МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ ВЛАДИМИРА ДАЛЯ»

Краснодонский факультет инженерии и менеджмента (филиал)
Кафедра информационных технологий и транспорта

УТВЕРЖДАЮ:
Директор
Панайотов К.К.
(подпись)
«14» марта 2025 года

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по учебной дисциплине
Защита данных в сетях ЭВМ
(наименование учебной дисциплины, практики)

09.04.01 Информатика и вычислительная техника
(код и наименование направления подготовки (специальности))

«Интеллектуальные системы
в производственно-транспортных комплексах»
наименование профиля подготовки (специальности, магистерской программы); при отсутствии ставится прочерк)

Разработчик(разработчики):
доцент _____ Панайотов К. К.
(подпись)

ФОС рассмотрен и одобрен на заседании кафедры информационных технологий и транспорта от «26» февраля 2025 г., протокол № 7

Заведующий кафедрой
информационных
технологий и транспорта _____ Верительник Е. А.
(подпись)

Краснодон 2025

Комплект оценочных материалов по дисциплине
«Защита данных в сетях ЭВМ»

Задания закрытого типа

Задания закрытого типа на выбор правильного ответа

1. *Выберите один правильный ответ*.
Какой из перечисленных алгоритмов является симметричным алгоритмом шифрования?
А) RSA.
Б) Diffie-Hellman.
В) AES.
Г) SHA-256.
Правильный ответ: В.
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

2. *Выберите один правильный ответ*.
Какой тип атак направлен на перегрузку сетевых ресурсов, делая их недоступными для законных пользователей?
А) Фишинг.
Б) SQL-инъекция.
В) DDoS.
Г) MITM (Man-in-the-Middle).
Правильный ответ: В
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

3. *Выберите один правильный ответ*.
Какой протокол шифрования считается наиболее безопасным для защиты беспроводных сетей Wi-Fi?
А) WEP.
Б) WPA.
В) WPA2.
Г) WPA3.
Правильный ответ: Г
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

4. *Выберите один правильный ответ*.
Какая технология позволяет запускать подозрительные файлы в изолированной среде, чтобы изучить их поведение без риска заражения основной системы?
А) Брандмауэр (Firewall).
Б) Антивирус.
В) Песочница (Sandbox).

Г) Система обнаружения вторжений (IDS).
Правильный ответ: В
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

Задания закрытого типа на установление соответствия

1. *Сопоставьте метод аутентификации с его описанием Каждому элементу левого столбца соответствует только один элемент правого столбца*.

Метод аутентификации	Описание
1) Многофакторная аутентификация (MFA)	А) Использование уникальных биологических характеристик для идентификации пользователя.
2) Биометрическая аутентификация	Б) Использование цифровых сертификатов для подтверждения подлинности пользователя или устройства.
3) Аутентификация на основе сертификатов	В) Использование нескольких независимых факторов для подтверждения личности пользователя.
4) Аутентификация по паролю	Г) Использование секретного слова или фразы для идентификации пользователя.

Правильный ответ: 1-Г, 2-В, 3-А, 4-Б
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

2. *Сопоставьте тип вредоносного программного обеспечения с его описанием. Каждому элементу левого столбца соответствует только один элемент правого столбца*.

Тип ПО	Описание
1) Вирус	А) Вредоносная программа, которая маскируется под полезное ПО.
2) Червь	Б) Вредоносная программа, которая шифрует данные и требует выкуп за их расшифровку.
3) Троянский конь	В) Вредоносная программа, которая распространяется, копируя себя на другие компьютеры в сети.
4) Программа-вымогатель (Ransomware)	Г) Вредоносная программа, которая внедряется в другие файлы и распространяется при их запуске.

Правильный ответ: 1-Г, 2-В, 3-А, 4-Б
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

3. *Сопоставьте протокол безопасности с его функцией. Каждому элементу левого столбца соответствует только один элемент правого столбца*.

