**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
«02» февраля 2026 г.

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

# ЗАЩИТА ИНФОРМАЦИИ В ЦЕНТРАХ ОБРАБОТКИ ДАННЫХ

***Направление подготовки***
**09.03.01 Информатика и вычислительная техника**

***Профиль***: специалист по компьютерным системам

Квалификация
**Бакалавр**

Для всех
форм обучения

Симферополь, 2026 г.

## 1. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

Средства оценивания в ходе текущего контроля:

- устные опросы в ходе лекционных и лабораторных занятий;
- отчеты по лабораторным работам;
- рефераты;
- тестирование;
- задания, выполняемые в ходе лабораторного занятия или рекомендуемые для самостоятельной работы.

| Коды компетенции | Результаты освоения ОПОП | Перечень планируемых результатов обучения по дисциплине |
|---|---|---|
| **ПК-1** | Способен разрабатывать компоненты системных программных продуктов и программное обеспечение | ПК-1.1. Знать: принципы и методы разработки программного обеспечения, работы компиляторов, сетевых служб, операционных систем, драйверов и т.д.<br>ПК-1.2. Уметь: разрабатывать программное обеспечение и системные программные продукты, в том числе сетевые службы, отдельный модули операционной системы, драйверы и т.д.<br>ПК-1.3. Владеть: навыками системного программирования |

### 1.1 Вопросы к текущему контролю

1. Понятия информация, информатизация, информационная система, информационная безопасность.
2. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене
3. Защита информации, тайна, средства защиты информации.
4. Показатели информации: важность, полнота, адекватность, релевантность, толерантность.
5. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.
6. Идентификация, аутентификация и авторизация: определения, различия, примеры реализации.
7. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
8. Структура государственной системы информационной безопасности.
9. Доктрина информационной безопасности Российской Федерации.
10. Понятие угрозы. Виды противников или «нарушителей».
11. Классификация угроз информационной безопасности. Виды угроз. Основные нарушения.
12. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз.
13. Основные положения теории информационной безопасности информационных систем.
14. Системы обнаружения и предотвращения вторжений (IDS/IPS): принципы работы, виды (сетевые, хостовые), методы анализа.
15. Модели безопасности и их применение.
16. Формальные модели безопасности. Дискреционная модель Харрисона-Руззо-Ульмана.
17. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant.
18. Мандатная модель Белла-Ла-Падулы. Ролевая политика безопасности.
19. Уязвимости веб-приложений: SQL-инъекции, межсайтовый скриптинг (XSS), CSRF.

20. Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от НСД.
21. Методы криптографии. Симметричное и асимметричное шифрование.
22. Социальная инженерия: определение, виды атак (фишинг, претекстинг, услуга за услугу), методы противодействия.
23. Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи.
24. Безопасность операционных систем: механизмы защиты (разграничение доступа, аудит), средства усиления (SELinux, AppArmor).
25. Безопасность беспроводных сетей: уязвимости протоколов WEP, WPA, WPA2; преимущества WPA3.
26. Криптографические генераторы случайных чисел.
27. Способы распространения ключей. Обеспечиваемая шифром степень защиты.
28. Анализаторы сетевого трафика (снифферы): назначение, примеры (Wireshark, tcpdump), методы защиты от перехвата трафика.
29. Системы централизованного сбора и анализа событий безопасности (SIEM): архитектура, функции.
30. Основные технологии построения защищенных экономических информационных систем. Функции защиты информации.

