Ассоциация научно-технических организаций "Уральский профессиональный форум"
Автономная некоммерческая профессиональная образовательная организация
"Современный цифровой колледж при Западно-Уральском институте экономики и права"
(АНПОО "СЦК при ЗУИЭП")

РАССМОТРЕНО
на заседании Педагогического совета
протокол от «16» февраля 2026 г.
№ 4

УТВЕРЖДАЮ:
Директор АНПОО СЦК при ЗУИЭП"

_____ А.С. Волков
«16» февраля 2026 г.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ТЕКУЩЕГО КОНТРОЛЯ
И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ
МДК.03.03 Технологии безопасности ИТ-инфраструктуры

по специальности
09.02.11 Разработка и управление программным обеспечением
квалификация «Программист»

форма обучения: заочная

форма промежуточной аттестации: дифференцированный зачет

Пермь 2026

СОДЕРЖАНИЕ

1. ПАСПОРТ ОЦЕНОЧНЫХ МАТЕРИАЛОВ

1.1. Общая характеристика оценочных материалов.

Оценочные материалы предназначен для контроля и оценки результатов освоения междисциплинарного курса МДК.03.03 Технологии безопасности ИТ-инфраструктуры, входящего в ПМ.03 Конфигурирование, управление, и мониторинг ИТ-инфраструктуры специальности СПО 09.02.11 Разработка и управление программным обеспечением.

Оценочные материалы состоит из оценочных материалов текущего контроля и контрольно-измерительных материалов промежуточной аттестации.

Характеристика текущего контроля

Целью текущего контроля является контроль запланированных по дисциплине знаний и умений. Текущий контроль по дисциплине проводится в следующих формах: тестирование, практическое занятие и других формах.

Текущий контроль проводится в соответствии с рабочей программой по дисциплине и структурных элементов электронного курса в СДО. Периодичность проведения текущего контроля зависит от сроков выполнения заданий обучающимися в пределах установленного учебным планом семестра.

Текущий контроль проводится только с помощью электронного обучения и дистанционных образовательных технологий. Текущий контроль включает в себя оценку выполнения практической работы и тестирования по каждому разделу тематического плана учебной дисциплины. Порядок проведения текущего контроля определяется оценочными средствами.

Характеристика промежуточной аттестации

Целью контроля промежуточной аттестации является контроль освоения запланированных по дисциплине знаний и умений. Форма промежуточной аттестации: экзамен. Промежуточная аттестация с помощью электронного обучения и дистанционных образовательных технологий.

Контрольно-измерительные материалы промежуточной аттестации состоят из:

1) теоретической части, которая выполняется письменно при проведении промежуточной аттестации обучающихся с применением дистанционных образовательных технологий, представляет собой ответ на теоретический вопрос по программе курса;

2) тестовой части, которая выполняется письменно и включает в себя:

- задание типа А (базовый уровень) - 10 тестовых вопросов с 4 вариантами ответов;
- задание типа В (задания повышенной сложности) - 2 задания с 4 вариантами ответов;
- задание типа С (практико-ориентированное комплексное задание) - 1 задание с 4 вариантами ответов.

Первая часть (А) теста включает 10 заданий базового уровня сложности. Данные задания направлены на выявление сформированности полученных в ходе изучения дисциплины базовых знаний, соответствующих заданным стандартом компетенциям. Каждое тестовое задание данной части содержит 4 варианта ответов, один или несколько из которых является правильным.

Вторая часть (В) теста состоит из 2 заданий повышенного уровня сложности. Данные задания направлены на выявление усвоения основных алгоритмов профессиональной деятельности, соответствующих заданным стандартом компетенциям.

Практическая часть (С) состоит из 1 практико-ориентированного задания повышенного уровня сложности (задачи, ситуации).

Для каждого варианта теста подготовлены эталоны ответов для проверки

результатов теста.

Данные задания направлены на выявление уровня сформированности опыта практической деятельности, соответствующего заданным стандартом компетенциям, и выполняются с учетом смоделированной ситуации.

1.2. Требования к результатам освоения учебной дисциплины

Код ОК, ПК	**Уметь**	**Знать**
ОК.01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности
ОК.02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации, современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств
ОК.03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях	содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования; основы предпринимательской деятельности; основы финансовой грамотности; правила разработки бизнес-планов; порядок выстраивания презентации; кредитные банковские продукты
ОК.04	Эффективно взаимодействовать и работать в коллективе и команде	психологические основы деятельности коллектива, психологические особенности личности; основы проектной деятельности
ОК.05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	особенности социального и культурного контекста; правила оформления документов и построения устных сообщений

