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.02.06 Безопасность программного обеспечения

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

форма обучения: заочная

форма промежуточной аттестации: экзамен

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.02.06 Безопасность программного обеспечения, входящего в ПМ.02 Разработка и интеграция модулей программного обеспечения 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
ПК 2.4	− анализировать требования к программному	− принципы и методы тестирования программного обеспечения;

	обеспечению и составлять планы тестирования; − создавать тестовые сценарии и тест-кейсы для проверки функциональности и соответствия требованиям; − выполнять тестирование программного обеспечения вручную и автоматизировать процесс тестирования; − анализировать результаты тестирования и документировать найденные ошибки; − разрабатывать стратегии отладки и исправлять ошибки в программном обеспечении; − выполнять модульные тесты с использованием инструментов тестирования, в том числе автоматизированного тестирования; − использовать системы контроля дефектов ПО; составлять отчет о выполнении тестирования ПО	− основы программирования и архитектуры программного обеспечения; − основы баз данных и SQL-запросов; − инструменты для автоматизации тестирования; − основы разработки и отладки программного обеспечения на разных языках программирования; − понятие дефекта программного обеспечения; − критерии качества ПО; − виды и типы тестирования ПО; − техники ручного тестирования; − техники автоматизированного тестирования; − жизненный цикл дефекта ПО; − принципы работы в системе контроля дефектов; основные понятия о качестве ПО
ПК 2.5	− описывать функциональность модулей в документации; − создавать диаграммы для иллюстрации работы модулей; − программировать с использованием комментариев для документирования кода; − использовать специальные метки/теги для отметки важных	− стандарты технической документации; − принципы документирования программного обеспечения; инструменты для создания технической документации и комментирования кода

	частей кода в документации; − вести журнал изменений и фиксировать обновления программных модулей; − разбивать модули на логические блоки и описывать каждый блок отдельн; − включать в документацию особенности модулей, такие как ограничения, уязвимости или оптимальные настройки; проводить регулярное обновление документации при изменении модулей или добавлении нового функционала.	

2. КОМПЛЕКТ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ

2.1 Примерная тематика практических заданий

Задача 1: Анализ кода на уязвимости (ручной review)
Цель: Научиться находить уязвимости в исходном коде вручную.
Описание:
Студенту выдаётся фрагмент веб-приложения на Python (Flask) объёмом около 1000 строк. Приложение позволяет пользователям оставлять комментарии.
Задание:

1. Проведите ручной аудит кода.
2. Найдите **минимум 3 уязвимости** (например: небезопасная работа с файлами, отсутствие валидации ввода, жёстко закодированные пароли).
3. Опишите каждую уязвимость:
   - Где находится (файл, строка)
   - Какой тип угрозы (CWE)
   - Как её можно эксплуатировать
   - Как исправить
4. Предложите хотя бы одно средство автоматического анализа (например, Bandit) и проверьте им код.

Результат: Отчёт с описанием уязвимостей и рекомендациями по исправлению.

Задача 2: SQL-инъекции — эксплуатация и защита
Цель: Понять, как работают SQL-инъекции, и научиться защищать приложения.

Описание:
Дано уязвимое веб-
приложение (например, на PHP или Python), где для входа используется запрос вида:
python

```python
query = "SELECT * FROM users WHERE login = '" + login + "' AND password = '" + password + "'"
```

Задание:

1. Используя SQL-
   инъекцию, войдите в систему без знания логина и пароля (например, через
   ' OR '1'='1).
2. Попробуйте извлечь список таблиц через UNION-инъекцию (если СУБД — SQLite или MySQL).
3. Перепишите код, используя **параметризованные запросы** (prepared statements).
4. Объясните, почему это защищает от инъекций.

Результат: Видеозапись или скриншоты успешной атаки и защищённой версии кода.

Задача 3: XSS-атаки — создание и защита
Цель: Научиться распознавать и предотвращать межсайтовый скриптинг.
Описание:
Есть веб-
страница с формой комментариев, где введённый текст отображается напрямую в HTML.
Задание:

1. Введите комментарий с XSS-вектором:

```html
<script>alert('XSS')</script>
```

Убедитесь, что скрипт выполняется.