### 1.2 Темы рефератов

1. Современные угрозы кибербезопасности: анализ новых видов кибератак и методов защиты (фишинг, ransomware, атаки на IoT).
2. Криптография в сетевой безопасности: применение алгоритмов шифрования (AES, RSA) для защиты данных в компьютерных сетях.
3. Защита облачных технологий: риски и решения для безопасности в облачных сервисах (AWS, Azure).
4. Безопасность беспроводных сетей: уязвимости Wi-Fi и методы защиты (WPA3, аутентификация 802.1X).
5. Социальная инженерия в киберпреступности: техники манипуляции (фишинг, вишинг) и способы противодействия.
6. Анализ и сравнение межсетевых экранов нового поколения (NGFW).
7. Методы обнаружения и предотвращения вторжений (IDS/IPS): современное состояние и перспективы.
8. Технологии виртуальных частных сетей (VPN): обзор протоколов и анализ безопасности.
9. Атаки типа «отказ в обслуживании» (DoS/DDoS): классификация, инструменты и методы защиты.
10. Безопасность протокола DNS: атаки (DNS spoofing, cache poisoning) и способы защиты (DNSSEC).
11. Анализ защищённости веб-приложений с помощью OWASP ZAP и Burp Suite.
12. Криптографические протоколы TLS/SSL: эволюция, уязвимости и настройка безопасных конфигураций.
13. Основы управления уязвимостями: сканирование, оценка рисков и приоритезация исправлений.
14. Роль и применение технологии блокчейн в обеспечении информационной безопасности.
15. Нормативно-правовое обеспечение информационной безопасности в Российской Федерации (ФЗ-149, ФЗ-152, требования ФСТЭК).
16. Методы двухфакторной и многофакторной аутентификации: сравнительный анализ.
17. Безопасность электронной почты: протоколы SPF, DKIM, DMARC.
18. Анализ угроз для промышленных систем управления (АСУ ТП) и методы их защиты.
19. Применение машинного обучения для обнаружения сетевых аномалий и вторжений.
20. Этичный хакинг и тестирование на проникновение: методологии и инструменты.

### 1.2 Тестовые задания

1. Какой стандарт устанавливает основные требования к защите информации в сетях?
   а) ISO 9001
   б) ISO 27001 *(Правильный ответ: б)*
   в) ISO 14001
   г) ISO 45001
2. Какой протокол обеспечивает защиту данных на транспортном уровне?
   а) HTTP
   б) TLS *(Правильный ответ: б)*
   в) FTP
   г) ARP
3. Какой элемент сетевой архитектуры обеспечивает разделение внутренней сети и интернета?
   а) Маршрутизатор
   б) DMZ *(Правильный ответ: б)*
   в) Концентратор
   г) Модем
4. Какой тип межсетевого экрана анализирует содержимое пакетов на уровне приложений?
   а) Пакетный фильтр
   б) NGFW *(Правильный ответ: б)*
   в) Stateful firewall
   г) Прокси-сервер
5. Какой протокол используется для безопасного удалённого администрирования?
   а) Telnet
   б) SSH *(Правильный ответ: б)*
   в) RDP
   г) VNC
6. Какой компонент PKI отвечает за выдачу сертификатов?
   а) Репозиторий
   б) Центр сертификации *(Правильный ответ: б)*
   в) OCSP-сервер
   г) CRL
7. Какой метод защиты наиболее эффективен против MITM-атак?
   а) NAT
   б) Сертификаты и шифрование *(Правильный ответ: б)*
   в) VLAN
   г) MAC-фильтрация
8. Какой инструмент используется для обнаружения сетевых аномалий?
   а) Антивирус
   б) IDS *(Правильный ответ: б)*
   в) Брандмауэр
   г) VPN
9. Какой стандарт рекомендуется для защиты беспроводных сетей?
   а) WEP
   б) WPA3 *(Правильный ответ: б)*
   в) WPA
   г) WPS
10. Какой параметр наиболее важен для стойкости парольной защиты?
    а) Регулярная смена пароля
    б) Длина и сложность *(Правильный ответ: б)*

