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 МАТЕРИАДЫ ТЕКУЩЕГО КОНТРОЛЯ**
**И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ**
**ОП.05 Основы информационной безопасности**

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

форма обучения: заочная

форма промежуточной аттестации по дисциплине: экзамен

Пермь 2026

**СОДЕРЖАНИЕ**

# 1. ПАСПОРТ ОЦЕНОЧНЫХ МАТЕРИАЛОВ

**1.1. Общая характеристика оценочных материалов.**

Оценочные материалы (ОМ) разработан с целью установления соответствия образовательных достижений студентов требованиям программы подготовки специалистов среднего звена по дисциплине ОП.05 Основы информационной безопасности специальности 09.02.11 Разработка и управление программным обеспечением.

ОМ включают контрольные материалы для проведения текущего контроля и 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 | распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составлять план действия; определять необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах реализовывать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника) | 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 | определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение; использовать различные цифровые средства для решения профессиональных задач | 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 09 | понимать тексты на базовые профессиональные темы | лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности |
| ПК 1.1 | - | принципы безопасности хранения данных |
| ПК 1.4 | - | методы защиты баз данных от внешних угроз |
| ПК 1.5 | шифровать данные и обеспечивать их конфиденциальность | принципы криптографии и методов шифрования данных |

| | | |
|---|---|---|
| | | стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.<br>методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных<br>законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др. |
| ПК 3.1 | - | отраслевая нормативная техническая документация<br>источники информации, необходимой для профессиональной деятельности |
| | | современный отечественный и зарубежный опыт в профессиональной деятельности |
| ПК 3.2 | - | принципы и методы обеспечения безопасности информационных систем |
| ПК 3.3 | анализ требований безопасности информационных систем | принципов безопасности информационных систем<br>современных методов и технологий в области безопасности информационных систем<br>законодательных и нормативных актов в области безопасности информационных систем |
| ПК 3.5 | - | источники угроз информационной безопасности и меры по их предотвращению |
| ПК 3.7 | разрабатывать и реализовывать меры безопасности<br>реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию | основные угрозы безопасности мобильных приложений<br>принципы криптографии и шифрования данных.<br>стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect<br>законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA<br>основные принципы безопасности информации и методов ее защиты.<br>стандартные криптографические алгоритмы для шифрования данных<br>принципы обеспечения безопасности передачи данных по |

| | | |
|---|---|---|
| | | сети<br>основы безопасности приложений и инфраструктуры<br>методы анализа на уязвимости и мониторинга безопасности<br>знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений<br>понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения<br>знание инструментов и технологий 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 Практические работы

1. Задание: «Анализ угрозы и разработка правил поведения в сети»
Тема: Основные понятия ИБ, социальная инженерия
Практическая часть:
Просмотрите 2–3 примера фишинговых писем.
Определите признаки фишинга: подозрительные ссылки, срочность, ошибки в тексте, поддельные логотипы.
Отметьте, какие данные пытаются получить злоумышленники.
Самостоятельная работа:
Создайте памятку для сотрудников офиса:
Как распознать фишинг?
Что делать при подозрении на атаку?
Какие пароли безопасны?

2. Задание: «Настройка прав доступа и резервного копирования»
Тема: Управление доступом, резервное копирование
Практическая работа:
На компьютере с Windows:
Создайте 2 учётные записи: «Администратор» и «Пользователь».
Ограничьте доступ пользователя к папке «Документы» администратора.
С помощью встроенной утилиты «Резервное копирование и восстановление» создайте точку восстановления.
Удалите файл и восстановите его.
Самостоятельная работа:
Ответьте письменно:
Почему важно разделять права пользователей?

Как часто нужно делать резервные копии?

3. Задание: «Работа с антивирусом и фаерволом»
Тема: Сетевая безопасность, защита от атак
Практическая работа:
Установите бесплатный антивирус (например, Kaspersky Free, Avast или Windows Defender, если не включён).
Проверьте систему на вирусы.
Откройте брандмауэр Windows и посмотрите:
Какие программы имеют доступ в интернет?
Как добавить правило для блокировки программы?
Создайте правило, запрещающее одному приложению (например, браузеру) выход в сеть.
Самостоятельная работа:
Напишите краткий отчёт: зачем нужен фаервол и как антивирус помогает в борьбе с угрозами.