2. Попробуйте внедрить внешний скрипт (например, через <script src="...">).
3. Реализуйте защиту:
   - Экранирование тегов (HTML-entities)
   - Использование Content Security Policy (CSP) в заголовке ответа:

```http
Content-Security-Policy: default-src 'self'
```

4. Проверьте, что атака больше не работает.

Результат: Сравнение уязвимой и защищённой версий с пояснениями.

Задача 4: CSRF — защита с токенами и проверкой заголовков
Цель: Реализовать защиту от подделки межсайтовых запросов.
Описание:
Есть форма перевода денег между счетами, которая не проверяет источник запроса.
Задание:

1. Создайте HTML-страницу на другом домене, которая автоматически отправляет POST-запрос на перевод средств (имитация CSRF-атаки).
2. Добавьте в форму **CSRF-токен** (сгенерированный сервером, хранится в сессии).
3. Модифицируйте серверную логику, чтобы он проверял токен при каждом изменяющем запросе.
4. Дополнительно: добавьте проверку заголовков Origin или Referer.
5. Убедитесь, что поддельный запрос больше не проходит.

Результат: Работающий пример с защитой и объяснением механизма.

Задача 5: Составление модели угроз для веб-приложения
Цель: Научиться системно подходить к анализу рисков.
Описание:
Рассматривается типовое веб-приложение для онлайн-голосования.
Задание:

1. Постройте **диаграмму потоков данных (DFD)** приложения (регистрация, голосование, подсчёт).
2. Примените метод **STRIDE**:
    - Для каждого элемента (пользователь, сервер, БД, API) определите возможные угрозы:
        - Подделка (Spoofing)
        - Подмена (Tampering)
        - Отказ в обслуживании (DoS) и т.д.
3. Для каждой угрозы предложите контрмеру (например, шифрование, аутентификация, логирование).
4. Выделите **топ-3 критические угрозы**.

Результат: Таблица угроз + краткий отчёт с приоритезацией.

Задача 6: Безопасная аутентификация с JWT и refresh-токенами
Цель: Реализовать современную схему аутентификации.
Описание:
Нужно реализовать систему входа для SPA-приложения (например, на Flask + JS).
Задание:

1. При успешном входе сервер генерирует:
    - **JWT-токен** (access token) на 15 минут
    - **Refresh-токен** (хранится в HTTP-only куке, срок — 7 дней)
2. Настройте эндпоинт /refresh, который выдаёт новый access-токен по валидному refresh-токену.
3. Реализуйте защиту:
    - Подпись JWT (HS256 или RS256)
    - Проверку срока действия
    - Блокировку украденных refresh-токенов (через blacklist или короткий TTL)
4. Объясните, зачем нужен refresh-токен и почему access-токен не хранится в куках.

Результат: Работающий API с демонстрацией получения и обновления токенов.

2.2 Задания в тестовой форме

Тестовые задания типа А (Необходимо выбрать один наиболее правильный ответ

из нескольких предложенных вариантов)

1. Что из перечисленного НЕ входит в определение кибербезопасности?
   а) Защита конфиденциальности данных
   б) Обеспечение доступности систем
   в) Повышение производительности серверов
   г) Целостность информации
2. Какой из перечисленных терминов означает слабость в системе, которую можно использовать для нарушения её безопасности?
   а) Угроза
   б) Риск
   в) Уязвимость
   г) Атака
3. Какая модель угроз включает категории: Подделка, Подмена, Отказ в обслуживании?
   а) DREAD
   б) CIA
   в) STRIDE
   г) ISO 27001
4. В модели DREAD буква “R” означает:
   а) Risk (риск)
   б) Reproducibility (воспроизводимость)
   в) Reliability (надёжность)
   г) Response (реакция)
5. Какой из принципов безопасного кодирования предполагает, что компонент должен иметь только те привилегии, которые необходимы для выполнения своих функций?
   а) Глубокая защита
   б) Принцип наименьших привилегий
   в) Отказоустойчивость
   г) Минимизация доверия
6. К какой категории OWASP Top 10 относится уязвимость, возникающая при вставке непроверенных данных в SQL-запрос?
   а) Broken Access Control
   б) Cryptographic Failures
   в) Injection
   г) Security Misconfiguration
7. Какой тип атаки позволяет злоумышленнику выполнить произвольный JavaScript-код в браузере жертвы?
   а) CSRF
   б) SSRF
   в) XSS
   г) XXE
8. Какой из следующих пунктов НЕ входит в OWASP Top 10?
   а) Insecure Deserialization
   б) Insufficient Logging and Monitoring
   в) Poor UI Design
   г) Vulnerable and Outdated Components
9. Какой из подходов к оценке рисков использует количественные значения (например, вероятность и ущерб)?
   а) Качественный анализ
   б) Матрица рисков
   в) Количественный анализ