ОК.06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	сущность гражданско-патриотической позиции, общечеловеческих ценностей; значимость профессиональной деятельности по специальности; стандарты антикоррупционного поведения и последствия его нарушения
ОК.07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения; принципы бережливого производства; основные направления изменения климатических условий региона
ОК.09	Пользоваться профессиональной документацией на государственном и иностранном языках	правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности
ПК 3.7.	− обеспечивать безопасность во всех этапах DevOps-процесса; − выявлять и устранять уязвимости и потенциальные угрозы; − реагировать на инциденты и проводить расследования; − анализировать уязвимости и риски в ИТ-инфраструктуре и веб-приложениях; − разрабатывать и реализовывать меры безопасности для защиты ИТ-инфраструктуры и веб-приложений; мониторить и обнаруживать инциденты безопасности, а также реагировать на них	− основы безопасности приложений и инфраструктуры; − методы анализа на уязвимости и мониторинга безопасности; − основные принципы и методы обеспечения безопасности ИТ-инфраструктуры и веб-приложений; − различные уязвимости и угрозы безопасности, а также способы их предотвращения и обнаружения; инструменты и технологии для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы.

2. КОМПЛЕКТ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ

2.1 Примерная тематика практических заданий

Задача 1. Анализ уязвимостей в конфигурации веб-сервера
В вашей команде развернут веб-сервер на базе Apache 2.4.29, работающий под Linux. При аудите безопасности выяснилось, что:

- Сервер отвечает с заголовком Server: Apache/2.4.29 (Ubuntu);
- Директория /backup доступна по прямой ссылке извне;
- Учётная запись admin имеет пароль admin123.

Вопросы:

1. Какие уязвимости вы можете выделить?
2. Какие меры безопасности вы предложите для устранения каждого из рисков?
3. Какой инструмент можно использовать для автоматического сканирования таких уязвимостей?

Задача 2. Настройка брандмауэра для DevOps-среды
Вы настраиваете сервер в CI/CD-пайплайне. На нём работает:

- Веб-приложение на порту 80 и 443;
- GitLab Runner на порту 8080;
- SSH-доступ для администраторов.

Задание:
Составьте правила для брандмауэра ufw (Linux), чтобы:

- Разрешить входящие подключения только с доверенных IP-адресов для порта 8080;
- Разрешить HTTP и HTTPS для всех;
- Ограничить SSH-доступ только с IP-адреса вашей команды (например, 192.168.1.100);
- Запретить всё остальное.

Приведите команды для настройки.

Задача 3. Обнаружение и анализ инцидента безопасности
При мониторинге логов сервера вы обнаружили следующие строки в файле /var/log/auth.log:

- Failed password for root from 195.14.88.123 port 22 ssh2
- Failed password for root from 195.14.88.123 port 22 ssh2
- ...
- Accepted password for root from 195.14.88.123 port 22 ssh2

Задание:

1. Какой тип атаки мог произойти?
2. Какие действия вы предпримете немедленно после обнаружения этого инцидента?
3. Какие меры можно было бы применить заранее, чтобы предотвратить подобное?

Задача 4. Безопасность в DevOps: безопасный CI/CD пайплайн
Вы разрабатываете CI/CD-процесс с использованием GitLab CI. В одном из шагов пайплайна выполняется:

yaml Переносить Свернуть Копировать

```yaml
script:
  - echo "DB_PASSWORD=supersecret" >> .env
  - docker build -t myapp .
```

Задание:

1. Какие риски безопасности содержит данный фрагмент?
2. Как можно безопасно передавать секреты (например, пароли) в пайплайн?
3. Какие инструменты (внутри GitLab или сторонние) помогут защитить конфиденциальные данные?

Задача 5. Сканирование веб-приложения на уязвимости
Вы тестируете веб-приложение, в котором есть форма входа:

html Переносить Свернуть Копировать

```html
<form action="/login" method="GET">
  <input type="text" name="username">
  <input type="password" name="password">
  <input type="submit">
</form>
```

Задание:

1. Какой потенциальный риск содержит использование метода GET для отправки логина и пароля?
2. Какой тип атаки может быть реализован через эту форму (например, при отсутствии фильтрации ввода)?
3. Какой инструмент (например, OWASP ZAP или Burp Suite) можно использовать для тестирования на такую уязвимость?

Задача 6. Мониторинг и реагирование с помощью IDS
В вашей ИТ-инфраструктуре установлен Suricata — система обнаружения вторжений. Вы получили оповещение:

[**1:2001219:1**] ET WEB_SERVER SQL Injection Attempt [**Classification**: Attempted Information Leak] [**Priority**: 2]

Задание:

1. Что означает данное предупреждение?
2. Какие действия вы предпримете при получении такого алерта?
3. Как можно настроить автоматическое реагирование на подобные события (например, блокировку IP)?