4. Задание: «Шифрование файлов с помощью 7-Zip»
Тема: Основы криптографии, шифрование данных
Практическая работа:
Установите 7-Zip.
Создайте архив с несколькими файлами, защитите его паролем (AES-256).
Попробуйте открыть архив без пароля.
Перешлите архив одногруппнику (в классе) — тот должен распаковать его.
Самостоятельная работа:
Ответьте:
В каких случаях нужно шифровать файлы?
Почему важно использовать надёжный пароль?

5. Задание: «Настройка Wi-Fi: безопасность роутера»
Тема: Сетевая безопасность, защита от атак
Практическая работа (в лаборатории с роутером):
Подключитесь к роутеру через браузер (адрес 192.168.1.1 или 192.168.0.1).
Смените пароль администратора.
Включите шифрование WPA2/WPA3.
Смените имя сети (SSID), отключите её трансляцию (по указанию преподавателя).
Запретите доступ по MAC-адресу одному устройству (условно).
Самостоятельная работа:
Составьте чек-лист: «5 правил безопасного домашнего Wi-Fi».

6. Задание: «Реакция на инцидент: что делать, если заразился?»
Тема: Реакция на инциденты
Практическая работа:
Смоделируйте ситуацию:
Условно «заразитесь» — откройте файл с подозрительным расширением (в учебных целях, без настоящего вируса).
Заметьте симптомы: тормоза, новые ярлыки, блокировка файлов.
Отключите компьютер от сети.
Запустите антивирусную проверку.
Восстановите файлы из резервной копии.
Самостоятельная работа:
Составьте схему действий:
Обнаружение

Сдерживание
Устранение
Восстановление
(Можно в виде блок-схемы в Word или на бумаге.)

### 2.2 Задания в тестовой форме

**1.** Что является основной целью информационной безопасности?
а) Увеличение скорости работы компьютера
б) Обеспечение удобства пользователей
**в) Сохранение конфиденциальности, целостности и доступности информации**
г) Снижение стоимости программного обеспечения
**2.** Какая из перечисленных угроз относится к социальной инженерии?
а) Вирус, блокирующий доступ к файлам
б) Сбой в работе сервера
**в) Фишинговое письмо с просьбой ввести логин и пароль**
г) Перегрев жесткого диска
**3.** Какой документ регулирует защиту персональных данных в Российской Федерации?
а) Конвенция о киберпреступности
б) Стандарт ISO 27001
**в) Федеральный закон № 152-ФЗ**
г) Директива GDPR (для РФ не действует)
**4.** Что означает принцип «разделения обязанностей» в политике безопасности?
а) Все сотрудники работают по 8 часов
б) Один сотрудник отвечает за всё ИТ-обеспечение
**в) Критические операции требуют участия нескольких лиц**
г) Работники не общаются друг с другом
**5.** Какой стандарт регулирует системы менеджмента информационной безопасности?
а) PCI DSS
б) NIST SP 800-53
**в) ISO/IEC 27001**
г) IEEE 802.11
**6.** Что такое хэш-функция?
а) Алгоритм шифрования с ключом
б) Способ передачи данных по сети
**в) Функция, преобразующая данные в уникальную строку фиксированной длины**
г) Протокол безопасного соединения
**7.** Какой алгоритм относится к симметричному шифрованию?
а) RSA
б) ECC
**в) AES**
г) Diffie-Hellman
**8.** Для чего используется цифровая подпись?
а) Чтобы ускорить передачу файлов
б) Чтобы сжать документ
**в) Чтобы подтвердить авторство и целостность сообщения**
г) Чтобы изменить формат файла
**9.** Какой метод позволяет скрыть информацию внутри изображения?
а) Шифрование AES
б) Архивация 7-Zip