в) Использование цифр
г) Хранение в зашифрованном виде

11. Вставьте пропущенное слово:
Атака, направленная на переполнение буфера и выполнение произвольного кода, называется _____.
*(Правильный ответ: buffer overflow / переполнение буфера)*
12. Вставьте пропущенное слово:
Протокол _____ используется для защищённой передачи гипертекста (HTTP over TLS).
*(Правильный ответ: HTTPS)*
13. Вставьте пропущенное слово:
Свойство информации, означающее её доступность только авторизованным пользователям, называется _____.
*(Правильный ответ: конфиденциальность / confidentiality)*
14. Вставьте пропущенное слово:
Система, предназначенная для обнаружения вторжений в сеть, обозначается аббревиатурой _____.
*(Правильный ответ: IDS)*
15. Вставьте пропущенное слово:
Утилита _____ является стандартным инструментом для сканирования портов и определения сервисов в сети.
*(Правильный ответ: Nmap)*

1. Установите соответствие между типом атаки и её описанием:

| Тип атаки | Описание |
|---|---|
| 1. DoS | А) Атака с целью сделать ресурс недоступным для легитимных пользователей |
| 2. MITM | Б) Перехват и, возможно, изменение трафика между двумя узлами |
| 3. SQL-инъекция | В) Внедрение вредоносного SQL-кода в поля ввода веб-приложения |
| 4. XSS | Г) Внедрение вредоносного скрипта в веб-страницу, просматриваемую жертвой |

*Правильный ответ: 1-А, 2-Б, 3-В, 4-Г*

17. Установите соответствие между протоколом VPN и его характеристикой:

| Протокол | Характеристика |
|---|---|
| 1. PPTP | А) Устаревший, имеет известные уязвимости |
| 2. L2TP/IPsec | Б) Обеспечивает хорошую безопасность, но сложен в настройке |

| Протокол | Характеристика |
|---|---|
| 3. OpenVPN | В) Гибкий, с открытым исходным кодом, использует SSL/TLS |
| 4. WireGuard | Г) Современный, высокопроизводительный, минималистичный |

*Правильный ответ: 1-А, 2-Б, 3-В, 4-Г*

18. Установите соответствие между моделью контроля доступа и её принципом:

| Модель | Принцип |
|---|---|
| 1. DAC | А) Владелец объекта сам определяет права доступа к нему |
| 2. MAC | Б) Доступ определяется на основе меток безопасности и централизованных правил |
| 3. RBAC | В) Права доступа назначаются на основе ролей пользователей в организации |

*Правильный ответ: 1-А, 2-Б, 3-В*

19. Установите соответствие между инструментом и его назначением:

| Инструмент | Назначение |
|---|---|
| 1. Wireshark | А) Анализатор сетевого трафика |
| 2. Nmap | Б) Сканер портов и обнаружение сервисов |
| 3. Metasploit | В) Фреймворк для тестирования на проникновение |
| 4. OWASP ZAP | Г) Сканер уязвимостей веб-приложений |

*Правильный ответ: 1-А, 2-Б, 3-В, 4-Г*

20. Установите соответствие между свойством безопасности и его описанием в модели CIA:

| Свойство | Описание |
|---|---|
| 1. Конфиденциальность | А) Гарантия того, что информация доступна только авторизованным субъектам |

| Свойство | Описание |
|---|---|
| 2. Целостность | Б) Гарантия того, что информация не была изменена несанкционированно |
| 3. Доступность | В) Гарантия того, что информация доступна авторизованным субъектам по требованию |

*Правильный ответ: 1-А, 2-Б, 3-В*

21. Расположите этапы тестирования на проникновение в правильном порядке:

1. Получение доступа (Exploitation)
2. Сбор информации (Reconnaissance)
3. Сканирование и анализ (Scanning)
4. Составление отчёта (Reporting)
   *(Правильный ответ: 2 → 3 → 1 → 4)*

22. Расположите уровни модели OSI в порядке от физического к прикладному:

1. Сетевой (Network)
2. Канальный (Data Link)
3. Физический (Physical)
4. Транспортный (Transport)
   *(Правильный ответ: 3 → 2 → 1 → 4)*