2.2 Задания в тестовой форме

Тестовые задания типа А (Необходимо выбрать один наиболее правильный ответ из нескольких предложенных вариантов)

1. Какой из перечисленных элементов чаще всего используется для защиты перим етра ИТ-инфраструктуры?
a) Антивирусная утилита
b) Система резервного копирования
c) Брандмауэр
d) Менеджер паролей
2. Какой метод аутентификации считается наиболее безопасным при доступе к Dev Ops-среде?
a) Пароль из 8 символов
b) Пароль, хранящийся в текстовом файле
c) Двухфакторная аутентификация (2FA)
d) Общий пароль для всей команды
3. Что такое уязвимость типа XSS?
a) Атака на базу данных через SQL-запросы
b) Переполнение буфера памяти
c) Внедрение вредоносного JavaScript-кода в веб-страницу
d) Подмена IP-адреса в сети
4. Какой инструмент чаще всего используется для автоматизированного сканиров ания уязвимостей в веб-приложениях?
a) Wireshark
b) OWASP ZAP
c) Notepad++
d) Task Manager
5. Какой порт по умолчанию используется для защищённого SSH-доступа?
a) 80
b) 443
c) 22
d) 8080
6. Что означает принцип «наименьших привилегий» в ИБ?
a) Все пользователи получают админ-доступ для удобства
b) Пользователи могут менять настройки системы
c) Пользователи получают только те права, которые необходимы для выполнения задач
d) Администраторы не должны использовать пароли
7. Какой тип атаки происходит при попытке подбора пароля методом перебора?
a) XSS
b) SQL-инъекция
c) Брутфорс
d) Фишинг
8. Какой протокол обеспечивает шифрование трафика между веб-браузером и сервером?
a) HTTP
b) FTP
c) HTTPS
d) Telnet
9. Что такое IDS (Intrusion Detection System)?
a) Инструмент для шифрования файлов
b) Программа для резервного копирования
c) Система обнаружения вторжений, анализирующая сетевой трафик на признаки атак
d) Антивирус для мобильных устройств
10. Какой из следующих подходов помогает защитить конфиденциальные данные в CI/CD-пайплайне?

a) Хранение паролей в скриптах в открытом виде
b) Использование .env-файлов в репозитории Git
c) Применение секрет-менеджеров (например, GitLab CI Variables)
d) Передача паролей по электронной почте
11. Что такое DevSecOps?
a) Удаление всех тестов из пайплайна
b) Отдельная команда, отвечающая только за разработку
c) Интеграция мер безопасности на всех этапах DevOps-процесса
d) Использование только Linux-серверов
12. Какой из следующих файлов НЕ должен находиться в открытом репозитории Git?
a) README.md
b) Dockerfile
c) config.json с учётными данными базы данных
d) index.html
13. Какой тип атаки использует поддельные веб-сайты для кражи логинов и паролей?
a) DDoS
b) Фишинг
c) XSS
d) Переполнение буфера
14. Что такое SQL-инъекция?
a) Внедрение вредоносного SQL-кода через поля ввода формы
b) Шифрование базы данных
c) Удаление пользователей из системы
d) Подключение к базе данных через SSH
15. Какой инструмент используется для анализа сетевого трафика?
a) Photoshop
b) Excel
c) Wireshark
d) Notepad
16. Какой из перечисленных методов помогает предотвратить утечку данных при утере устройства?
a) Установка ярлыков на рабочем столе
b) Использование простых паролей
c) Шифрование диска (например, BitLocker или LUKS)
d) Отключение Wi-Fi
17. Что такое CVE?
a) Протокол шифрования
b) Тип вредоносного ПО
c) База данных общих уязвимостей и угроз
d) Система резервного копирования
18. Какой из следующих подходов используется для регулярного выявления уязвимостей в системе?
a) Ежедневная перезагрузка сервера
b) Отключение антивируса
c) Проведение регулярных сканирований уязвимостей
d) Удаление логов каждую неделю
19. Какой уровень модели OSI отвечает за шифрование данных?
a) Физический
b) Канальный
c) Сеансовый / Прикладной (в зависимости от реализации, например, TLS)
d) Сетевой

20. Что такое DDoS-атака?
a) Кража паролей через фишинг
b) Внедрение вредоносного кода в приложение
c) Массированная отправка запросов для перегрузки сервера
d) Подмена MAC-адреса
21. Какой из следующих инструментов является системой предотвращения вторжений (IPS)?
a) 7-Zip
b) VLC Media Player
c) Snort в режиме предотвращения
d) Paint
22. Какой из принципов безопасности подразумевает возможность отследить действия пользователя?
a) Конфиденциальность
b) Целостность
c) Отслеживаемость (аудит)
d) Доступность
23. Что такое «белое пятно» в контексте безопасности?
a) Область с высокой защитой
b) Успешно пройденный тест на проникновение
c) Участок системы, который не охвачен мониторингом или защитой
d) Лицензированный антивирус
24. Какой из следующих паролей наиболее безопасен?
a) 12345678
b) password
c) Tr0ub4dor&3_2025
d) qwerty
25. Какой протокол используется для безопасной передачи файлов?
a) HTTP
b) FTP
c) SFTP
d) Telnet
26. Что должен сделать администратор сразу после обнаружения взлома сервера?
a) Перезагрузить сервер и продолжить работу
b) Отключить антивирус
c) Изолировать систему и начать расследование инцидента
d) Удалить все логи
27. Какой из следующих подходов помогает защитить контейнеры в DevOps-среде?
a) Запуск всех контейнеров от имени root
b) Использование устаревших образов
c) Сканирование образов на уязвимости перед запуском (например, с помощью Trivy)
d) Отключение брандмауэра на хосте
28. Что такое лог-файл и зачем он нужен в ИБ?
a) Файл для хранения паролей
b) Временный файл для кеша
c) Журнал событий, используемый для анализа и расследования инцидентов
d) Файл для резервного копирования базы данных
29. Какой из следующих элементов является частью политики безопасности ИТ-инфраструктуры?
a) График обедов сотрудников
b) Список любимых сайтов