**в) Стеганография**
г) Хэширование SHA-256
**10.** Что защищает межсетевой экран (фаервол)?
а) От перепадов напряжения
б) От физического доступа к серверу
**в) От несанкционированных сетевых подключений**
г) От вредоносных звуковых файлов
**11.** Какая атака направлена на переполнение сервера трафиком?
а) Фишинг
б) SQL-инъекция
**в) DDoS-атака**
г) XSS
**12.** Что такое VPN?
а) Программа для резервного копирования
б) Антивирусное приложение
**в) Технология защищённого удалённого подключения к сети**
г) Сетевой протокол передачи файлов
**13.** Какая из уязвимостей входит в OWASP Top Ten?
а) Использование старого монитора
б) Слабая вентиляция серверной
**в) Несанкционированный доступ к данным (например, через SQL-инъекцию)**
г) Низкая скорость интернета
**14.** Что означает «безопасное программирование»?
а) Написание кода только на английском языке
б) Использование ярких цветов в редакторе кода
**в) Написание кода с учётом защиты от уязвимостей**
г) Программирование без подключения к интернету
**15.** Что такое резервное копирование?
а) Удаление старых файлов
б) Шифрование паролей
**в) Создание копии данных на случай их потери**
г) Перемещение файлов на другой диск
**16.** Какой метод управления доступом основан на ролях пользователя?
а) MAC — мандатный контроль доступа
б) DAC — дискреционный контроль доступа
**в) RBAC — ролевой контроль доступа**
г) PGP — шифрование с открытым ключом
**17.** В модели SaaS (Software as a Service) кто отвечает за безопасность приложения?
а) Только пользователь
б) Только владелец сервера
**в) В основном — поставщик сервиса**
г) Никто — безопасность не требуется
**18.** Что такое IaaS в облачных технологиях?
а) Облачная электронная почта
б) Онлайн-сервис для хранения фото
**в) Аренда виртуальных машин и серверов**
г) Облачный антивирус
**19.** Какой этап НЕ входит в процесс реагирования на инцидент?
а) Обнаружение
б) Сдерживание
**в) Увольнение сотрудника**
г) Восстановление

**20.** Что означает «OSINT» в контексте кибербезопасности?
а) Секретная разведывательная операция
б) Шифрование данных в облаке
**в) Сбор открытой информации из публичных источников**
г) Взлом защищённой сети

## 3. КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

### 3.1. Теоретические вопросы промежуточной аттестации

**1.** Дайте определение понятию «информационная безопасность». Назовите три основные с оставляющие информационной безопасности.
**2.** Перечислите три актуальные угрозы информационной безопасности в современных ком пьютерных сетях. Приведите пример реализации одной из них.
**3.** Что такое социальная инженерия? Приведите два примера атак, основанных на этом мет оде.
**4.** Какие меры можно предпринять для защиты от фишинговых атак? Назовите три правил а поведения пользователей.
**5.** Что регулирует Федеральный закон РФ № 152-
ФЗ? Какие категории данных он защищает?
**6.** В чём заключается принцип разделения обязанностей в системе информационной безоп асности? Почему он важен?
**7.** Что такое политика информационной безопасности? Перечислите три обязательных раз дела такой политики в организации.
**8.** Объясните разницу между симметричным и асимметричным шифрованием. Приведите по одному примеру алгоритма каждого типа.
**9.** Для чего используется хэш-
функция? Назовите один популярный алгоритм хэширования и его назначение.
**10.** Что такое электронная цифровая подпись (ЭЦП)? Какие задачи она решает в информац ионной системе?
**11.** Как работает технология VPN? В каких случаях её использование особенно важно?
**12.** Что такое межсетевой экран (фаервол)? Чем отличается программный фаервол от аппа ратного?
**13.** Опишите принцип действия DDoS-
атаки. Какие меры можно применить для защиты от неё?
**14.** Что такое SQL-
инъекция? Как программист может предотвратить такую уязвимость при разработке веб-приложения?
**15.** Объясните, что означает уязвимость «межсайтовый скриптинг (XSS)». Как она может быть использована злоумышленником?
**16.** Зачем необходимо резервное копирование данных? Назовите два способа хранения рез ервных копий и одно правило их организации.
**17.** Что входит в понятие «управление доступом к данным»? Приведите пример реализаци и в операционной системе Windows.
**18.** В чём разница между моделями облачных сервисов IaaS, PaaS и SaaS? Приведите прим ер сервиса для каждой модели.
**19.** Перечислите основные этапы реагирования на инцидент информационной безопасност и. Кратко опишите каждый этап.

