу UDP, а RADIUS — по TCP. б) TACACS+ шифрует весь пакет целиком, а RADIUS шифрует только поле пароля. в) RADIUS поддерживает двухфакторную аутентификацию, а TACACS+ — нет. г) TACACS+ используется только для беспроводных сетей, а RADIUS — для проводных. *Правильный ответ: б*

2. Какова основная цель механизма Control Plane Policing (CoPP) на маршрутизаторе?  
а) Увеличение скорости пересылки пакетов в аппаратных чипах (ASIC). б) Защита ресурсов центрального процессора (CPU) устройства от перегрузки служебным трафиком (атаки типа DoS). в) Шифрование таблиц маршрутизации при передаче между узлами. г) Ограничение скорости интернет-канала для пользователей. *Правильный ответ: б*
3. Почему использование протокола Telnet для управления современным коммутатором считается грубой ошибкой безопасности? а) Telnet потребляет слишком много оперативной памяти. б) Весь трафик Telnet, включая логины и пароли, передается в открытом (незашифрованном) виде. в) Telnet не поддерживает работу через интернет. г) Telnet не позволяет изменять настройки VLAN. *Правильный ответ: б*
4. Какую уязвимость в протоколе SNMP версий v1 и v2c считают критической? а) Отсутствие шифрования и аутентификации на основе открытых строк «community string», передаваемых в открытом виде. б) Невозможность мониторинга температуры устройства. в) Слишком высокая нагрузка на сеть из-за частых запросов. г) Несовместимость с оптоволоконными интерфейсами. *Правильный ответ: а*
5. Что проверяет механизм Secure Boot (доверенная загрузка) при старте сетевого устройства? а) Наличие активной подписки на техническую поддержку производителя. б) Целостность и подлинность цифровой подписи образа операционной системы перед её запуском. в) Скорость вращения вентиляторов охлаждения. г) Наличие подключенных USB-устройств. *Правильный ответ: б*
6. В архитектуре сетевой ОС какой компонент входит в «Доверенную вычислительную базу» (TCB — Trusted Computing Base)? а) Только пластиковый корпус устройства. б) Ядро операционной системы, стек протоколов и модули управления доступом. в) Только пользовательские скрипты автоматизации. г) Внешний блок питания. *Правильный ответ: б*
7. Какую атаку на протокол динамической маршрутизации BGP позволяет предотвратить технология RPKI (Resource Public Key Infrastructure)? а) Перегрузку таблицы маршрутизации (Memory Exhaustion). б) BGP Hijacking (ложное объявление чужих IP-префиксов). в) Физическое повреждение кабеля связи. г) Подбор пароля администратора. *Правильный ответ: б*
8. Почему хранение конфигурационных файлов сетевых устройств в открытом виде на TFTP-сервере является опасным? а) TFTP не поддерживает передачу файлов размером более 1 МБ. б) Конфигурация содержит чувствительные данные (хеши паролей, ключи SNMP, настройки VPN), которые может перехватить злоумышленник в локальной сети. в) TFTP работает слишком медленно для загрузки образа ОС. г) TFTP требует установки платной лицензии на сервере. *Правильный ответ: б*
9. Что такое «Firmware Rootkit» в контексте сетевого оборудования? а) Программа для автоматического обновления драйверов. б) Вредоносный код, внедренный на уровне прошивки устройства, который сохраняет присутствие даже после переустановки ОС. в) Графическая тема оформления интерфейса командной строки. г) Утилита для очистки кэша ARP. *Правильный ответ: б*
10. Какую роль играет протокол NTP (Network Time Protocol) в обеспечении безопасности сетевой инфраструктуры? а) Он распределяет IP-адреса между клиентами. б) Он обеспечивает синхронизацию времени, без которой невозможен корректный анализ логов и работа механизмов аутентификации (например, Kerberos или TLS-сертификатов). в) Он шифрует трафик между офисами компании. г) Он определяет оптимальную скорость загрузки файлов. *Правильный ответ: б*
11. В чем преимущество использования RBAC (Role-Based Access Control) на крупном сетевом оборудовании? а) Это позволяет устройству потреблять меньше электроэнергии. б) Это позволяет разграничить права (например, «Администратор», «Оператор», «Аудитор»), следуя принципу наименьших привилегий. в) Это автоматически обновляет

прошивку устройства. г) Это увеличивает количество физических портов на коммутаторе.