г) Метод экспертных оценок

10. Какой из перечисленных подходов помогает выявить уязвимости на этапе проектирования ПО?
    а) Пентест
    б) Аудит кода
    в) Threat modeling
    г) Обфускация
11. Какой механизм аутентификации использует три независимых фактора: пароль, токен и отпечаток пальца?
    а) Однофакторная
    б) Двухфакторная
    в) Трёхфакторная
    г) Многофакторная
12. Какой протокол позволяет пользователю входить в сторонние приложения, используя учётную запись Google или Facebook?
    а) SAML
    б) OAuth 2.0
    в) LDAP
    г) Kerberos
13. Что из перечисленного используется для управления правами доступа на основе ролей пользователя?
    а) ABAC
    б) JWT
    в) RBAC
    г) TLS
14. Какой алгоритм хеширования НЕ рекомендуется для хранения паролей из-за высокой скорости вычисления?
    а) bcrypt
    б) SHA-256
    в) Argon2
    г) PBKDF2
15. Какой из методов шифрования использует один и тот же ключ для шифрования и расшифрования?
    а) Асимметричное
    б) Симметричное
    в) Гибридное
    г) Квантовое
16. Какой алгоритм используется для создания цифровой подписи?
    а) AES
    б) RSA
    в) SHA-1
    г) MD5
17. Что означает “защита данных в покое”?
    а) Данные шифруются при передаче по сети
    б) Данные защищены от DDoS-атак
    в) Данные зашифрованы при хранении на диске
    г) Данные резервируются ежедневно
18. Какой из заголовков HTTP помогает предотвратить XSS-атаки, ограничивая источники исполняемого скрипта?
    а) X-Frame-Options
    б) Content-Security-Policy
    в) Strict-Transport-Security
    г) X-Content-Type-Options

19. Какой из принципов криптографии обеспечивает невозможность отрицания отпр авки сообщения?
    а) Конфиденциальность
    б) Целостность
    в) Аутентичность
    г) Невозможность отказа (non-repudiation)
20. Какой тип токена используется для передачи информации о пользователе между серверами в формате JSON?
    а) SAML
    б) JWT
    в) PGP
    г) X.509
21. Какой принцип предполагает наличие нескольких уровней защиты в системе?
    а) Принцип наименьших привилегий
    б) Глубокая защита (defence in depth)
    в) Минимизация поверхности атаки
    г) Отказоустойчивость
22. Какой из подходов к проектированию ПО предполагает разделение системы на н езависимые компоненты с ограниченным взаимодействием?
    а) Монолитная архитектура
    б) Микросервисы
    в) Слоистая архитектура
    г) Модульность
23. Что из перечисленного является примером безопасного шаблона проектировани я?
    а) Singleton
    б) Input validation filter
    в) Observer
    г) Factory
24. Какой инструмент позволяет автоматически находить уязвимости в сторонних б иблиотеках?
    а) Git
    б) Jenkins
    в) OWASP Dependency-Check
    г) Postman
25. Что означает “управление зависимостями” в контексте безопасности ПО?
    а) Контроль за версиями библиотек и их уязвимостями
    б) Оптимизация времени загрузки приложения
    в) Удаление неиспользуемого кода
    г) Обфускация скриптов
26. Какой из принципов означает, что система должна оставаться безопасной даже п ри частичном отказе компонентов?
    а) Гибкость
    б) Отказоустойчивость
    в) Масштабируемость
    г) Производительность
27. Какой протокол обеспечивает безопасную передачу данных в HTTPS?
    а) SSH
    б) FTPS
    в) TLS
    г) IPsec
28. Какой из алгоритмов используется для безопасного хранения паролей с “солью” и итерациями?