**20.** Что такое OSINT? Как открытые источники информации могут использоваться как в ц елях защиты, так и в атаках?

### 3.2 Тестовая часть промежуточной аттестации

**Тестовые задания типа А (Выберите один верный ответ)**
**1.** Что обеспечивает конфиденциальность информации?
а) Возможность быстро восстановить данные
б) Проверка целостности файлов после передачи
**в) Защита от несанкционированного доступа к данным**
г) Регулярное резервное копирование
**2.** Какой из перечисленных методов является примером пассивной угрозы?
а) Удалённый запуск вредоносной программы
б) Блокировка сервера трафиком
**в) Перехват сетевого трафика (сниффинг)**
г) Удаление файлов через вирус
**3.** Какой документ устанавливает требования к защите персональных данных в России?
а) Устав организации
б) Политика в области IT-аутсорсинга
**в) Федеральный закон № 152-ФЗ**
г) Трудовой кодекс РФ
**4.** Что такое «политика безопасности» в организации?
а) Правила внутреннего распорядка
б) Список установленного программного обеспечения
**в) Документ, определяющий правила обращения с информацией**
г) Инструкция по ремонту компьютеров
**5.** Какой стандарт используется для построения системы менеджмента информационной безопасности (СМИБ)?
а) ГОСТ Р 57580
б) PCI DSS
**в) ISO/IEC 27001**
г) IEEE 802.3
**6.** Что означает целостность информации?
а) Данные доступны в любое время
б) Информация зашифрована и скрыта
**в) Данные не были изменены без разрешения**
г) Информация хранится в облаке
**7.** Какой алгоритм используется для асимметричного шифрования?
а) AES
б) SHA-256
**в) RSA**
г) DES
**8.** Что такое цифровая подпись?
а) Электронная копия личной подписи
б) Пароль для входа в систему
**в) Криптографический механизм подтверждения авторства и целостности**
г) Хэш-сумма файла
**9.** Какой метод позволяет скрыть информацию в аудиофайле?
а) Шифрование с помощью 7-Zip
б) Архивация в формате RAR

**в) Стеганография**
г) Хэширование MD5
**10.** Что защищает антивирусная программа?
а) От перегрева процессора
б) От скачков напряжения
**в) От вредоносных программ (вирусов, троянов)**
г) От физического доступа к компьютеру
**11.** Какая атака основана на перехвате и подмене данных между двумя сторонами?
а) DDoS
б) Фишинг
**в) Атака «человек посередине» (MITM)**
г) SQL-инъекция
**12.** Что такое фаервол (межсетевой экран)?
а) Программа для резервного копирования
б) Устройство для подключения к Wi-Fi
**в) Средство фильтрации сетевого трафика**
г) Антивирусный сканер
**13.** Какой протокол обеспечивает шифрование при передаче данных в интернете?
а) HTTP
б) FTP
**в) HTTPS**
г) TCP
**14.** Какой тип атаки использует поддельный сайт, похожий на настоящий?
а) DDoS
б) Вирусная атака
**в) Фишинг**
г) Сниффинг
**15.** Что означает аббревиатура VPN?
а) Виртуальное публичное подключение
б) Визуальный протокол сети
**в) Виртуальная частная сеть**
г) Вертикальная передача данных
**16.** Какая уязвимость позволяет выполнить вредоносный код через веб-форму?
а) Перегрузка сервера
б) Ошибки в дизайне сайта
**в) SQL-инъекция**
г) Медленная загрузка страницы
**17.** Что такое XSS (межсайтовый скриптинг)?
а) Атака на жёсткий диск
б) Способ шифрования паролей
**в) Внедрение вредоносного скрипта в веб-страницу**
г) Ошибка в настройке роутера
**18.** Какой из принципов безопасного программирования помогает избежать переполнения буфера?
а) Использование сложных паролей
б) Регулярное обновление антивируса
**в) Проверка входных данных на длину и тип**
г) Установка фаервола
**19.** Что такое резервное копирование?
а) Удаление ненужных файлов
б) Шифрование паролей