*Правильный ответ: б*

12. Какой механизм защиты плоскости управления (Control Plane) позволяет ограничить количество входящих ICMP-пакетов, обрабатываемых процессором маршрутизатора? а) NAT (Network Address Translation) б) ACL (Access Control List) на физических интерфейсах в) CoPP (Control Plane Policing) или CPPr (Control Plane Protection) г) Port Security на коммутаторах *Правильный ответ: в*

13. Почему протокол SNMPv3 считается значительно более безопасным, чем его предшественники? а) Он работает только на новых моделях оборудования. б) Он вводит строгую аутентификацию (HMAC) и конфиденциальность (шифрование AES/DES) для всего трафика управления. в) Он полностью отказывается от использования UDP. г) Он позволяет управлять устройствами только через веб-интерфейс. *Правильный ответ: б*

14. Что представляет собой атака «Fallback Authentication» на сетевом устройстве? а) Использование биометрических данных для входа. б) Злоумышленник провоцирует отказ RADIUS-сервера, чтобы устройство переключилось на локальную базу с простым или стандартным паролем. в) Автоматическое создание резервной копии конфигурации. г) Ускорение процесса аутентификации за счет кэширования. *Правильный ответ: б*

15. Какую угрозу для протокола VRRP (Virtual Router Redundancy Protocol) устраняет использование аутентификации? а) Замедление сходимости сети при обрыве кабеля. б) Попытку злоумышленника захватить роль Master-роутера и стать шлюзом по умолчанию для перехвата трафика (Man-in-the-Middle). в) Физический выход из строя блока питания. г) Ошибку в таблице MAC-адресов. *Правильный ответ: б*

16. Протокол \_\_\_\_\_ + является предпочтительным для централизованного управления доступом (AAA) к сетевому оборудованию, так как он шифрует все тело пакета и разделяет функции аутентификации и авторизации. *(Правильный ответ: TACACS)*

17. Для защиты ресурсов центрального процессора (CPU) сетевого устройства от перегрузки служебным трафиком (например, атаками на отказ в обслуживании) применяется механизм \_\_\_\_\_ (CoPP). *(Правильный ответ: Control Plane Policing / Полиция плоскости управления)*

18. В отличие от Telnet, протокол \_\_\_\_\_ обеспечивает шифрование всего трафика управления, включая передаваемые пароли и команды конфигурации. *(Правильный ответ: SSH / Secure Shell)*

19. Критическая уязвимость протокола SNMP версий v1 и v2c заключается в использовании открытых строк \_\_\_\_\_, которые передаются по сети в незащищенном виде. *(Правильный ответ: community / сообщества)*

20. Механизм \_\_\_\_\_ Boot (Безопасная загрузка) проверяет цифровую подпись образа операционной системы перед её запуском, предотвращая запуск модифицированного вредоносного ПО. *(Правильный ответ: Secure)*

21. Вредоносный код, внедренный на уровне прошивки (Firmware) и сохраняющий свое присутствие даже после переустановки ОС, называется \_\_\_\_\_ kit. *(Правильный ответ: Root)*

22. Протокол динамической маршрутизации BGP может быть защищен от ложного объявления чужих IP-префиксов (Hijacking) с помощью инфраструктуры \_\_\_\_\_. *(Правильный ответ: Resource / Resource Public Key Infrastructure)*

23. Для защиты плоскости управления (Control Plane) от атак типа ICMP-флуд на уровне процессора используется механизм \_\_\_\_\_. *(Правильный ответ: Policing / Police)*

24. В протоколе SNMPv3 для обеспечения конфиденциальности и защиты от перехвата данных используется алгоритм шифрования \_\_\_\_\_ (или 3DES). *(Правильный ответ: AES / Advanced Encryption Standard)*

25. Технология \_\_\_\_\_ (RBAC) позволяет разграничить права администраторов, следуя принципу наименьших привилегий (например, разделяя роли «Администратор» и «Оператор»). (Правильный ответ: Role-Based Access Control / Управление доступом на основе ролей)