23. Расположите методы аутентификации в порядке возрастания их надёжности (от наименее к наиболее надёжному):

1. Парольная аутентификация
2. Двухфакторная аутентификация (пароль + SMS)
3. Биометрическая аутентификация + аппаратный токен
   *(Правильный ответ: 1 → 2 → 3)*

24. Расположите поколения межсетевых экранов в хронологическом порядке их появления:

1. Пакетные фильтры
2. Stateful inspection firewalls
3. Application-level gateways (прокси)
4. Next-Generation Firewalls (NGFW)
   *(Правильный ответ: 1 → 3 → 2 → 4)*

25. Расположите стандарты безопасности Wi-Fi в порядке возрастания их криптостойкости:

1. WEP
2. WPA
3. WPA2
4. WPA3
   *(Правильный ответ: 1 → 2 → 3 → 4)*

26. Какая из перечисленных атак относится к классу атак на доступность?
    а) SQL-инъекция
    б) DDoS *(Правильный ответ: б)*

в) Межсайтовый скриптинг (XSS)
г) Фишинг

27. Какой порт по умолчанию используется для HTTPS?
    а) 80
    б) 443 *(Правильный ответ: б)*
    в) 22
    г) 21
28. Какой алгоритм шифрования является асимметричным?
    а) AES
    б) 3DES
    в) RSA *(Правильный ответ: в)*
    г) ChaCha20
29. Что такое фишинг?
    а) Атака на переполнение буфера
    б) Массовая рассылка писем с целью получения конфиденциальной информации *(Правильный ответ: б)*
    в) Сканирование портов
    г) Подбор пароля методом перебора
30. Какой протокол используется для управления сетевыми устройствами, но передаёт данные в открытом виде и не рекомендуется к использованию?
    а) SSH
    б) SNMPv3
    в) Telnet *(Правильный ответ: в)*
    г) RDP

### 1.3 Задания

1. Провести сканирование сети с помощью Nmap, выявить открытые порты и уязвимые сервисы. Составить отчёт с рекомендациями по устранению рисков.
2. Настроить межсетевой экран с помощью iptables/nftables. Заблокировать нежелательный трафик (ICMP, попытки брутфорса SSH), настроить логирование подозрительных подключений.
3. С помощью OWASP ZAP проверить тестовое веб-приложение на уязвимости (SQL-инъекции, XSS). Проанализировать результаты и предложить меры защиты.
4. Смоделировать атаку типа «человек посередине» (MITM) с использованием Ettercap. Настроить защиту через VPN или HTTPS и проверить её эффективность.
5. Провести аудит безопасности ОС Linux/Windows на соответствие стандартам CIS Benchmark. Выявить слабые места в конфигурации, отключить ненужные службы, настроить SELinux/AppArmor.
6. Написать скрипт на Python для проверки сложности паролей пользователей на основе заданной политики (длина, наличие цифр, спецсимволов).
7. Создать самоподписанный SSL/TLS сертификат и настроить веб-сервер (Apache/Nginx) на работу по HTTPS.
8. Проанализировать дамп сетевого трафика в Wireshark, выявить подозрительную активность (сканирование портов, попытки эксплуатации).
9. Настроить VPN-сервер на базе OpenVPN или WireGuard, проверить подключение клиента и защищённость канала.
10. Реализовать простой межсетевой экран на Python с использованием библиотеки scapy, фильтрующий пакеты по IP-адресам и портам.
11. Разработать политику информационной безопасности для малого предприятия (описать основные разделы: управление доступом, защита данных, реагирование на инциденты).
12. Провести анализ защищённости веб-приложения с использованием инструмента Nikto.