**в) Создание копии данных для восстановления при потере**
г) Перемещение файлов на флешку
**20.** Какой метод резервного копирования хранит только изменившиеся файлы?
а) Полное
б) Зеркальное
**в) Инкрементное**
г) Статическое
**21.** Что такое управление доступом?
а) Контроль скорости интернета
б) Ограничение времени работы за компьютером
**в) Контроль, кто и к каким данным может получить доступ**
г) Настройка яркости экрана
**22.** Какой тип доступа позволяет владельцу файла самому назначать права?
а) Мандатный контроль доступа (MAC)
б) Ролевой контроль (RBAC)
**в) Дискреционный контроль доступа (DAC)**
г) Централизованный контроль
**23.** В модели IaaS клиент управляет:
а) Только приложением
б) Только данными
**в) Виртуальными машинами, ОС и приложениями**
г) Только сетевыми настройками провайдера
**24.** В чём заключается принцип «общей ответственности» в облачных технологиях?
а) Ответственность лежит только на пользователе
б) Облако само защищает все данные
**в) Поставщик и клиент разделяют зоны ответственности за безопасность**
г) Ответственность не регламентирована
**25.** Что такое SaaS?
а) Аренда серверов
б) Разработка программного обеспечения
**в) Использование приложений по подписке через интернет (например, Google Docs)**
г) Настройка локальной сети
**26.** Какой этап НЕ входит в жизненный цикл инцидента информационной безопасности?
а) Обнаружение
б) Сдерживание
**в) Удаление антивируса**
г) Анализ и документирование
**27.** Что включает в себя сдерживание инцидента?
а) Полное игнорирование проблемы
б) Увольнение сотрудника
**в) Отключение заражённого компьютера от сети**
г) Удаление всех данных
**28.** Что такое цифровая криминалистика?
а) Проверка работоспособности принтера
б) Настройка сетевого оборудования
**в) Сбор и анализ цифровых доказательств после атаки**
г) Резервное копирование файлов
**29.** Что означает термин «OSINT»?
а) Секретная операция по взлому
б) Программа шифрования данных
**в) Сбор информации из открытых источников (сайты, соцсети, форумы)**
г) Внутренняя политика компании

**30.** Какой из перечисленных факторов НЕ относится к человеческому риску в ИБ?
а) Незнание правил безопасности
б) Использование слабых паролей
**в) Установка обновлений ОС по расписанию**
г) Переход по подозрительным ссылкам

**Тестовые задания типа В (Установите соответствие между элементами)**

1. Установите соответствие между принципами информационной безопасности и их описанием:

| Понятие | Характеристика |
|---|---|
| а) Конфиденциальность | 1) Данные доступны авторизованным пользователям в нужное время |
| б) Целостность | 2) Информация защищена от несанкционированного доступа |
| в) Доступность | 3) Данные не были изменены без разрешения |

Верный ответ:
а — 2, б — 3, в — 1

2. Установите соответствие между типом угрозы и примером её реализации:

| Тип угрозы | Пример |
|---|---|
| а) Активная угроза | 1) Перехват трафика в открытой Wi-Fi сети |
| б) Пассивная угроза | 2) DDoS-атака, приводящая к отказу сервиса |
| в) Угроза со стороны персонала | 3) Сотрудник копирует клиентские данные на флешку |

Верный ответ:
а — 2, б — 1, в — 3

3. Установите соответствие между моделью облачных сервисов и объёмом контроля пользователя:

| Модель сервиса | Что контролирует пользователь |
|---|---|
| а) IaaS | 1) Только данные и настройки приложения |
| б) PaaS | 2) Приложения, данные, ОС, сеть, серверы |
| в) SaaS | 3) Приложения и данные, ОС и серверы — нет |

Верный ответ:
а — 2, б — 3, в — 1

4. Установите соответствие между средством защиты и его функцией:

| Средство защиты | Назначение |
|---|---|
| а) Антивирус | 1) Фильтрует входящий и исходящий сетевой трафик |
| б) Фаервол | 2) Обнаруживает и удаляет вредоносные программы |
| в) VPN | 3) Обеспечивает зашифрованное удалённое |

| | |
|---|---|
| | подключение к сети |

Верный ответ:
а — 2, б — 1, в — 3

5. Установите соответствие между видом кибератаки и её сутью:

| Вид атаки | Описание |
|---|---|
| а) Фишинг | 1) Внедрение вредоносного скрипта в веб-страницу |
| б) XSS | 2) Поддельное письмо с целью получения логина и пароля |
| в) SQL-инъекция | 3) Ввод в веб-форму команд для доступа к базе данных |