**26. Соответствие между протоколом управления и его характеристикой**

| Протокол  | Характеристика                                                                         |
|-----------|----------------------------------------------------------------------------------------|
| 1. Telnet | А. Современный стандарт, обеспечивающий полное шифрование сессии и целостность данных. |
| 2. SSH    | Б. Устаревший протокол, передающий все данные, включая пароли, в открытом виде.        |
| 3. HTTP   | В. Не рекомендуется для управления, если не используется совместно с TLS (HTTPS).      |
| 4. RADIUS | Г. Протокол AAA, шифрующий только поле пароля, но не имя пользователя или атрибуты.    |



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

**27. Соответствие между протоколом и его основной задачей безопасности**

| Протокол        | Основная задача                                                                       |
|-----------------|---------------------------------------------------------------------------------------|
| 1. NTP Autokey) | (с А. Защита от ложного объявления маршрутов (BGP Hijacking).                         |
| 2. RPKI         | Б. Защита от атак типа «Man-in-the-Middle» при управлении устройством.                |
| 3. SSH          | В. Обеспечение достоверности времени для работы логов и сертификатов.                 |
| 4. SNMPv3       | Г. Защита мониторинга и управления от перехвата данных (шифрование и аутентификация). |



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

**28. Соответствие между уровнем AAA и протоколом**

| Уровень AAA                        | Протокол                                                                     |
|------------------------------------|------------------------------------------------------------------------------|
| 1. Аутентификация (Authentication) | А. Определение того, какие именно команды пользователю разрешено выполнять.  |
| 2. Авторизация (Authorization)     | Б. Фиксация действий пользователя (кто, когда и что изменил в конфигурации). |
| 3. Учет (Accounting)               | В. Проверка личности пользователя (логин/пароль или сертификат).             |
| 4. TACACS+                         | Г. Протокол, позволяющий детально авторизовать каждую введенную команду.     |



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

**29. Соответствие между типом атаки и протоколом**

| Тип атаки                          | Протокол                                         |
|------------------------------------|--------------------------------------------------|
| 1. Перехват пароля в открытом виде | А. BGP (при отсутствии RPKI/аутентификации).     |
| 2. BGP Hijacking                   | Б. SNMP v1/v2c (использование community string). |
| 3. Отравление ARP-кэша             | В. Telnet.                                       |
| 4. Подмена строки сообщества       | Г. Локальная сеть (L2), протокол ARP.            |



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

**30. Соответствие между компонентом ОС и его ролью в безопасности**

| Компонент                       | Роль                                                           |
|---------------------------------|----------------------------------------------------------------|
| 1. TCB (Trusted Computing Base) | А. Ограничение скорости входящих пакетов, направленных на CPU. |

| Компонент              | Роль                                                                                        |
|------------------------|---------------------------------------------------------------------------------------------|
| 2. CoPP                | Б. Совокупность компонентов (ядро, стек), отказ которых нарушает безопасность всей системы. |
| 3. Secure Boot         | В. Изоляция процессов друг от друга для предотвращения утечек данных.                       |
| 4. Sandbox (Песочница) | Г. Проверка целостности образа ОС при включении устройства.                                 |

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

#### 1.4 Практические задания

**Задание 1.** Опишите концепцию доверенной вычислительной базы (TCB — Trusted Computing Base) применительно к операционной системе маршрутизатора. Какие компоненты входят в TCB и почему их компрометация критична?

**Задание 2.** Сравните монолитную и модульную архитектуру сетевых ОС (на примере Cisco IOS и Juniper Junos). Как архитектурные различия влияют на устойчивость к сбоям и поверхность атаки?

**Задание 3.** Модель «Запрос-Ответ» (Reference Monitor). Как в сетевой ОС реализуется принцип обязательного посредничества при доступе субъекта (процесса/пользователя) к объекту (таблице маршрутизации/памяти)?

**Задание 4.** Кольца защиты процессора в сетевом оборудовании. Объясните, как разделение на уровни привилегий (Kernel Mode/User Mode) защищает процесс пересылки пакетов (Data Plane) от вмешательства процессов управления (Control Plane).

**Задание 5.** Анализ поверхности атаки (Attack Surface) сетевой ОС. Перечислите типичные сервисы, включенные по умолчанию, которые следует отключить для минимизации векторов атаки.

**Задание 6.** Протоколы AAA: сравнительный анализ TACACS+ и RADIUS. Почему для администрирования сетевого оборудования TACACS+ считается более безопасным и функциональным?