Протокол	Функция
1) SSL/TLS	А) Безопасная передача файлов по сети.
2) IPsec	Б) Обеспечение конфиденциальности и целостности данных, передаваемых между веб-сервером и браузером.
3) HTTPS	В) Безопасность на сетевом уровне, обеспечивающая защиту для всех IP-трафиков.
4) SFTP	Г) Общий термин для протоколов, обеспечивающих шифрование соединений в Интернете.

Правильный ответ: 1-Г, 2-В, 3-Б, 4-А
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

4. *Сопоставьте метод защиты от утечек данных с его описанием. Каждому элементу левого столбца соответствует только один элемент правого столбца*.

Уровень RAID	Описание
1) Шифрование данных (Data Encryption)	А) Скрытие конфиденциальных данных путем замены их на фиктивные значения.
2) Маскирование данных (Data Masking)	Б) Отслеживание действий пользователей в сети для выявления подозрительной активности.
3) Мониторинг активности пользователей (User Activity Monitoring)	В) Преобразование данных в нечитаемый формат для защиты от несанкционированного доступа.
4) Контроль доступа (Access Control)	Г) Ограничение доступа к данным только авторизованным пользователям и процессам.

Правильный ответ: 1-В, 2-А, 3-Б, 4-Г
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

Задания закрытого типа на установление правильной последовательности

1. *Расположите этапы реагирования на инцидент безопасности в правильном порядке. Запишите правильную последовательность букв слева направо*:
А) Идентификация и анализ инцидента.
Б) Локализация и сдерживание инцидента.
В) Восстановление системы.

Г) Подготовка к реагированию на инцидент.
Д) Устранение последствий инцидента.
Правильный ответ: Г, А, Б, Д, В.
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

2. *Расположите шаги проведения аудита безопасности в правильном порядке. Запишите правильную последовательность букв слева направо*:
А) Подготовка отчета об аудите.
Б) Определение области аудита.
В) Сбор данных и анализ.
Г) Планирование аудита.
Д) Реализация рекомендаций.
Правильный ответ: Г, Б, В, А, Д.
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

3. *Расположите шаги развертывания системы обнаружения вторжений (IDS) в правильном порядке. Запишите правильную последовательность букв слева направо*:
А) Конфигурация и настройка IDS.
Б) Определение требований к системе IDS.
В) Мониторинг и анализ результатов.
Г) Выбор подходящего решения IDS.
Д) Тестирование и оптимизация.
Правильный ответ: Б, Г, А, Д, В.
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

4. *Расположите шаги создания надежного пароля. Запишите правильную последовательность букв слева направо*:
А) Избегать использования личной информации (имена, даты рождения и т.п.).
Б) Использовать генератор паролей (если возможно).
В) Использовать комбинацию букв верхнего и нижнего регистра, цифр и специальных символов.
Г) Выбрать пароль длиной не менее 12 символов.
Правильный ответ: Г, В, А, Б.
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

Задания открытого типа

Задания открытого типа на дополнение
1. *Напишите пропущенное слово или словосочетание*.
_____ действует как барьер, контролируя входящий и исходящий сетевой трафик на основе заданных правил, предотвращая несанкционированный доступ к сети.

Правильный ответ: Межсетевой экран / Брандмауэр / Firewall
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

2. *Напишите пропущенное слово или словосочетание.*
Для выявления уязвимостей и слабых мест в информационной системе проводится регулярный _____, который включает в себя сканирование на наличие известных уязвимостей и тестирование на проникновение.
Правильный ответ: анализ защищенности / анализ безопасности.
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

3. *Напишите пропущенное слово или словосочетание.*
Подтверждением подлинности и целостности электронного документа или программного обеспечения служит _____, созданная с использованием криптографических алгоритмов.
Правильный ответ: цифровая подпись / электронная подпись.
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

4. *Напишите пропущенное слово или словосочетание.*
Разделение сети на более мелкие, изолированные сегменты позволяет ограничить радиус поражения в случае компрометации одного из сегментов, что повышает общую _____.
Правильный ответ: безопасность / защищенность.
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

Задания открытого типа с кратким свободным ответом
1. *Дайте ответ на вопрос.*
Как называется метод сокрытия информации внутри другого файла, например, изображения или аудиофайла?
Правильный ответ: Стеганография / Сокрытие
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