а) SHA-256
б) AES-256
в) bcrypt
г) RSA-2048

29. Что из перечисленного НЕ является функцией KMS (Key Management Service) в облаке?
а) Генерация криптографических ключей
б) Хранение ключей в защищённом виде
в) Автоматическое шифрование пользовательских паролей
г) Управление доступом к ключам
30. Какой из методов используется для защиты данных в мобильном приложении на устройстве пользователя?
а) CSP
б) Code obfuscation
в) JWT
г) OAuth

3. КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

3.1 Вопросы для подготовки к промежуточной аттестации

1. Дайте определение кибербезопасности. Какие три компонента входят в модель CIA и что они означают?
2. Что такое уязвимость программного обеспечения? Приведите два примера и объясните, чем она отличается от угрозы.
3. В чём разница между риском и угрозой? Как связаны между собой уязвимость, угроза и риск?
4. Опишите модель угроз STRIDE. Какие шесть типов угроз она включает и как они расшифровываются?
5. Что означает аббревиатура DREAD? Какие критерии она использует для оценки уязвимостей?
6. Какие методы анализа рисков используются в информационной безопасности? В чём разница между качественным и количественным подходами?
7. Как классифицируются уязвимости по типу воздействия и по источнику возникновения?
8. Что входит в перечень OWASP Top 10? Назовите три наиболее распространённые уязвимости и кратко опишите каждую.
9. Что такое инъекция? Приведите пример SQL-инъекции и объясните, как её можно предотвратить.
10. Что такое межсайтовый скриптинг (XSS)? Какие виды XSS существуют и чем они отличаются?
11. Какие проблемы возникают при небезопасной аутентификации? Приведите три примера слабых практик.
12. Какие типичные ошибки приводят к уязвимостям конфигурации в веб-серверах и приложениях?
13. Перечислите основные принципы безопасного кодирования. Как они помогают снизить количество уязвимостей?
14. Почему важно проводить валидацию и экранирование входных данных? Какие последствия могут быть при их отсутствии?
15. Что такое многофакторная аутентификация (MFA)? Приведите пример её

реализации в реальной системе.

16. В чём разница между аутентификацией и авторизацией? Приведите пример из веб-приложения.
17. Как работает протокол OAuth 2.0? Для каких целей он используется и какие основные роли в нём выделяются?
18. Что такое OpenID Connect? Как он дополняет функциональность OAuth 2.0?
19. Как управляются сессии в веб-приложениях? Какие атрибуты cookie используются для их защиты?
20. В чём отличие между ролевой (RBAC) и атрибутной (ABAC) моделью управления доступом? Приведите пример использования каждой.
21. Объясните разницу между симметричным и асимметричным шифрованием. Приведите по одному примеру алгоритма для каждого типа.
22. Какие требования предъявляются к хешированию паролей? Почему bcrypt, Argon2 и PBKDF2 предпочтительнее, чем SHA-256?
23. Что такое “соль” (salt) и “итерации” при хешировании паролей? Как они повышают безопасность?
24. Что такое цифровая подпись? Какие задачи она решает и на каких принципах криптографии основана?
25. В чём разница между защитой данных “в покое” и “в передаче”? Приведите по одному примеру метода защиты для каждого случая.
26. Сформулируйте принцип наименьших привилегий. Как он применяется в операционных системах и приложениях?
27. Что означает “глубокая защита” (defence in depth)? Приведите пример реализации на трёх уровнях веб-приложения.
28. Какие меры обеспечивают отказоустойчивость системы при сбое отдельных компонентов с точки зрения безопасности?
29. Какие методы используются для аудита безопасности на этапе проектирования ПО? Что входит в threat modeling?
30. Как обеспечивается безопасность зависимостей в современных проектах? Назовите инструменты для анализа уязвимостей в сторонних библиотеках.