**Задание 7.** Ролевое управление доступом (RBAC). Разработайте матрицу прав доступа для ролей «Администратор», «Оператор» и «Аудитор» на коммутаторе уровня 2.

**Задание 8.** Безопасность протокола SSHv2. Опишите процесс обмена ключами (Key Exchange) и объясните, как механизм проверки хост-ключа защищает от атак «человек посередине» (MITM).

**Задание 9.** Локальная база пользователей vs Удаленная (RADIUS/TACACS+). Опишите сценарий атаки «Fallback Authentication», когда при недоступности сервера AAA устройство разрешает вход по статическому паролю.

**Задание 10.** Управление парольной политикой на сетевых устройствах. Почему использование алгоритма хеширования MD5 для хранения паролей в конфигурациях современных устройств недопустимо?

**Задание 11.** Протокол SNMP (v1, v2c, v3). Опишите эволюцию безопасности: от открытых community string до модели безопасности USM (User-based Security Model) в SNMPv3.

**Задание 12.** Защита службы времени (NTP). Почему компрометация NTP на сетевом устройстве критична для безопасности (влияние на логи, сертификаты, аутентификацию) и как работает Autokey?

**Задание 13.** Безопасность протоколов NETCONF/RESTCONF. Как использование транспорта SSH или HTTPS защищает конфигурацию устройства от перехвата и модификации в процессе передачи?

**Задание 14.** Защита протоколов динамической маршрутизации (OSPF, BGP). Опишите механизмы аутентификации соседей (MD5/SHA) и роль RPKI в предотвращении BGP Hijacking.

**Задание 15.** Протокол LLDP (Link Layer Discovery Protocol). Какие риски утечки топологии сети несет этот протокол и как правильно настроить его безопасность (LLDP-MED, TLV validation)?

**Задание 16.** Secure Boot и Trusted Boot. Как процесс цепочки доверия (Chain of Trust) от аппаратного корня (Root of Trust) до образа ОС предотвращает запуск вредоносного ПО на этапе старта?

**Задание 17.** Управление обновлениями (Patch Management). Опишите риски использования ПО, достигшего End-of-Life (EOL). В чем разница между процессом ISSU (In-Service Software Upgrade) и обычным обновлением с перезагрузкой?

**Задание 18.** Защита конфигурационных файлов. Почему хранение конфигураций в открытом виде (например, через TFTP) недопустимо? Опишите методы шифрования конфигураций (AES) и цифрового подписания.

**Задание 19.** Control Plane Policing (CoPP) и Control Plane Protection (CPPr). Как эти механизмы защищают ресурсы CPU сетевого устройства от перегрузки служебным трафиком (ICMP, ARP, Routing updates)?

**Задание 20.** Безопасность протоколов резервирования шлюза (FHRP). Проанализируйте уязвимости HSRP, VRRP и GLBP (атаки перехвата роли Default Gateway) и методы защиты (аутентификация, ACL).

**Задание 21.** Атаки на встроенное ПО (Firmware Attacks). Что такое «Firmware Rootkit» и почему обнаружение вредоносного кода на уровне прошивки значительно сложнее, чем на уровне ОС?

**Задание 22.** Реверс-инжиниринг сетевых ОС. Зачем злоумышленники анализируют бинарные образы IOS/Junos? Какие инструменты (Ghidra, IDA Pro) используются для поиска Hardcoded-секретов?

**Задание 23.** Обфускация кода в сетевых ОС. Как производители (Cisco, Juniper) защищают свои операционные системы от анализа и модификации логики?

**Задание 24.** Root/Jailbreak Detection. Почему сетевые ОС (особенно в потребительском сегменте, например, SOHO-роутеры) проверяют наличие прав суперпользователя и как злоумышленники обходят эти проверки?

**Задание 25.** Атаки на цепочку поставок (Supply Chain). Риски использования скомпрометированных сторонних библиотек и SDK при разработке сетевых ОС.

**Задание 26.** Безопасность SDN (Software Defined Networking). В чем заключаются уникальные риски безопасности контроллера SDN (например, OpenDaylight) и как компрометация контроллера влияет на всю сеть?