Верный ответ:
а — 2, б — 1, в — 3

6. Установите соответствие между типом резервного копирования и его особенностью:

| Тип резервного копирования | Характеристика |
|---|---|
| а) Полное | 1) Копируются только изменившиеся файлы с момента предыдущего резервного копирования |
| б) Инкрементное | 2) Копируются все файлы независимо от изменений |
| в) Дифференциальное | 3) Копируются все изменённые файлы с момента последнего полного копирования |

Верный ответ:
а — 2, б — 1, в — 3

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

**Задание 1: Подозрительное письмо на корпоративную почту**
Сотрудник отдела бухгалтерии получил письмо от «администрации банка» с темой: «Сроч но Ваш счёт заблокирован». В письме —
ссылка на сайт для «подтверждения данных», внешне очень похожий на настоящий банк. Адрес ссылки сложный и содержит странные символы.
Что должен сделать сотрудник?
а) Перейти по ссылке и ввести данные, чтобы разблокировать счёт
б) Ответить на письмо и уточнить, от кого оно пришло
**в) Не переходить по ссылке и сообщить системному администратору**
г) Сохранить письмо и подождать следующего уведомления

**Задание 2: Подключение к Wi-Fi в кафе**
Студент подключается к бесплатному Wi-
Fi в кафе, чтобы проверить почту и залогиниться в личный кабинет университета. Сеть на зывается «Free_WiFi», пароля нет.
Как ему обеспечить безопасность при работе в такой сети?
а) Использовать любые сайты без ограничений — Wi-Fi бесплатный, значит, безопасный
б) Отключить антивирус, чтобы не мешал работе в интернете

**в) Подключиться через VPN и избегать ввода логинов и паролей без HTTPS**
г) Всегда включать автоматическую синхронизацию данных для быстрого доступа

**Задание 3: Коллега просит пароль от учётной записи**
Системный администратор получил звонок от коллеги: «Привет, я в командировке, не мог у войти в почту — забыл пароль. Дай временно свой, я быстро проверю письма и верну».
Как правильно поступить?
а) Отправить пароль по SMS — это быстро и надёжно
б) Сменить свой пароль на простой и сообщить его коллеге
**в) Отказать и предложить воспользоваться восстановлением доступа через почту ил и SMS**
г) Войти от его имени самому и переслать нужные письма

**Задание 4: Подозрительная активность на компьютере**
У пользователя внезапно замедлилась работа ПК, появились всплывающие окна с надпись ю «Ваш компьютер заражён Нажмите сюда для очистки». Антивирус не установлен.
Что нужно сделать в первую очередь?
а) Нажать на всплывающее окно — оно предлагает помощь
б) Перезагрузить компьютер и продолжить работу
**в) Не нажимать на окна, отключить ПК от сети и сообщить администратору**
г) Скачать первый попавшийся антивирус с сайта из рекламы

## 4. ПОКАЗАТЕЛИ И КРИТЕРИИ ОЦЕНИВАНИЯ

Дифференцированный зачёт проводится в режиме онлайн, студенты отвечают на теоретические вопросы. Ответы предоставляются в виде скан-копий или фотографий.
**Количество вариантов теоретического задания для экзаменующегося** – 1 теоретический вопрос.
**Время выполнения задания** - 30 минут для подготовки по теоретическому вопросу и демонстрация задания одного из выполненных работ по выбору преподавателя на виртуальной машине. Итоговая отметка складывается из среднего значения оценок текущего контроля, составляющих 70% итоговой отметки и устного ответа на вопрос, составляющего 30% итоговой отметки.