c) Требования к сложности паролей и частоте их смены
d) Цвет корпоративной формы
30. Какой из перечисленных инструментов используется для управления конфигу рациями и обеспечения их безопасности?
a) Microsoft Word
b) Google Chrome
c) Ansible
d) Calculator

3. КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

3.1 Вопросы для подготовки к экзамену

1. Что означает принцип «сдвиг влево» в контексте DevSecOps?
2. Какие преимущества даёт интеграция безопасности на ранних этапах разработки?
3. Назовите три ключевых принципа DevSecOps.
4. Как автоматизация проверок безопасности влияет на скорость и надёжность CI/CD-пайплайна?
5. Что такое культура ответственности за безопасность в DevOps-команде?
6. Какие этапы CI/CD подходят для внедрения автоматизированных проверок безопасности?
7. Как pre-commit хуки способствуют повышению безопасности кода?
8. В чём разница между SAST и DAST?
9. Что такое SCA и зачем он нужен в DevOps?
10. Какие уязвимости из OWASP Top 10 чаще всего обнаруживаются в веб-приложениях?
11. Назовите три инструмента для статического анализа кода (SAST) и кратко опишите их назначение.
12. Какие риски несёт использование устаревших или уязвимых библиотек в проекте?
13. Как инструменты вроде Snyk и Trivy помогают в управлении безопасностью зависимостей?
14. Что такое ложноположительный результат в сканировании кода и как с ним работать?
15. Какие механизмы изоляции используются в Linux для повышения безопасности контейнеров?
16. В чём разница между AppArmor и SELinux?
17. Как seccomp помогает защитить контейнеры от вредоносных системных вызовов?
18. Что означает минимизация attack surface, и как её достичь в контейнерной среде?
19. Какие практики безопасной настройки контейнеров вы знаете?
20. Какие инструменты используются для обнаружения несанкционированных изменений в файловой системе?
21. Почему опасно хранить пароли и токены в исходном коде или .env-файлах?
22. Как HashiCorp Vault обеспечивает безопасное управление секретами?
23. Что такое динамические секреты и в чём их преимущество перед статическими?
24. Как настраивается аутентификация и политики доступа в HashiCorp Vault?
25. Какие облачные альтернативы HashiCorp Vault существуют (например, в AWS, Azure)?
26. Зачем нужна ротация секретов, и как она реализуется автоматически?
27. Какие меры защиты используются на сетевом уровне (брандмауэры, IDS/IPS, VPN)?

28. В чём разница между IDS и IPS? Приведите примеры инструментов.
29. Какие механизмы обеспечивают безопасность API (аутентификация, rate limiting, CORS)?
30. Какие требования к безопасности предъявляют стандарты ISO/IEC 27001 и SOC 2, и как они реализуются в DevOps-среде?

3.2 Тестовые задания для промежуточной аттестации

Тестовые задания типа А

1. Что означает принцип «сдвиг влево» в DevSecOps?
a) Перенос тестирования на финальные этапы пайплайна
b) Упрощение документации
c) Внедрение проверок безопасности на самых ранних стадиях разработки
d) Увеличение количества ручных проверок
2. Какой из этапов CI/CD наиболее подходит для запуска SAST-инструментов?
a) После деплоя в продакшн
b) На этапе ручного тестирования
c) На этапе сборки (build)
d) Перед написанием кода
3. Какой инструмент позволяет выполнять проверки безопасности ещё до коммита кода?
a) Jenkins
b) Docker
c) pre-commit хуки с линтерами и сканерами
d) Grafana
4. Что из перечисленного является целью автоматизации безопасности в DevOps?
a) Увеличение времени на ручные проверки
b) Полное исключение разработчиков из процесса
c) Быстрое выявление уязвимостей без замедления пайплайна
d) Отключение всех тестов для ускорения сборки
5. Какой из подходов лучше всего способствует культуре безопасности в команде?
a) Назначение одного ответственного за безопасность
b) Скрытие информации об уязвимостях от разработчиков
c) Назначение «security champions» в каждой команде
d) Проведение аудитов раз в год
6. Что проверяет SAST (Static Application Security Testing)?
a) Работающее веб-приложение под нагрузкой
b) Сетевой трафик между сервисами
c) Исходный код на наличие уязвимостей без запуска приложения
d) Конфигурацию сервера
7. Какой тип анализа используется для поиска уязвимостей в сторонних библиотеках?
a) DAST
b) Fuzzing
c) SCA (Software Composition Analysis)
d) Penetration testing
8. Какой из перечисленных инструментов НЕ предназначен для анализа уязвимостей в зависимостях?
a) Snyk
b) Trivy