**Задание 27.** Микросегментация в сетях ЦОД. Как протоколы VXLAN и NVGRE обеспечивают изоляцию трафика и какие угрозы безопасности возникают в оверлейных сетях?

**Задание 28.** Использование гипервизоров в сетевом оборудовании (NFV — Network Functions Virtualization). Сравните риски безопасности виртуальных сетевых функций (VNF) и аппаратных устройств.

**Задание 29.** EAL (Evaluation Assurance Level) и Common Criteria. Как сертификация сетевых ОС по стандарту ISO/IEC 15408 гарантирует определенный уровень доверия к безопасности продукта?

**Задание 30.** Аудит безопасности сетевой ОС. Составьте план аудита конфигурации маршрутизатора, включающий проверку сервисов, прав доступа, протоколов маршрутизации и настроек логирования (Syslog).

## **2. КРИТЕРИИ ОЦЕНИВАНИЯ ПРИ ПРОВЕДЕНИИ ТЕКУЩЕГО КОНТРОЛЯ**

| Вид контроля     | Наименование работы                                                                                                                                                                                                                                                                                                                 | Наименование оценочных средств                                                                                                              | Шкала оценивания                                                                 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| Текущий контроль | <ul style="list-style-type: none"> <li>- Вопросы для обсуждения на занятиях;</li> <li>- Устные опросы по ранее изученному материалу;</li> <li>- Письменные работы: рефераты, тестовые задания;</li> <li>- Практические задания;</li> <li>- Рефераты и доклады по темам (вопросам), вынесенным на самостоятельную работу.</li> </ul> | Оценка выступлений на практическом (семинарском) занятии, проверка заданий и аудиторных работ, устный опрос, оценивание докладов, рефератов | <p>отлично</p> <p>хорошо</p> <p>удовлетворительно</p> <p>неудовлетворительно</p> |

### 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);<br>2. Своевременность выполнения задания;<br>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.<br>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;<br>5. Самостоятельность решения (владение дополнительным материалом);<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>Тема реферата не раскрыта или выполнена не по существу ранее поставленного вопроса.<br>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                                                                                                                                                                                                                       |
|------------------|------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ПК-1             | Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе | ПК-1.1. Знает современные виды информационного взаимодействия и обслуживания, принципы и методы противодействия несанкционированному воздействию на вычислительные сети и системы передачи информации, основные задачи и понятия криптографии, требования к шифрам и основные |

|  |                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | криптографических) и технических средств защиты информации | <p>характеристики шифров, модели шифров и математические методы их исследования, принципы построения криптографических алгоритмов.</p> <p>ПК-1.2. Умеет использовать и настраивать программно-аппаратные средства защиты информации, проводить анализ показателей качества сетей и систем связи</p> <p>ПК-1.3. Владеет навыками по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации</p> |
|--|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### 3.1. Вопросы к зачету