3.2 Тестовые задания для промежуточной аттестации

Тестовые задания типа А

1. Какой из перечисленных подходов позволяет проверить, что входные данные соответствуют ожидаемому формату и не содержат вредоносных символов?
а) Шифрование
б) Валидация ввода
в) Аутентификация
г) Логирование
2. Какой тип уязвимости возникает при передаче чувствительных данных в URL?
а) XSS
б) Информационный лейк
в) CSRF
г) DoS
3. Что из перечисленного является примером атаки “человек посередине” (MitM)?
а) Подбор пароля методом перебора
б) Перехват трафика между клиентом и сервером

в) Внедрение вредоносного скрипта на сайт
г) Подделка электронной почты
4. Какой стандарт используется для безопасного обмена утверждениями о пользователе между системами?
а) OAuth 2.0
б) SAML
в) JWT
г) OpenID Connect
5. Какой из принципов означает, что система должна по умолчанию быть максимально закрытой для внешнего доступа?
а) Глубокая защита
б) Безопасность по умолчанию
в) Принцип наименьших привилегий
г) Открытый дизайн
6. Какой тип атаки использует уязвимость в обработке XML-данных для чтения файлов на сервере?
а) XSS
б) SQLi
в) XXE
г) CSRF
7. Что из перечисленного является наиболее безопасным способом хранения паролей?
а) Хранение в открытом виде
б) Хранение в Base64
в) Хэширование с солью (например, bcrypt)
г) Хэширование с SHA-256 без соли
8. Какой из заголовков HTTP помогает предотвратить кликджекинг?
а) Content-Security-Policy
б) X-Frame-Options
в) X-XSS-Protection
г) Strict-Transport-Security
9. Какой из методов защиты используется для предотвращения подделки запросов от имени авторизованного пользователя?
а) HTTPS
б) CSRF-токен
в) HTTP Strict Transport Security
г) Кэширование
10. Что означает термин “security by obscurity”?
а) Защита на основе открытых стандартов
б) Попытка скрыть уязвимость за счёт неочевидности реализации
в) Использование сложных паролей
г) Применение шифрования
11. Какой из алгоритмов является асимметричным?
а) AES
б) SHA-256
в) RSA
г) HMAC
12. Что из перечисленного используется для защиты целостности сообщения?
а) Шифрование
б) Хэш-функция или цифровая подпись
в) Сессионный идентификатор
г) CAPTCHA
13. Какой протокол заменил SSL и обеспечивает безопасную передачу данных?
а) SSH

б) TLS
в) FTPS
г) IPsec
14. Какой из принципов означает, что доверие к компоненту должно быть минимальным и обоснованным?
а) Глубокая защита
б) Минимизация доверия (least trust)
в) Отказоустойчивость
г) Аудит
15. Что из перечисленного является примером атаки на уровень сессии?
а) SQL-инъекция
б) Перехват сессионного токена (session hijacking)
в) XSS
г) DDoS
16. Какой из подходов используется для защиты от перебора паролей?
а) Увеличение длины пароля
б) Ограничение числа попыток входа (rate limiting)
в) Использование CAPTCHA
г) Все перечисленные
17. Какой тип токена может быть использован для одноразового подтверждения действия (например, сброса пароля)?
а) JWT
б) Одноразовый код (OTP)
в) Refresh-токен
г) API-ключ
18. Что из перечисленного НЕ является частью безопасной политики управления сессиями?
а) Использование безопасных кук (Secure, HttpOnly)
б) Очистка сессии при выходе
в) Короткое время жизни сессии
г) Хранение идентификатора сессии в URL
19. Какой из методов используется для защиты от атак перебора (brute force)?
а) Двухфакторная аутентификация
б) Ограничение попыток входа
в) CAPTCHA
г) Все перечисленные
20. Какой из стандартов используется для защиты API с помощью токенов?
а) OAuth 1.0
б) OAuth 2.0
в) SAML
г) LDAP
21. Что из перечисленного является примером уязвимости в конфигурации?
а) Использование слабого пароля
б) Открытый доступ к административной панели
в) XSS в форме комментариев
г) SQL-инъекция
22. Какой из инструментов используется для анализа уязвимостей в веб-приложениях?
а) Wireshark
б) Burp Suite
в) Postman
г) Figma
23. Что означает термин “secure by design”?
а) Безопасность закладывается на этапе проектирования ПО