13. Настроить брандмауэр Windows в режиме повышенной безопасности: создать правила для разрешения только определённых входящих подключений.
14. Используя утилиту fail2ban, настроить защиту SSH-сервера от брутфорс-атак.
15. Проверить стойкость паролей с помощью утилиты john the ripper или hashcat на примере хешей из тестового файла.
16. Написать эссе на тему «Этические и правовые аспекты тестирования на проникновение».
17. Составить чек-лист для аудита безопасности беспроводной точки доступа (Wi-Fi).
18. Провести анализ журналов событий Windows/Linux на предмет обнаружения следов вторжения.
19. Разработать скрипт для мониторинга целостности критических системных файлов (например, с использованием хеш-сумм).
20. Настроить на маршрутизаторе правила NAT и проброса портов, оценить влияние на безопасность сети.
21. Сравнить функциональность и безопасность протоколов удалённого доступа RDP, VNC, TeamViewer.
22. Создать ловушку (honeypot) на базе Cowrie для эмуляции SSH-сервера и анализа действий злоумышленников.
23. Провести тестирование на проникновение методом социальной инженерии (симулированная фишинговая рассылка с согласия руководства) и анализ результатов.
24. Настроить централизованный сбор логов с нескольких серверов с использованием syslog-ng или rsyslog.
25. Реализовать программу для шифрования/дешифрования файлов с использованием алгоритма AES в режиме CBC.
26. Создать и подписать цифровую подпись для файла с использованием GPG.
27. Исследовать уязвимость CVE-XXXX-XXXX (по указанию преподавателя) и продемонстрировать способ эксплуатации на виртуальном стенде.
28. Написать правила для Snort или Suricata для обнаружения атак на веб-сервер (например, попытки SQL-инъекций).
29. Провести анализ защищённости базы данных MySQL/PostgreSQL с помощью специализированного сканера (например, sqlmap).
30. Разработать план реагирования на инцидент информационной безопасности (на примере заражения вирусом-шифровальщиком).

## 2. КРИТЕРИИ ОЦЕНИВАНИЯ ПРИ ПРОВЕДЕНИИ ТЕКУЩЕГО КОНТРОЛЯ

| Вид контроля | Наименование работы | Наименование оценочных средств | Шкала оценивания |
|---|---|---|---|
| Текущий контроль | Вопросы для обсуждения на занятиях;<br>Устные опросы по ранее изученному материалу;<br>Письменные работы: рефераты, тестовые задания;<br>Практические задания;<br>Рефераты и доклады по темам (вопросам), вынесенным на самостоятельную работу. | Оценка выступлений на практическом (семинарском) занятии, проверка заданий, устный опрос, оценивание докладов, рефератов | отлично<br>хорошо<br>удовлетворительно<br>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. |
| удовлетво-рительно | 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. |
| неудовлет-ворительно | оценивается ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа. |

**Критерии оценивания работы обучающихся на семинарских занятиях**

| Шкала оценивания | Показатели | Критерии |
|---|---|---|

| 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);<br>4. Правильность ответов на вопросы;<br>5. Самостоятельность решения (владение дополнительным материалом);<br>6. Знание нормативно-законодательной базы и терминологии курса | 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 | | 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. |
| Удовлетво-рительно | | 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. |
| Неудовлет-ворительно | | 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 объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы. | отлично |

| | | |
|---|---|---|
| | Реферат раскрывает поднятую проблематику в полном объеме. | |
| | Основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.<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. | удовлетвори тельно |
| | 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. | неудовлетво рительно |