c) Wireshark
d) Dependabot
9. Какой из следующих пунктов входит в OWASP Top 10?
a) Использование Docker
b) Наличие комментариев в коде
c) Уязвимости в цепочке поставок ПО (Software and Data Integrity Failures)
d) Длительные имена переменных
10. Когда целесообразно запускать DAST-сканирование?
a) До написания первой строки кода
b) На этапе проектирования БД
c) После развертывания приложения в тестовой среде
d) В момент коммита в Git
11. Какой инструмент может интегрироваться в CI/CD и проверять код на стиль и безопасность?
a) Slack
b) SonarQube
c) Zoom
d) Notepad++
12. Что такое «ложноположительный результат» в SAST?
a) Уязвимость, которую не удалось обнаружить
b) Сообщение об уязвимости, которой на самом деле нет
c) Успешный запуск сканера
d) Отсутствие отчёта
13. Какой механизм используется для ограничения системных вызовов в контейнерах?
a) DNSSEC
b) OAuth
c) seccomp
d) TLS
14. Что такое AppArmor?
a) Протокол шифрования
b) Система резервного копирования
c) Модуль принудительного контроля доступа в Linux
d) Инструмент мониторинга CPU
15. Какой из следующих подходов минимизирует attack surface контейнера?
a) Запуск от имени root
b) Установка всех возможных пакетов
c) Использование минимального образа (например, alpine)
d) Отключение сетевого экрана
16. Какой инструмент позволяет обнаружить несанкционированные изменения в файловой системе?
a) curl
b) ping
c) AIDE (Advanced Intrusion Detection Environment)
d) top
17. Что такое SELinux?
a) Виртуальная машина от Microsoft
b) Система управления базами данных
c) Механизм принудительного контроля доступа в Linux
d) Протокол маршрутизации
18. Какая проблема возникает при хранении паролей в коде?
a) Увеличивается скорость загрузки приложения
b) Упрощается процесс тестирования

c) Риск утечки секретов при попадании кода в публичный репозиторий
d) Улучшается читаемость кода
19. Какой инструмент предоставляет динамические секреты и централизованное управление доступом?
a) GitLab CI
b) Docker Hub
c) HashiCorp Vault
d) Nginx
20. Что такое ротация секретов?
a) Изменение цветовой схемы интерфейса
b) Удаление всех пользователей
c) Регулярная смена паролей, токенов и ключей
d) Обновление версии ОС
21. Какой из сервисов является альтернативой HashiCorp Vault в облаке AWS?
a) AWS S3
b) AWS EC2
c) AWS Secrets Manager
d) AWS Lambda
22. Какой подход обеспечивает наименьшие привилегии при доступе к секретам?
a) Выдача полного доступа всем разработчикам
b) Хранение секретов в .env-файле
c) Настройка политик доступа в Vault на основе ролей
d) Отправка секретов по почте
23. На каком уровне модели OSI работает шифрование в TLS?
a) Физический
b) Сетевой
c) Сеансовый / Прикладной
d) Канальный
24. Что такое DNSSEC?
a) Протокол для ускорения DNS-запросов
b) Инструмент для блокировки рекламы
c) Механизм проверки подлинности DNS-ответов с помощью цифровых подписей
d) Вид вируса
25. Какой инструмент может автоматически блокировать IP-адреса после множества неудачных попыток входа?
a) Wireshark
b) Nmap
c) Fail2ban
d) curl
26. Что делает iptables?
a) Сканирует вирусы
b) Шифрует файлы
c) Управляет правилами межсетевого экрана в Linux
d) Анализирует логи в реальном времени
27. Какой инструмент используется для аудита системных событий в Linux?
a) htop
b) df
c) auditd
d) ps
28. Какой механизм используется для защиты API от чрезмерных запросов?
a) CORS без ограничений
b) Открытый доступ ко всем эндпоинтам

c) Rate limiting и throttling
d) Отключение аутентификации
29. Что такое SIEM?
a) Система управления проектами
b) Инструмент для рисования диаграмм
c) Система сбора, анализа и корреляции логов безопасности
d) Протокол передачи данных
30. Что включает postmortem-анализ после инцидента?
a) Скрытие информации о произошедшем
b) Увольнение ответственного сотрудника
c) Документирование причин, последствий и мер по предотвращению повторения
d) Перезапуск сервера без расследования

Тестовые задания типа B. (Установите соответствие между элементами)
Задание 1. Установите соответствие между методами тестирования безопасности и их описанием.