1. Концепция доверенной вычислительной базы (TCB — Trusted Computing Base) в сетевых ОС. Какие компоненты входят в TCB маршрутизатора и почему компрометация любого из них ведет к полной потере контроля над устройством?
2. Модель «Запрос-Ответ» (Reference Monitor). Как в сетевой ОС реализуется принцип обязательной проверки каждого обращения субъекта (администратора или процесса) к объекту (таблице маршрутизации, интерфейсу) и почему монитор обращений должен быть защищен от модификации?
3. Кольца защиты процессора в сетевом оборудовании. Объясните, как разделение на уровни привилегий (например, User Mode для процессов мониторинга и Kernel Mode для пересылки пакетов) защищает критический трафик от влияния пользовательских скриптов.
4. Архитектура сетевой ОС (монолитная vs микроядерная). Сравните подходы Cisco IOS (монолитная) и современных SDN-контроллеров (микросервисы) с точки зрения поверхности атаки и отказоустойчивости.
5. Анализ поверхности атаки (Attack Surface Analysis). Перечислите не менее 5 потенциальных точек входа для злоумышленника в операционной системе сетевого устройства.
6. Протокол TACACS+ против RADIUS. Сравните эти протоколы централизованного управления доступом (AAA) с точки зрения разделения функций аутентификации, авторизации и учета, а также безопасности передачи паролей.
7. Ролевое управление доступом (RBAC) в сетевых ОС. Разработайте матрицу прав для ролей «Администратор», «Оператор» и «Аудитор» на коммутаторе, ограничив доступ к изменению конфигурации VLAN для роли «Оператор».
8. Безопасность протоколов удаленного управления (SSH vs Telnet). Опишите процесс установления защищенного соединения в SSHv2 (обмен ключами, выбор алгоритма шифрования) и объясните, почему использование Telnet недопустимо в современных сетях.
9. Локальная и удаленная аутентификация. В чем заключается риск использования только локальной базы пользователей на устройстве? Опишите сценарий атаки «Fallback Authentication», когда при недоступности RADIUS-сервера устройство разрешает вход по статическому паролю.
10. Управление парольной политикой. Почему использование слабых алгоритмов хеширования (например, Type 7 или MD5) для хранения паролей в конфигурациях современных устройств считается критической уязвимостью?
11. Безопасность протокола SNMP (v1, v2c, v3). Почему community string в SNMPv1/v2c считается небезопасным, и какие механизмы (Authentication/Privacy protocols) предлагает SNMPv3 для защиты от перехвата и подмены команд?
12. Защита протокола NTP (Network Time Protocol). К чему может привести компрометация службы времени на сетевом устройстве (атака на аутентификацию по сертификатам, сбой логирования) и как работает симметричное/асимметричное шифрование в NTP?
13. Безопасность протоколов управления (NETCONF/RESTCONF). Как использование транспорта SSH (для NETCONF) или HTTPS (для RESTCONF) защищает конфигурацию устройства от несанкционированного чтения и модификации в процессе передачи?
14. Протоколы динамической маршрутизации (OSPF, BGP). Опишите механизмы защиты: использование аутентификации (MD5/SHA) в OSPF и расширение RPKI (Resource Public Key Infrastructure) для предотвращения BGP Hijacking.

15. Безопасность LLDP (Link Layer Discovery Protocol). Какие риски утечки топологии сети несет этот протокол и как правильно настроить его безопасность (TLV validation, отключение на граничных интерфейсах)?
16. Безопасная загрузка (Secure Boot) и доверенная загрузка (Trusted Boot). Как процесс проверки цифровой подписи образа ОС (UEFI Secure Boot / Boot Guard) предотвращает запуск вредоносного ПО на этапе старта сетевого устройства?
17. Управление обновлениями (Patch Management). Опишите риски использования ПО, достигшего End-of-Life (EOL). Какова процедура безопасной установки патча на критически важный маршрутизатор (стратегия ISSU — In-Service Software Upgrade)?
18. Защита конфигурационных файлов. Почему хранение конфигураций в открытом виде (например, в TFTP без ACL или в Git-репозитории без шифрования) является критической уязвимостью? Как правильно организовать резервное копирование (Backup) с шифрованием?
19. Изоляция процессов и контроль ресурсов (Control Plane Policing — CoPP). Как механизм CoPP защищает процесс управления (CPU) сетевого устройства от перегрузки (DoS-атаки) служебным трафиком (ICMP, ARP, Routing updates)?
20. Безопасность протоколов резервирования шлюза (FHRP). Анализ уязвимостей HSRP, VRRP и GLBP (атаки перехвата роли Default Gateway) и методы защиты (аутентификация, ACL).
21. Атаки на встроенное ПО (Firmware Attacks). Что такое «Firmware Rootkit»? Почему обнаружение вредоносного кода на уровне прошивки сетевого устройства значительно сложнее, чем на обычном ПК?
22. Реверс-инжиниринг сетевых ОС. Зачем злоумышленники декомпилируют образы Cisco IOS или Juniper Junos? Какие инструменты используются для поиска Hardcoded-секретов?
23. Обфускация кода в сетевых ОС. Как производители защищают свои операционные системы от анализа и взлома логики (на примере Cisco Type 5/8/9 паролей или обфускации ядра)?
24. Root/Jailbreak Detection. Почему обнаружение взлома ОС (особенно в SOHO-оборудовании) критически важно для безопасности? Опишите два метода определения Jailbreak и два метода их обхода.
25. Аудит безопасности сетевой ОС. Составьте чек-лист из 10 пунктов для проверки конфигурации маршрутизатора перед вводом в эксплуатацию (проверка сервисов, паролей, логирования, ACL).
26. Безопасность SDN (Software Defined Networking). В чем заключаются уникальные риски безопасности контроллера SDN (например, OpenDaylight)? Как компрометация единственного контроллера влияет на всю сетевую инфраструктуру?
27. Микросегментация и оверлейные сети. Как протоколы VXLAN и NVGRE обеспечивают изоляцию трафика в ЦОД и какие угрозы безопасности (VXLAN spoofing) возникают в таких сетях?
28. Сетевые функции в виртуализации (NFV — Network Functions Virtualization). Сравните риски безопасности виртуальных сетевых функций (VNF) и традиционных аппаратных устройств.
29. Оценка доверия (Common Criteria / EAL). Как сертификация сетевых ОС по стандарту ISO/IEC 15408 (на примере уровней EAL) гарантирует определенный уровень доверия к безопасности продукта?
30. Безопасность цепочки поставок (Supply Chain Security). Риски использования скомпрометированных сторонних библиотек и SDK при разработке сетевых ОС. Как проверить подлинность образа ОС, скачанного с сайта производителя?