**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 к экзамену;
- практические задания экзамена.

| Коды компетенции | Результаты освоения ОПОП | Перечень планируемых результатов обучения по дисциплине |
|---|---|---|
| **ПК-1** | Способен разрабатывать компоненты системных программных продуктов и программное обеспечение | ПК-1.1. Знать: принципы и методы разработки программного обеспечения, работы компиляторов, сетевых служб, операционных систем, драйверов и т.д.<br>ПК-1.2. Уметь: разрабатывать программное обеспечение и системные программные продукты, в том числе сетевые службы, отдельный модули операционной системы, драйверы и т.д.<br>ПК-1.3. Владеть: навыками системного |

| | | |
|---|---|---|
| | | программирования |

### 3.1 Вопросы к экзамену

31. Понятия информация, информатизация, информационная система, информационная безопасность.
32. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене
33. Защита информации, тайна, средства защиты информации.
34. Показатели информации: важность, полнота, адекватность, релевантность, толерантность.
35. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.
36. Идентификация, аутентификация и авторизация: определения, различия, примеры реализации.
37. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
38. Структура государственной системы информационной безопасности.
39. Доктрина информационной безопасности Российской Федерации.
40. Понятие угрозы. Виды противников или «нарушителей».
41. Классификация угроз информационной безопасности. Виды угроз. Основные нарушения.
42. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз.
43. Основные положения теории информационной безопасности информационных систем.
44. Системы обнаружения и предотвращения вторжений (IDS/IPS): принципы работы, виды (сетевые, хостовые), методы анализа.
45. Модели безопасности и их применение.
46. Формальные модели безопасности. Дискреционная модель Харрисона-Руззо-Ульмана.
47. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant.
48. Мандатная модель Белла-Ла-Падулы. Ролевая политика безопасности.
49. Уязвимости веб-приложений: SQL-инъекции, межсайтовый скриптинг (XSS), CSRF.
50. Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от НСД.
51. Методы криптографии. Симметричное и асимметричное шифрование.
52. Социальная инженерия: определение, виды атак (фишинг, претекстинг, услуга за услугу), методы противодействия.
53. Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи.
54. Безопасность операционных систем: механизмы защиты (разграничение доступа, аудит), средства усиления (SELinux, AppArmor).
55. Безопасность беспроводных сетей: уязвимости протоколов WEP, WPA, WPA2; преимущества WPA3.
56. Криптографические генераторы случайных чисел.
57. Способы распространения ключей. Обеспечиваемая шифром степень защиты.
58. Анализаторы сетевого трафика (снифферы): назначение, примеры (Wireshark, tcpdump), методы защиты от перехвата трафика.
59. Системы централизованного сбора и анализа событий безопасности (SIEM): архитектура, функции.
60. Основные технологии построения защищенных экономических информационных систем. Функции защиты информации.
61. Ядро и ресурсы средств защиты информации. Стратегии защиты информации.
62. Оценка защищённости: аудит безопасности, тестирование на проникновение, анализ уязвимостей.

63. Межсетевые экраны. Проектирование МЭ.
64. Инструменты для анализа защищённости: сканеры уязвимостей (Nessus, OpenVAS), фреймворки (Metasploit).
65. Управление уязвимостями: жизненный цикл, приоритезация, Patch Management.
66. Антивирусная защита: принципы работы, виды антивирусов (сигнатурные, эвристические, поведенческие).
67. Защита от вредоносного ПО: классификация вредоносных программ (вирусы, черви, трояны, руткиты, шифровальщики).
68. Ботнеты: структура, способы управления, использование в кибератаках.
69. Атаки на сервера. Атаки на рабочие станции. Атака типа «отказ в обслуживании»..
70. Безопасность облачных вычислений: модели ответственности, основные риски, средства защиты.
71. Контейнеризация и безопасность: особенности защиты Docker, Kubernetes.
72. Безопасность электронной почты: протоколы SPF, DKIM, DMARC для защиты от спуфинга и фишинга.
73. Защита DNS: атаки (спуфинг, отравление кэша), DNSSEC.
74. Управление доступом к сетевым устройствам: протоколы AAA (RADIUS, TACACS+).
75. Сетевое сегментирование и микросегментация как методы повышения безопасности.
76. Изоляция трафика: VLAN, приватные VLAN, VXLAN.
77. Туннелирование и инкапсуляция: GRE, IPsec, VXLAN.
78. Безопасность протоколов маршрутизации: защита OSPF, BGP.
79. Безопасность IPv6: особенности и угрозы по сравнению с IPv4.
80. Физическая безопасность сетевой инфраструктуры: контроль доступа, защита от перехвата.
81. Инсайдерские угрозы: виды, методы выявления и предотвращения.
82. Управление инцидентами ИБ: этапы реагирования (подготовка, обнаружение, сдерживание, ликвидация, восстановление, анализ).
83. Цифровая криминалистика (форензика): цели, этапы, инструменты.
84. Резервное копирование и восстановление данных как элемент обеспечения доступности.
85. Катастрофоустойчивость и планирование непрерывности бизнеса (BCP/DRP).
86. Принципы построения защищённых сетей: глубокая эшелонированная защита (Defense in Depth).
87. Концепция Zero Trust Network Access (ZTNA): основные принципы.
88. Безопасность промышленных сетей (АСУ ТП): особенности, протоколы (Modbus, Profinet), угрозы.
89. Безопасность Интернета вещей (IoT): проблемы, методы защиты.
90. Этика в области информационной безопасности. Правовые аспекты деятельности специалиста по ИБ.