Метод	Описание
1. SAST	A. Тестирование работающего приложения на уязвимости
2. DAST	B. Анализ сторонних библиотек на наличие уязвимостей
3. SCA	C. Анализ исходного кода без запуска приложения
4. Penetration Testing	D. Имитация атаки злоумышленника для проверки защиты

Верный ответ:
1 — C
2 — A
3 — B
4 — D

Задание 2. Установите соответствие между инструментами и их назначением.

Инструмент	Назначение
1. SonarQube	A. Сканирование образов контейнеров на уязвимости
2. Trivy	B. Централизованное управление секретами
3. HashiCorp Vault	C. Статический анализ кода и проверка на безопасность
4. Fail2ban	D. Автоматическая блокировка IP после множества неудачных входов

Верный ответ:
1 — C
2 — A
3 — B
4 — D

Задание 3. Установите соответствие между механизмами безопасности Linux и их функцией.

Механизм	Функция

1. SELinux	A. Ограничение системных вызовов процесса
2. AppArmor	B. Принудительный контроль доступа на основе политик (Mandatory Access Control)
3. seccomp	C. Профиль безопасности на основе путей к файлам
4. auditd	D. Аудит системных событий и вызовов

Верный ответ:
1 — B
2 — C
3 — A
4 — D

Задание 4. Установите соответствие между компонентами DevSecOps и этапом CI/CD, на котором они применяются.

Компонент	Этап CI/CD
1. pre-commit хуки	A. После развертывания приложения
2. SAST-сканирование	B. На этапе сборки (build)
3. DAST-тестирование	C. До отправки кода в репозиторий
4. Ротация секретов	D. Периодически, в рамках эксплуатации

Верный ответ:
1 — C
2 — B
3 — A
4 — D

Задание 5. Установите соответствие между сервисами облака и их функцией безопасности.

Сервис	Функция
1. AWS CloudTrail	A. Обнаружение угроз с использованием машинного обучения
2. Azure Defender	B. Управление доступом и правами пользователей
3. AWS GuardDuty	C. Аудит всех API-вызовов в аккаунте AWS
4. IAM (в облаках)	D. Мониторинг аномальной активности в инфраструктуре

Верный ответ:
1 — C
2 — D
3 — A
4 — B

Задание 6. Установите соответствие между принципами безопасности и их описанием.

Принцип	Описание
1. Наименьшие привилегии	A. Все действия пользователей должны фиксироваться
2. Сдвиг влево (shift-left)	B. Пользователи получают только необходимые права

3. Аудит и отслеживаемость	C. Безопасность интегрируется на ранних этапах разработки
4. Ротация секретов	D. Регулярная смена паролей, ключей и токенов

Верный ответ:
1 — B
2 — C
3 — A
4 — D

Тестовые задания типа C. (Выбор правильного варианта ответа из предложенного списка)

1. Утечка токена в репозитории Git
Ситуация:
Студент разрабатывает приложение в GitLab. При публикации кода случайно в репозиторий попал файл .env с токеном доступа к облачному хранилищу:

env Переносить Свернуть Копировать

```
CLOUD_TOKEN=abc123xyz
```

Файл уже закоммичен и отправлен в ветку main. Токен даёт полный доступ к данным компании.

Что нужно сделать в первую очередь?
a) Оставить как есть — токен уже использован, и пересоздавать его сложно
b) Удалить файл из репозитория и сообщить только своему другу из команды
c) Немедленно отозвать токен в панели управления облаком, удалить файл из истории Git и настроить .gitignore
d) Переименовать файл в .env.bak, чтобы он больше не использовался

2. Подозрительная активность в логах сервера
Ситуация:
Вы администрируете веб-сервер. В логах /var/log/auth.log обнаружены сотни попыток входа по SSH с разных IP-адресов:

Переносить Свернуть Копировать

```
Failed password for root from 185.123.45.67
Failed password for admin from 185.123.45.67
...
```

Через некоторое время вход успешен:

Не переносить Свернуть Копировать

```
Accepted password for root from 185.123.45.67
```

Какое действие наиболее правильно?

a) Проигнорировать — возможно, это был легальный сотрудник
b) Сменить пароль от своего аккаунта и продолжить работу
c) Изолировать сервер, провести расследование, заблокировать IP и сменить все учётные данные
d) Перезагрузить сервер и удалить логи, чтобы скрыть следы

3. Запуск контейнера с избыточными привилегиями
Ситуация:
Разработчик запускает контейнер с командой:

bash Переносить Свернуть Копировать

```
docker run -d --privileged --name app myapp:latest
```

Приложение — простой веб-сервис, не требующий доступа к ядру или устройствам.