### 3.2. Задания для зачета:

**Задание 1.** Опишите концепцию доверенной вычислительной базы (TCB — Trusted Computing Base) применительно к операционной системе маршрутизатора. Какие компоненты входят в TCB и почему их компрометация критична?

**Задание 2.** Сравните монолитную и модульную архитектуру сетевых ОС (на примере Cisco IOS и Juniper Junos). Как архитектурные различия влияют на устойчивость к сбоям и поверхность атаки?

**Задание 3.** Модель «Запрос-Ответ» (Reference Monitor). Как в сетевой ОС реализуется принцип обязательного посредничества при доступе субъекта (процесса/пользователя) к объекту (таблице маршрутизации/памяти)?

**Задание 4.** Кольца защиты процессора в сетевом оборудовании. Объясните, как разделение на уровни привилегий (Kernel Mode/User Mode) защищает процесс пересылки пакетов (Data Plane) от вмешательства процессов управления (Control Plane).

**Задание 5.** Анализ поверхности атаки (Attack Surface) сетевой ОС. Перечислите типичные сервисы, включенные по умолчанию, которые следует отключить для минимизации векторов атаки.

**Задание 6.** Протоколы AAA: сравнительный анализ TACACS+ и RADIUS. Почему для администрирования сетевого оборудования TACACS+ считается более безопасным и функциональным?

**Задание 7.** Ролевое управление доступом (RBAC). Разработайте матрицу прав доступа для ролей «Администратор», «Оператор» и «Аудитор» на коммутаторе уровня 2.

**Задание 8.** Безопасность протокола SSHv2. Опишите процесс обмена ключами (Key Exchange) и объясните, как механизм проверки хост-ключа защищает от атак «человек посередине» (MITM).

**Задание 9.** Локальная база пользователей vs Удаленная (RADIUS/TACACS+). Опишите сценарий атаки «Fallback Authentication», когда при недоступности сервера AAA устройство разрешает вход по статическому паролю.

**Задание 10.** Управление парольной политикой на сетевых устройствах. Почему использование алгоритма хеширования MD5 для хранения паролей в конфигурациях современных устройств недопустимо?

**Задание 11.** Протокол SNMP (v1, v2c, v3). Опишите эволюцию безопасности: от открытых community string до модели безопасности USM (User-based Security Model) в SNMPv3.

**Задание 12.** Защита службы времени (NTP). Почему компрометация NTP на сетевом устройстве критична для безопасности (влияние на логи, сертификаты, аутентификацию) и как работает Autokey?

**Задание 13.** Безопасность протоколов NETCONF/RESTCONF. Как использование транспорта SSH или HTTPS защищает конфигурацию устройства от перехвата и модификации в процессе передачи?

**Задание 14.** Защита протоколов динамической маршрутизации (OSPF, BGP). Опишите механизмы аутентификации соседей (MD5/SHA) и роль RPKI в предотвращении BGP Hijacking.

**Задание 15.** Протокол LLDP (Link Layer Discovery Protocol). Какие риски утечки топологии сети несет этот протокол и как правильно настроить его безопасность (LLDP-MED, TLV validation)?

**Задание 16.** Secure Boot и Trusted Boot. Как процесс цепочки доверия (Chain of Trust) от аппаратного корня (Root of Trust) до образа ОС предотвращает запуск вредоносного ПО на этапе старта?