### 3.2 Практические задания к экзамену

1. **Задание «Сканирование сети с помощью Nmap».**
   Выполнить сканирование указанного преподавателем диапазона IP-адресов, определить открытые порты, версии сервисов и ОС. Составить краткий отчёт.
2. **Задание «Настройка межсетевого экрана iptables».**
   Создать набор правил для iptables, разрешающий только входящие SSH, HTTP, HTTPS и блокирующий всё остальное. Продемонстрировать работу правил.
3. **Задание «Анализ трафика в Wireshark».**
   Открыть предоставленный pcap-файл, найти в нём попытку аутентификации по FTP и восстановить логин/пароль. Объяснить, как защититься от подобного перехвата.

4. **Задание «Поиск уязвимостей веб-приложения с OWASP ZAP».**
   Запустить сканирование тестового веб-приложения (например, DVWA), выявить уязвимости, классифицировать их по степени риска, предложить меры по устранению.
5. **Задание «Моделирование MITM-атаки и защита».**
   В виртуальной среде с помощью Ettercap продемонстрировать перехват HTTP-трафика. Затем настроить HTTPS для веб-сервера и показать, что трафик стал нечитаемым.
6. **Задание «Аудит ОС на соответствие CIS Benchmark».**
   С помощью скрипта или вручную проверить несколько пунктов CIS Benchmark для Linux (например, срок действия паролей, разрешения на файлы). Выписать несоответствия.
7. **Задание «Создание самоподписанного сертификата».**
   Сгенерировать самоподписанный SSL/TLS сертификат с помощью OpenSSL, настроить Apache/Nginx на его использование. Проверить подключение браузером.
8. **Задание «Настройка OpenVPN сервера».**
   Установить и настроить OpenVPN сервер в режиме «точка-точка», создать клиентский конфигурационный файл, проверить соединение и шифрование трафика.
9. **Задание «Блокировка brute-force атак с fail2ban».**
   Настроить fail2ban для защиты SSH сервера: установить порог неудачных попыток и время бана. Продемонстрировать блокировку IP-адреса.
10. **Задание «Анализ защищённости БД с sqlmap».**
    На тестовом уязвимом приложении с помощью sqlmap обнаружить SQL-инъекцию, получить список баз данных. Объяснить, как исправить уязвимость.
11. **Задание «Настройка Honeypot Cowrie».**
    Установить и запустить Cowrie на нестандартном порту, залогировать попытку подключения, проанализировать действия злоумышленника (введённые команды).
12. **Задание «Написание правила для Snort».**
    Написать правило Snort для обнаружения попытки доступа к файлу `/etc/passwd` через веб-сервер. Проверить срабатывание правила.
13. **Задание «Проверка сложности паролей с John the Ripper».**
    Получить хеш пароля (из тестового файла) и попытаться восстановить его с помощью словарной атаки в John the Ripper. Оценить время подбора.
14. **Задание «Настройка централизованного сбора логов».**
    Настроить rsyslog на клиенте для отправки логов на центральный сервер. Проверить поступление сообщений.
15. **Задание «Создание GPG ключа и подпись файла».**
    Сгенерировать пару GPG ключей, подписать файл, экспортировать открытый ключ и проверить подпись на другой машине.
16. **Задание «Настройка брандмауэра Windows».**
    Через графический интерфейс или PowerShell создать правило, разрешающее входящий RDP только с определённого IP-адреса.
17. **Задание «Мониторинг целостности файлов с AIDE».**
    Инициализировать базу данных AIDE, изменить один из отслеживаемых файлов, выполнить проверку и найти изменения.
18. **Задание «Анализ дампа памяти с volatility».**
    Используя фреймворк Volatility, проанализировать предоставленный дамп памяти Windows, найти запущенные процессы и сетевые соединения.
19. **Задание «Поиск уязвимостей с Nikto».**
    Запустить Nikto против тестового веб-сервера, интерпретировать полученные результаты.
20. **Задание «Эксплуатация уязвимости с Metasploit».**
    Найти подходящий эксплойт для уязвимой службы (например, vsftpd 2.3.4) в Metasploit, провести эксплуатацию и получить сессию meterpreter.