Какой риск возникает при таком запуске?

a) Контейнер будет работать медленнее
b) Приложение не сможет подключиться к базе данных
c) При компрометации приложения атакующий получит полный контроль над хост-системой
d) Docker-образ станет больше по размеру

4. Небезопасная передача данных через API
Ситуация:
Вы тестируете мобильное приложение, которое отправляет логин и пароль на сервер через API:

http Переносить Свернуть Копировать

```
POST /api/login
{
  "login": "user",
  "password": "12345"
}
```

Запрос идёт по незашифрованному HTTP, а в коде приложения пароль хранится в открытом виде.

Какое решение наиболее безопасное?

a) Оставить как есть — приложение работает стабильно
b) Добавить капчу, чтобы замедлить ботов
c) Использовать HTTPS, хранить пароль в защищённом хранилище (Keychain/Keystore) и применять OAuth2 для аутентификации
d) Заменить пароль на более длинный, но оставить HTTP

4. ПОКАЗАТЕЛИ И КРИТЕРИИ ОЦЕНИВАНИЯ

Код ПК, ОК	Критерии оценки результата (показатели освоенности компетенций)	Формы контроля и методы оценки
ПК 3.7.	Оценка «отлично» – выполнен анализ уязвимостей и угроз; реализованы комплексные меры безопасности; настроен мониторинг и реагирование на инциденты; проведены мероприятия по расследованию и устранению последствий. Оценка «хорошо» – выполнен анализ рисков; реализованы основные меры защиты; настроены базовые средства мониторинга безопасности. Оценка «удовлетворительно» – определены потенциальные угрозы; реализованы отдельные меры безопасности; инциденты фиксируются, но реагирование ограничено.	*Контрольные работы, зачеты, квалификационные испытания, защита курсовых и дипломных проектов (работ), экзамены. Интерпретация результатов выполнения практических и лабораторных заданий, оценка решения ситуационных задач, оценка тестового контроля.*
ОК.01	распознает задачу и/или проблему в профессиональном и/или социальном контексте; анализирует задачу и/или проблему; определяет этапы решения задачи; выявляет и эффективно находит информацию, необходимую для решения задачи и/или проблемы; составляет план действия; определяет необходимые ресурсы; оценивает результат и последствия своих действий (самостоятельно или с помощью наставника)	
ОК.02	определяет задачи для поиска информации; определяет необходимые источники информации; планирует процесс поиска; структурирует полученную информацию; выделяет наиболее значимое в перечне информации; оценивает практическую значимость результатов поиска; оформляет результаты поиска	
ОК.03	определяет актуальность нормативно-правовой документации в профессиональной деятельности; применяет современную научную профессиональную терминологию; определяет и выстраивает траектории профессионального развития и самообразования	
ОК.04	организовывает работу коллектива и команды; взаимодействует с коллегами, руководством, клиентами в ходе профессиональной деятельности	
ОК.05	излагает свои мысли и оформлять документы по профессиональной тематике на государственном	

	языке, проявлять толерантность в рабочем коллективе	
ОК.06	описывает значимость своей специальности	
ОК.07	соблюдает нормы экологической безопасности определять направления ресурсосбережения в рамках профессиональной деятельности по специальности	
ОК.09	понимает общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимает тексты на базовые профессиональные темы участвовать в диалогах на знакомые общие и профессиональные темы; пишет простые связные сообщения на знакомые или интересующие профессиональные темы	

Критерии оценки устного ответа обучающихся в 5-балльной системе. При оценке ответа обучающегося учитывается:

1) полнота и правильность ответа;

2) степень осознанности, понимания изученного;

3) языковое оформление ответа. Отметка «5»: ответ исчерпывающий, точный, полный и правильный на основании изученного материала; материал изложен в определенной логической последовательности, литературным языком; ответ самостоятельный.

Отметка «4»: ответ полный, обнаруживающий хорошее знание и понимание изученного материала; материал изложен в определенной логической последовательности, последовательно и грамотно, возможны отдельные затруднения в формулировке выводов.

Отметка «3»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный ответ, изложенный нелогично, ставится за ответ, в котором в основном правильно, но схематично или с отклонениями от последовательности изложения раскрыт материал.

Отметка «2»: при ответе обнаружено непонимание обучающимся основного содержания учебного материала, неумение его анализировать допущены существенные ошибки, которые обучающийся не смог исправить при наводящих вопросах преподавателя, отсутствует логика в изложении материала, нет необходимых обобщений и самостоятельной оценки фактов; недостаточно сформированы навыки устной речи.

Общая классификация ошибок. При оценке знаний, умений, навыков учитываются все ошибки (грубые и негрубые), а также недочёты в работе.