**Задание 17.** Управление обновлениями (Patch Management). Опишите риски использования ПО, достигшего End-of-Life (EOL). В чем разница между процессом ISSU (In-Service Software Upgrade) и обычным обновлением с перезагрузкой?

**Задание 18.** Защита конфигурационных файлов. Почему хранение конфигураций в открытом виде (например, через TFTP) недопустимо? Опишите методы шифрования конфигураций (AES) и цифрового подписания.

**Задание 19.** Control Plane Policing (CoPP) и Control Plane Protection (CPPr). Как эти механизмы защищают ресурсы CPU сетевого устройства от перегрузки служебным трафиком (ICMP, ARP, Routing updates)?

**Задание 20.** Безопасность протоколов резервирования шлюза (FHRP). Проанализируйте уязвимости HSRP, VRRP и GLBP (атаки перехвата роли Default Gateway) и методы защиты (аутентификация, ACL).

**Задание 21.** Атаки на встроенное ПО (Firmware Attacks). Что такое «Firmware Rootkit» и почему обнаружение вредоносного кода на уровне прошивки значительно сложнее, чем на уровне ОС?

**Задание 22.** Реверс-инжиниринг сетевых ОС. Зачем злоумышленники анализируют бинарные образы IOS/Junos? Какие инструменты (Ghidra, IDA Pro) используются для поиска Hardcoded-секретов?

**Задание 23.** Обфускация кода в сетевых ОС. Как производители (Cisco, Juniper) защищают свои операционные системы от анализа и модификации логики?

**Задание 24.** Root/Jailbreak Detection. Почему сетевые ОС (особенно в потребительском сегменте, например, SOHO-роутеры) проверяют наличие прав суперпользователя и как злоумышленники обходят эти проверки?

**Задание 25.** Атаки на цепочку поставок (Supply Chain). Риски использования скомпрометированных сторонних библиотек и SDK при разработке сетевых ОС.

**Задание 26.** Безопасность SDN (Software Defined Networking). В чем заключаются уникальные риски безопасности контроллера SDN (например, OpenDaylight) и как компрометация контроллера влияет на всю сеть?

**Задание 27.** Микросегментация в сетях ЦОД. Как протоколы VXLAN и NVGRE обеспечивают изоляцию трафика и какие угрозы безопасности возникают в оверлейных сетях?

**Задание 28.** Использование гипервизоров в сетевом оборудовании (NFV — Network Functions Virtualization). Сравните риски безопасности виртуальных сетевых функций (VNF) и аппаратных устройств.

**Задание 29.** EAL (Evaluation Assurance Level) и Common Criteria. Как сертификация сетевых ОС по стандарту ISO/IEC 15408 гарантирует определенный уровень доверия к безопасности продукта?

**Задание 30.** Аудит безопасности сетевой ОС. Составьте план аудита конфигурации маршрутизатора, включающий проверку сервисов, прав доступа, протоколов маршрутизации и настроек логирования (Syslog).

#### **4. ОСНОВНЫЕ КРИТЕРИИ ОЦЕНИВАНИЯ ПРИ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ**

##### **Шкала оценивания уровня сформированности универсальной компетенций (зачет)**

| Шкала оценивания | Уровень освоение компетенции         | Критерии оценивания                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Зачет            | Базовый уровень освоения компетенции | Дан правильный и исчерпывающий ответ на вопрос. Обучающийся демонстрирует знание теоретического материала, изложено правильное понимание вопроса, дано достаточно подробное описание предмета ответа, приведены и раскрыты в тезисной форме основные понятия, относящиеся к предмету ответа. Имеется базовый уровень овладения практическими умениями и навыками по данной дисциплине в соответствии с ФГОС . |
| Незачет          | Неудовлетворительный уровень         | Отсутствует ответ или в ответе есть грубые ошибки, свидетельствующие о отсутствии знаний соответствующего                                                                                                                                                                                                                                                                                                     |

|  |  |                                                                                                                                                                    |
|--|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  | программного материала; отсутствие умений и навыков по данной дисциплине в соответствии с ФГОС и/или фрагментарные знания основного учебно-программного материала. |
|--|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**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.

Форма проведения промежуточной аттестации – письменный зачет.