21. **Задание «Настройка VLAN для изоляции трафика».**
    На управляемом коммутаторе (или в эмуляторе) создать два VLAN, настроить порты доступа и транк, проверить изоляцию трафика между VLAN.
22. **Задание «Создание DMZ на базе iptables».**
    С помощью iptables организовать демилитаризованную зону: разрешить доступ извне к веб-серверу в DMZ, но запретить доступ из DMZ во внутреннюю сеть.
23. **Задание «Анализ безопасности заголовков HTTP».**
    Проверить заданный веб-сайт на наличие security-заголовков (HSTS, CSP, X-Frame-Options и др.) и написать рекомендации по их внедрению.
24. **Задание «Настройка DNS over HTTPS (DoH)».**
    Настроить браузер или системный резолвер на использование DoH для шифрования DNS-запросов. Проверить с помощью Wireshark.
25. **Задание «Разработка скрипта для проверки открытых портов».**
    Написать на Python скрипт, который принимает IP-адрес и список портов, и проверяет их доступность (аналог простого сканера портов).
26. **Задание «Шифрование файла с помощью AES».**
    Написать программу (на Python с использованием PyCryptodome), которая шифрует и расшифровывает файл алгоритмом AES-256 в режиме GCM.
27. **Задание «Анализ фишингового письма».**
    Изучить предоставленное фишинговое письмо, определить признаки фишинга (адрес отправителя, ссылки, вложения), объяснить механизм обмана.
28. **Задание «Настройка двухфакторной аутентификации SSH».**
    Настроить SSH сервер для аутентификации с помощью ключа и одноразового пароля (Google Authenticator).
29. **Задание «Составление плана реагирования на инцидент».**
    На основе предложенного сценария (например, заражение шифровальщиком) составить краткий план реагирования, указав основные шаги и ответственных.
30. **Задание «Аудит конфигурации сетевого устройства».**
    Проверить конфигурацию маршрутизатора (Cisco/HP) на предмет соответствия базовым требованиям безопасности (отключение ненужных сервисов, настройка паролей, SSH вместо Telnet).

## 4. КРИТЕРИИ ОЦЕНИВАНИЯ ПРИ ПРОВЕДЕНИИ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

### Шкала оценивания уровня сформированности компетенций (по пятибалльной системе) экзамен

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

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

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

Вид промежуточной аттестации – экзамен.

Форма проведения промежуточной аттестации – письменный экзамен.