Результатом освоения учебной дисциплины являются сформированные умения и освоенные знания:

| Результаты обучения | Показатели освоенности компетенций | Методы оценки |
|---|---|---|
| ***Знает:***<br>- актуальный профессиональный и социальный контекст, в котором приходится работать и жить;<br>-основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; | Ориентируется в профессиональном и социальном контексте, в котором приходится работать и жить;<br>Владеет основными источниками информации и ресурсами для решения задач и проблем в профессиональном и/или социальном контексте; | Экспертное наблюдение выполнения практических работ и видов работ по практике<br>Диагностика (тестирование, контрольные работы) |

| | | |
|---|---|---|
| - алгоритмы выполнения работ в профессиональной и смежных областях;<br>- методы работы в профессиональной и смежных сферах;<br>- структуру плана для решения задач;<br>- порядок оценки результатов решения задач профессиональной деятельности<br>- номенклатуру информационных источников, применяемых в профессиональной деятельности;<br>- приемы структурирования информации;<br>- формат оформления результатов поиска информации, современные средства и устройства информатизации;<br>- порядок применения современных средств и устройств информатизации и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств;<br>- лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности;<br>- принципы безопасности хранения данных;<br>- методы защиты баз данных от внешних угроз<br>- принципы криптографии и методов шифрования данных;<br>- стандарты и протоколы безопасности, таких как | Знает алгоритмы выполнения работ в профессиональной и смежных областях;<br>Знает методы работы в профессиональной и смежных сферах;<br>Знает структуру плана для решения задач;<br>Может произвести оценку результатов решения задач профессиональной деятельности<br>Владеет номенклатурой информационных источников, применяемых в профессиональной деятельности;<br>Знает приемы структурирования информации;<br>Знает формат оформления результатов поиска информации, современные средства и устройства информатизации;<br>Может применять современные средства и устройства информатизации и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств;<br>Владеет лексическим минимумом, относящимся к описанию предметов, средств и процессов профессиональной деятельности;<br>Знает принципы безопасности хранения данных;<br>Владеет методами защиты баз данных от внешних угроз<br>Знает принципы криптографии и методов шифрования данных;<br>Ориентируется в стандартах и протоколах безопасности, | |

| | | |
|---|---|---|
| SSL/TLS, SSH, Kerberos и др.;<br>- методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.;<br>- отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности;<br>- современный отечественный и зарубежный опыт в профессиональной деятельности;<br>- принципы и методы обеспечения безопасности информационных систем;<br>- принципы безопасности информационных систем;<br><br>- современные методы и технологии в области безопасности информационных систем;<br>- законодательные и нормативные акты в области безопасности информационных систем;<br>-источники угроз информационной безопасности и меры по их предотвращению;<br>- основные угрозы безопасности мобильных приложений;<br><br>- принципы криптографии и шифрования данных;<br><br>- стандарты и протоколы безопасности, такие как | таких как SSL/TLS, SSH, Kerberos и др.;<br>Знает методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.;<br>Знает отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности;<br><br>Знает современный отечественный и зарубежный опыт в профессиональной деятельности;<br>Владеет принципами и методами обеспечения безопасности информационных систем;<br>Знает принципы безопасности информационных систем;<br>Владеет современными методами и технологиями в области безопасности информационных систем;<br>Знает законодательные и нормативные акты в области безопасности информационных систем;<br>Знает источники угроз информационной безопасности и меры по их предотвращению;<br>Имеет представление об основных угрозах безопасности мобильных приложений;<br>Ориентируется в принципах криптографии и шифрования данных;<br>Знает стандарты и | |

| | | |
|---|---|---|
| HTTPS, OAuth и OpenID Connect;<br>- законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA;<br>- основные принципы безопасности информации и методов ее защиты;<br><br>- стандартные криптографические алгоритмы для шифрования данных;<br>- принципы обеспечения безопасности передачи данных по сети;<br><br>- основы безопасности приложений и инфраструктуры;<br>- методы анализа на уязвимости и мониторинга безопасности;<br>- знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений;<br>- понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения;<br>- знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы.<br><br>***Умеет:***<br>-распознавать задачу и/или проблему в профессиональном и/или социальном контексте;<br>-анализировать задачу | протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect;<br>Знает законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA;<br>Владеет основными принципами безопасности информации и методов ее защиты;<br>Знает стандартные криптографические алгоритмы для шифрования данных;<br>Имеет представление о принципах обеспечения безопасности передачи данных по сети;<br>Знает основы безопасности приложений и инфраструктуры;<br>Знает методы анализа на уязвимости и мониторинга безопасности;<br><br>Знает основные принципы и методы обеспечения безопасности ИТ-инфраструктуры и веб-приложений;<br>Понимает различные уязвимости и угрозы безопасности, а также способы их предотвращения и обнаружения;<br><br>Знает инструменты и технологии для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы.<br><br><br>Может распознавать задачу и/или проблему в профессиональном и/или социальном контексте;<br>Анализирует задачу и/или | |