Грубыми считаются ошибки: - незнание определения основных понятий, законов, общепринятых символов обозначений величин; - неумение выделить в ответе главное; обобщить результаты изучения; - неумение применить знания для решения задач, объяснения явления; - неумение подготовить установку или лабораторное оборудование, провести опыт, наблюдение, использовать полученные данные для выводов; - неумение пользоваться первоисточниками, учебником, справочником; - нарушение техники безопасности, небрежное отношение к оборудованию, приборам, материалам.

Негрубыми считаются ошибки: - неточность формулировок, определений, понятий, законов, вызванная неполнотой охвата основных признаков определяемого понятия или заменой 1-3 из этих признаков второстепенными; - ошибки при снятии показаний с измерительных приборов, не связанные с определением цены деления шкалы; - ошибки, вызванные несоблюдением условий проведения опыта, наблюдения, условий работы прибора, оборудования; - нерациональный метод решения задачи, выполнения части практической работы, недостаточно продуманный план устного

ответа (нарушение логики изложения, подмена отдельных основных вопросов второстепенными); - нерациональные методы работы со справочной литературой; - неумение решать задачи, выполнять задания в общем виде.

Недочётами являются: - нерациональные приёмы выполнения опытов, наблюдений, практических заданий; - арифметические ошибки в вычислениях; - орфографические и пунктуационные ошибки.

3.2. Критерии оценивания выполнения практического задания обучающихся в 5-балльной системе:

– Отметка «5»: работа выполнена полностью и правильно; сделаны правильные выводы.

– Отметка «4»: работа выполнена правильно с учетом 1-2 несущественных ошибок, исправленных самостоятельно по требованию преподавателя.

– Отметка «3»: работа выполнена правильно не менее чем на половину или допущены 3-4 существенные ошибки.

– Отметка «2»: допущены 5 и более существенные ошибки в ходе работы, которые обучающийся не может исправить даже по требованию преподавателя.

3.3. Критерии оценивания результатов тестирования

Оценка в баллах	*Степень выполнения задания*
Неудовлетворительно	Выполнено не менее 40 % предложенных заданий
Удовлетворительно	Выполнено не менее 41-70 % предложенных заданий
Хорошо	Выполнено не менее 71-95% предложенных заданий
Отлично	Выполнено не менее 96-100% предложенных заданий

3.4. Критерии оценки написания сообщений, докладов:

- оценка «отлично» выставляется обучающемуся, если выполнены все требования к написанию сообщения (доклада): обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы;

- оценка «хорошо» выставляется обучающемуся, если основные требования к сообщению, докладу и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём доклада (сообщения); имеются упущения в оформлении; на дополнительные вопросы даны неполные ответы.

- оценка «удовлетворительно» выставляется обучающемуся, если имеются существенные отступления от требований к написанию сообщения (доклада). В частности, тема освещена лишь частично; допущены фактические ошибки в содержании сообщения (доклада) или при ответе на дополнительные вопросы; во время защиты отсутствует вывод;

- оценка «неудовлетворительно» выставляется обучающемуся, если тема сообщения (доклада) не раскрыта, обнаруживается существенное непонимание проблемы.

3.5 Критерии оценивания презентаций:

– Оценка «отлично»: Содержание: Работа полностью завершена, обучающийся демонстрирует глубокое понимание описываемых процессов, даны интересны дискуссионные материалы, грамотно используется лексика, предлагается собственная интерпретация или развитие темы. Дизайн логичен. Все параметры шрифта хорошо подобраны. Текст хорошо читается. Графика подобрана грамотно, соответствует содержанию. Нет орфографических и синтаксических ошибок.

– Оценка «хорошо»: Полностью сделаны наиболее важные компоненты работы, обучающийся демонстрирует понимание основных моментов, хотя некоторые детали не

уточняются. Некоторые материалы носят дискуссионный характер. Научная лексика используется, но иногда не корректно. Обучающийся в большинстве случаев предлагает собственную интерпретацию или развитие темы. Дизайн презентации выдержан и соответствует содержанию. Параметры шрифта подобраны. Графика соответствует содержанию. Минимальное количество ошибок.

– Оценка «удовлетворительно»: В содержании не выделены все важные компоненты. Обучающийся демонстрирует неполное понимание темы. Дискуссионные материалы есть в наличии, но не способствуют раскрытию проблемы. Научная терминология используется не всегда корректно. Дизайн не соответствует полному раскрытию содержания. Параметры шрифта недостаточно хорошо подобраны и могут мешать восприятию. Графика не в полной мере соответствует содержанию. Имеются орфографические и пунктуационные ошибки, мешающие восприятию.

– Оценка «неудовлетворительно»: Работа выполнена фрагментарно и с посторонней помощью, обучающийся демонстрирует минимальное понимание темы. Минимум дискуссионных материалов и научных терминов. Интерпретация ограничена или беспочвенна. Дизайн неясен. Элементы дизайна мешают содержанию. Текст трудночитаемый. Графика не соответствует содержанию. Много орфографических и пунктуационных ошибок, делающих материал трудночитаем.