2. *Дайте ответ на вопрос.*
Как называется попытка получить конфиденциальную информацию, такую как имена пользователей, пароли и данные кредитных карт, выдавая себя за доверенное лицо или организацию?
Правильный ответ: Фишинг / Выуживание
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

3. *Дайте ответ на вопрос.*
Как называется создание копии данных для восстановления в случае потери или повреждения?
Правильный ответ: Резервирование / Бэкап
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

4. *Дайте ответ на вопрос*.
Как называется слабое место в системе, которое может быть использовано злоумышленником для нанесения ущерба?
Правильный ответ: Уязвимость / Дыра.
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

Задания открытого типа с развернутым ответом

1. *Дайте развернутый ответ на вопрос*.
Опишите подробно основные меры по защите периметра корпоративной сети. Обоснуйте важность каждого из предложенных вами средств защиты?
Время выполнения: 20 мин.
Ожидаемый результат:
Защита периметра сети является критически важной для предотвращения несанкционированного доступа к внутренним ресурсам. Основными мерами являются.
1. Межсетевой экран (Firewall). Фильтрует сетевой трафик на основе заданных правил, блокируя нежелательные соединения. Важен для предотвращения атак извне, таких как сканирование портов и DDoS.
2. Системы обнаружения и предотвращения вторжений (IDS/IPS). Обнаруживают подозрительную активность в сети и могут автоматически блокировать атаки. Важны для выявления атак, которые прошли через межсетевой экран.
3. Прокси-сервер. Действует как посредник между внутренними пользователями и внешними ресурсами, скрывая внутреннюю структуру сети и контролируя доступ к внешним сайтам. Важен для предотвращения утечек данных и фильтрации контента.
4. Виртуальные частные сети (VPN). Обеспечивают зашифрованное соединение для удаленных пользователей, обеспечивая безопасный доступ к корпоративным ресурсам. Важны для защиты данных при передаче по незащищенным сетям.
5. Аутентификация и авторизация. Строгая проверка подлинности пользователей при доступе к сети и ограничение прав доступа в соответствии с принципом наименьших привилегий. Важны для предотвращения несанкционированного доступа со стороны злоумышленников или внутренних пользователей.
Критерии оценивания: наличие в ответе трёх основных мер по защите периметра корпоративной сети.
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

2. *Дайте развернутый ответ на вопрос.*
Опишите различные методы защиты данных при хранении, как локально, так и в облачных средах. Объясните, какие угрозы могут быть нейтрализованы с помощью каждого из этих методов.

Время выполнения: 20 мин.
Ожидаемый результат:
Защита данных при хранении является важным аспектом информационной безопасности, так как данные часто являются наиболее ценным активом организации. Методы защиты включают.
1. Шифрование. Преобразование данных в нечитаемый формат, доступный только при наличии ключа шифрования. Защищает от несанкционированного доступа к данным в случае кражи или потери носителя.
2. Контроль доступа. Ограничение доступа к данным на основе ролей и привилегий. Защищает от несанкционированного доступа со стороны внутренних пользователей.
3. Маскирование данных. Замена конфиденциальных данных фиктивными значениями, сохраняя при этом структуру данных. Используется для защиты данных при разработке и тестировании, а также в аналитических системах.
4. Удаление данных. Безопасное удаление данных, предотвращающее их восстановление. Используется при утилизации оборудования или выводе его из эксплуатации.
5. DLP (Data Loss Prevention). Обнаружение и предотвращение утечек конфиденциальных данных за пределы организации. Используется для защиты от несанкционированной передачи данных по электронной почте, веб-трафику и другим каналам.
Критерии оценивания: наличие в ответе трёх методов защиты данных при хранении.
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