| | | |
|---|---|---|
| и/или проблему и выделять её составные части;<br>- определять этапы решения задачи;<br>- выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы;<br>-составлять план действия;<br>- определять необходимые ресурсы;<br>- владеть актуальными методами работы в профессиональной и смежных сферах;<br>- реализовывать составленный план;<br>- оценивать результат и последствия своих действий (самостоятельно или с помощью наставника);<br>- определять задачи для поиска информации;<br>- определять необходимые источники информации;<br>- планировать процесс поиска;<br>- структурировать получаемую информацию; - выделять наиболее значимое в перечне информации;<br>- оценивать практическую значимость результатов поиска;<br>- оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач;<br>- использовать современное программное обеспечение;<br>- использовать различные цифровые средства для решения | проблему и может выделить её составные части;<br>Умеет определять этапы решения задачи;<br>Может выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы;<br>Составляет план действия;<br>Может определять необходимые ресурсы;<br>Владеет актуальными методами работы в профессиональной и смежных сферах;<br>Может реализовывать составленный план;<br>Оценивает результат и последствия своих действий (самостоятельно или с помощью наставника);<br>Умеет определять задачи для поиска информации;<br>Умеет определять необходимые источники информации;<br>Планирует процесс поиска;<br>Умеет структурировать получаемую информацию;<br>Может выделить наиболее значимое в перечне информации;<br>Умеет оценивать практическую значимость результатов поиска;<br>Оформляет результаты поиска и применяет средства информационных технологий для решения профессиональных задач;<br>Может использовать современное программное обеспечение;<br>Может использовать различные цифровые средства для решения | |

| | | |
|---|---|---|
| профессиональных задач;<br>- понимать тексты на базовые профессиональные темы;<br>- шифрование данных и обеспечивает их конфиденциальность;<br>- анализировать требования безопасности информационных систем;<br>- разрабатывать и реализовывать меры безопасности;<br>- реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию. | профессиональных задач;<br>Понимает тексты на базовые профессиональные темы;<br><br>Умеет шифровать данные и обеспечивать их конфиденциальность;<br>Умеет анализировать требования безопасности информационных систем;<br>Может разрабатывать и реализовывать меры безопасности;<br>Может реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию. | |

**Критерии оценки выполнения практических заданий**

При оценивании практической работы студента учитывается следующее:

- качество выполнения практической части работы;
- качество оформления отчета по работе;

Каждый вид работы оценивается по пяти бальной шкале:

«5» (отлично) – за глубокое и полное овладение содержанием учебного материала, в котором студент свободно и уверенно ориентируется; за умение практически применять теоретические знания, высказывать и обосновывать свои суждения. Оценка «5» (отлично) предполагает грамотное и логичное изложение ответа.

«4» (хорошо) – если студент полно освоил учебный материал, владеет научно-понятийным аппаратом, ориентируется в изученном материале, осознанно применяет теоретические знания на практике, грамотно излагает ответ, но содержание и форма ответа имеют отдельные неточности.

«3» (удовлетворительно) – если студент обнаруживает знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности, в применении теоретических знаний при ответе на практико-ориентированные вопросы; не умеет доказательно обосновать собственные суждения.

«2» (неудовлетворительно) – если студент имеет разрозненные, бессистемные знания, допускает ошибки в определении базовых понятий, искажает их смысл; не может практически применять теоретические знания.

Контрольное задание в форме тестов

| Процент результативности (правильных ответов) | Оценка уровня подготовки | |
|---|---|---|
| | балл (отметка) | вербальный аналог |
| 100 - 90 | 5 | отлично |
| 89 - 80 | 4 | хорошо |
| 79 - 70 | 3 | удовлетворительно |
| Менее 70 | 2 | неудовлетворительно |