б) Применение шифрования ко всем данным
в) Использование только лицензионного ПО
г) Регулярное обновление паролей
24. Какой из методов используется для защиты от подделки данных при передаче?
а) Шифрование
б) Цифровая подпись
в) Хэширование без соли
г) Кодирование в Base64
25. Какой из заголовков HTTP заставляет браузер использовать только HTTPS?
а) X-Content-Type-Options
б) Content-Security-Policy
в) Strict-Transport-Security
г) X-Frame-Options
26. Какой из подходов используется для безопасного обновления ПО?
а) Подписание обновлений цифровой подписью
б) Проверка хэша загружаемого файла
в) Автоматическая установка обновлений
г) Все перечисленные
27. Что из перечисленного является примером атаки на уровень API?
а) XSS
б) Недостаточная проверка прав доступа (Broken Object Level Authorization)
в) CSRF
г) Clickjacking
28. Какой из методов используется для защиты от утечки данных через логи?
а) Шифрование логов
б) Фильтрация чувствительных данных перед записью
в) Ограничение доступа к файлам логов
г) Все перечисленные
29. Какой из принципов означает, что система должна вести подробные записи о событиях безопасности?
а) Аутентификация
б) Авторизация
в) Аудит и логирование
г) Шифрование
30. Какой из подходов используется для защиты мобильного приложения от анализа и модификации кода?
а) Шифрование трафика
б) Обфускация кода
в) Использование JWT
г) Валидация ввода

Тестовые задания типа В. (Установите соответствие между элементами)
1. Установите соответствие между типом атаки и её описанием:

Атака	Описание
1. SQL-инъекция	а) Выполнение вредоносного скрипта в браузере пользователя
2. XSS	б) Подмена запроса от авторизованного пользователя
3. CSRF	в) Внедрение SQL-кода через входные данные

4. XXE	г) Обработка вредоносного XML-документа

Верный ответ:
1 – в
2 – а
3 – б
4 – г

2. Установите соответствие между протоколом и его назначением:

Протокол	Назначение
1. TLS	а) Управление доступом через токены
2. OAuth 2.0	б) Аутентификация на основе утверждений
3. SAML	в) Безопасная передача данных по сети
4. JWT	г) Формат для передачи утверждений о пользователе

Верный ответ:
1 – в
2 – а
3 – б
4 – г

3. Установите соответствие между принципом безопасности и его объяснением:

Принцип	Объяснение
1. Принцип наименьших привилегий	в) Компонент получает только необходимые права
2. Глубокая защита	а) Несколько уровней защиты в системе
3. Отказоустойчивость	б) Система остаётся безопасной при частичном сбое
4. Безопасность по умолчанию	г) Система по умолчанию закрыта для атак

Верный ответ:
1 – в
2 – а
3 – б
4 – г

4. Установите соответствие между уязвимостью и категорией из OWASP Top 10:

Уязвимость	Категория OWASP
1. Подделка токена сессии	г) Identification and Authentication Failures
2. Хранение паролей в открытом виде	г) Identification and Authentication Failures
3. Отсутствие проверки прав при доступе к API	б) Broken Access Control
4. Отсутствие логирования входов	в) Security Logging and Monitoring Failures

Верный ответ:
1 – г
2 – г
3 – б
4 – в

5. Установите соответствие между заголовком HTTP и его функцией:

Заголовок	Функция

1. Content-Security-Policy	в) Ограничивает источники исполняемых скриптов
2. X-Frame-Options	а) Запрещает отображение страницы во фреймах
3. Strict-Transport-Security	б) Указывает браузеру использовать только HTTPS
4. X-Content-Type-Options	г) Отключает MIME-сниффинг