3. *Дайте развернутый ответ на вопрос.*
Опишите наиболее распространенные типы атак на веб-приложения и методы защиты от них.
Время выполнения: 20 мин.
Ожидаемый результат:
Веб-приложения являются частой целью для злоумышленников, так как они часто имеют прямой доступ к конфиденциальным данным. Наиболее распространенные типы атак включают.
1. SQL-инъекции. Внедрение вредоносного SQL-кода в запросы к базе данных. Защита – использование параметризованных запросов и валидация входных данных.
2. Межсайтовый скриптинг (XSS). Внедрение вредоносного JavaScript-кода на веб-страницу, который выполняется в браузере пользователя. Защита – экранирование выводимых данных и Content Security Policy (CSP).
3. Межсайтовая подделка запросов (CSRF). Выполнение авторизованным пользователем нежелательных действий на веб-сайте без его ведома. Защита – использование CSRF-токенов.
4. Включение локальных/удаленных файлов (LFI/RFI). Эксплуатация уязвимостей, позволяющих злоумышленнику включать файлы с сервера или

из внешних источников. Защита – валидация входных данных и ограничение доступа к файловой системе.
5. Атаки перебора паролей (Brute-force). Попытки подбора пароля путем перебора различных комбинаций. Защита – сложные пароли, ограничение количества попыток входа и двухфакторная аутентификация.
Критерии оценивания: наличие в ответе трёх типов атак.
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

4. *Дайте развернутый ответ на вопрос.*
Опишите этапы реагирования на инцидент информационной безопасности. Объясните, какие действия необходимо предпринять на каждом этапе, чтобы эффективно локализовать, устранить и восстановить систему после инцидента.
Время выполнения: 20 мин.
Ожидаемый результат:
Реагирование на инцидент – это структурированный процесс, предназначенный для управления и минимизации последствий инцидентов информационной безопасности. Этот процесс обычно состоит из нескольких этапов.
Первый этап – подготовка, включает разработку планов реагирования на инциденты, создание команды реагирования, определение каналов связи и сбор информации об инфраструктуре.
Второй этап – выявление и анализ. На этом этапе происходит обнаружение признаков инцидента, например, аномальной активности в журналах, сообщений от пользователей или срабатывания систем обнаружения вторжений. Анализ позволяет определить тип инцидента, его масштаб и потенциальный ущерб.
Третий этап – локализация и сдерживание. Цель этого этапа – предотвратить дальнейшее распространение инцидента. Действия могут включать отключение зараженных систем от сети, блокировку доступа к ресурсам или изменение паролей.
Четвертый этап – устранение. На этом этапе удаляется вредоносное программное обеспечение, исправляются уязвимости и восстанавливаются системы из резервных копий.
Пятый этап – восстановление. На этом этапе возвращаются в строй все системы и сервисы, убедившись в их работоспособности и безопасности.
Шестой этап – послеинцидентный анализ. Проводится анализ причин инцидента, выявляются слабые места в системе защиты и разрабатываются меры по предотвращению подобных инцидентов в будущем.
Критерии оценивания: каждый этап реагирования на инцидент должен быть описан минимум одним предложением.
Компетенции (индикаторы): ОПК-5 (ОПК-5.2).

Экспертное заключение

Представленный фонд оценочных средств (далее – ФОС) по дисциплине «Защита данных в сетях ЭВМ» соответствует требованиям ФГОС ВО.

Предлагаемые формы и средства текущего и промежуточного контроля адекватны целям и задачам реализации основной профессиональной образовательной программы по направлению подготовки 09.04.01 Информатика и вычислительная техника.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины представлены в полном объеме.

Виды оценочных средств, включенные в представленный фонд, отвечают основным принципам формирования ФОС.

Разработанный и представленный для экспертизы фонд оценочных средств рекомендуется к использованию в процессе подготовки обучающихся по указанному направлению 09.04.01 Информатика и вычислительная техника.

Председатель учебно-методической комиссии Краснодонского факультета инженерии и менеджмента (филиала) _____ Родионова О.Ю.

Лист изменений и дополнений

№ п/п	Виды дополнений и изменений	Дата и номер протокола заседания кафедры (кафедр), на котором были рассмотрены и одобрены изменения и дополнения	Подпись (с расшифровкой) заведующего кафедрой (заведующих кафедрами)