Верный ответ:
1 – в
2 – а
3 – б
4 – г

6. Установите соответствие между криптографическим методом и его применением:

Метод	Применение
1. AES	б) Шифрование чувствительных данных в базе
2. RSA	в) Создание цифровой подписи
3. SHA-256	а) Проверка целостности и авторства сообщения
4. HMAC	г) Проверка целостности сообщения с ключом

Верный ответ:
1 – б
2 – в
3 – а
4 – г

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

1: Уязвимость в веб-форме
Разработчик создал форму входа на сайт, где пользователь вводит логин и пароль. Данные передаются на сервер через POST-запрос.
При тестировании выяснилось, что при вводе в поле логина строки ' OR '1'='1 пользователь получает доступ без пароля.
Какую уязвимость обнаружили?
а) XSS — вредоносный скрипт выполняется в браузере
б) CSRF — запросы отправляются от имени пользователя без его ведома
в) Небезопасное хранение пароля в базе данных
г) SQL-инъекция — в запрос подставляется вредоносный SQL-код

2: Защита сессии пользователя
Разработчик реализовал систему входа в веб-приложение. После авторизации пользователю выдаётся идентификатор сессии,
который передаётся в cookie. Однако при анализе безопасности выяснилось, что токен можно перехватить и использовать на другом устройстве.
Как правильно защитить сессию?
а) Использовать короткие имена cookie для экономии трафика
б) Передавать идентификатор сессии в URL для удобства
в) Установить флаги Secure и HttpOnly для cookie
г) Генерировать предсказуемый токен на основе времени

3: Хранение паролей в базе данных
При разработке системы аутентификации студент предложил хранить пароли пользователей в базе данных. Он предлагает несколько вариантов.
Какой способ хранения паролей является безопасным?
а) В открытом виде — для быстрой проверки
б) В формате Base64 — чтобы скрыть текст
в) С помощью SHA-256 без соли — быстро и просто
г) С помощью bcrypt с солью — медленно и устойчиво к перебору

4: Защита от XSS-атак
Разрабатывается веб-
приложение, где пользователи могут оставлять комментарии. Комментарии отображаются на странице без изменений. Один из тестировщиков ввёл в комментарий строку `<script>alert('XSS')</script>`, и код выполнился.
Как предотвратить такую атаку?
а) Разрешить HTML-теги для всех пользователей
б) Хранить комментарии в JSON-формате
в) Использовать HTTPS на сайте
г) Экранировать специальные символы перед выводом на страницу

4. ПОКАЗАТЕЛИ И КРИТЕРИИ ОЦЕНИВАНИЯ

Код ПК, ОК	Критерии оценки результата (показатели освоенности компетенций)	Формы контроля и методы оценки
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)	Контрольные работы, зачеты, квалификационные испытания, защита курсовых и дипломных проектов (работ), учебная и производственная практики, экзамены. Интерпретация результатов выполнения практических и лабораторных заданий, оценка решения ситуационных задач, оценка тестового контроля, результатов наблюдений за деятельностью обучающегося в процессе учебной и производственной практики
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	
ПК 2.4	проводит отладку программного обеспечения на уровне программных модулей; тестирует программное обеспечение; формирует тестовые сценарии; готовит тестовые платформы (устанавливает операционную систему, дополнительное программное обеспечение и другое по необходимости); проводит оценку объема тестирования программного обеспечения с целью определения необходимых ресурсов для его выполнения; настраивает тестовые среды и аппаратные средства для выполнения тестирования программного обеспечения в соответствии с заданием на тестирование в пределах своей компетенции; формирует и предоставляет отчетность о подготовке к выполнению задания на тестирование программного обеспечения в соответствии с установленными регламентами; выполняет тестовые процедуры на тестовых данных	
ПК 2.5	создает техническую документацию для модулей; документирует код, API и интерфейсов; работает со специализированным программным обеспечением по документированию программного кода	

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.