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

Институт компьютерных систем и информационных технологий
Кафедра компьютерных систем и сетей

УТВЕРЖДАЮ
Директор _____ Кочевский А. А.
(подпись)
«10» 03 2025 года

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по учебной дисциплине

«Защита данных в сетях ЭВМ»
09.04.01 Информатика и вычислительная техника
«Сети ЭВМ и телекоммуникации»

Разработчик:
доцент _____ Попов С.В.
(подпись)

ФОС рассмотрен и одобрен на заседании кафедры
компьютерных систем и сетей

от «10» 03 2025 г., протокол № 8

Заведующий кафедрой _____ Попов С. В.
(подпись)

Луганск 2025 г.

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 протокол обеспечивает защиту данных при передаче по сети Интернет?
А) HTTP.
Б) FTP.
В) HTTPS.
Г) SMTP.
Правильный ответ: В
Компетенции (индикаторы): ПК-1, ПК-4

2. Выберите один правильный ответ
Что такое "атака типа "Man-in-the-Middle"?
А) Внедрение вредоносного ПО в систему.
Б) Перехват и изменение данных между двумя сторонами.
В) Подбор паролей методом грубой силы.
Г) Атака на физическую инфраструктуру сети.
Правильный ответ: Б
Компетенции (индикаторы): ПК-1, ПК-4

3. Выберите один правильный ответ
Какой из перечисленных алгоритмов используется для создания электронной подписи?
А) MD5.
Б) SHA-256.
В) RSA.
Г) AES.
Правильный ответ: В
Компетенции (индикаторы): ПК-1, ПК-4

4. Выберите один правильный ответ
Что такое "блокчейн" в контексте защиты данных?
А) Метод шифрования данных.
Б) Децентрализованная база данных, защищенная криптографией.
В) Протокол для передачи данных.
Г) Система управления ключами шифрования.
Правильный ответ: Б

Компетенции (индикаторы): ПК-1

Задания закрытого типа на установление соответствия

1. Установите соответствие между типами атак и их описаниями:

	Тип атаки		Описание
1)	Фишинг	А)	Атака, направленная на переполнение ресурсов системы запросами
2)	DDoS-атака	Б)	Внедрение вредоносного кода в базы данных через уязвимости в SQL-запросах
3)	SQL-инъекция	В)	Получение конфиденциальной информации через манипуляции с людьми
4)	Социальная инженерия	Г)	Поддельные сообщения или сайты для получения данных пользователей

Правильный ответ:

1	2	3	4
Г	А	Б	В

Компетенции (индикаторы): ПК-1, ПК-4

2. Установите соответствие между протоколами и их назначением:

	Протокол		Назначение
1)	SSL/TLS	А)	Защита данных при передаче по IP-сетям
2)	IPsec	Б)	Шифрование электронной почты
3)	SSH	В)	Безопасный удаленный доступ к серверам
4)	PGP	Г)	Защита данных при передаче по HTTP

Правильный ответ:

1	2	3	4
Г	А	В	Б

Компетенции (индикаторы): ПК-1, ПК-4

3. Установите соответствие между стандартами и их назначением:

	Стандарт		Назначение
1)	GDPR	А)	Защита персональных данных в Европейском Союзе
2)	PCI DSS	Б)	Защита данных в медицинских учреждениях

3)	HIPAA	В)	Стандарт для управления информационной безопасностью
4)	ISO 27001	Г)	Стандарт для защиты данных в платежных системах

Правильный ответ:

1	2	3	4
А	Г	Б	В

Компетенции (индикаторы): ПК-1

4. Установите соответствие между типами ключей и их использованием:

Тип ключа		Использование ключа	
1)	Открытый ключ	А)	Используется для расшифрования данных в асимметричных системах
2)	Закрытый ключ	Б)	Используется для шифрования данных в асимметричных системах
3)	Сессионный ключ	В)	Временный ключ для шифрования данных в сессии
4)	Мастер-ключ	Г)	Ключ, используемый для генерации других ключей

Правильный ответ:

1	2	3	4
Б	А	В	Г

Компетенции (индикаторы): ПК-1, ПК-4

Задания закрытого типа на установление правильной последовательности

1. Установите правильную последовательность этапов создания цифровой подписи:

А) Хэширование данных.

Б) Шифрование хэша с использованием закрытого ключа.

В) Передача данных вместе с подписью.

Г) Проверка подписи с использованием открытого ключа.

Правильный ответ: А, Б, В, Г

Компетенции (индикаторы): ПК-1, ПК-4

2. Установите правильную последовательность этапов установления защищенного соединения по протоколу SSL/TLS:

А) Обмен сертификатами и проверка подлинности.

Б) Установление TCP-соединения.

В) Обмен ключами и настройка шифрования.

Г) Начало защищенной передачи данных.

Правильный ответ: Б, А, В, Г

Компетенции (индикаторы): ПК-1, ПК-4

3. Установите правильную последовательность этапов обработки данных в системе с использованием брандмауэра:

А) Анализ входящего трафика по правилам брандмауэра.

Б) Принятие решения о разрешении или блокировке пакета.

В) Передача пакета в защищенную сеть.

Г) Получение пакета из внешней сети.

Правильный ответ: Г, А, Б, В

Компетенции (индикаторы): ПК-1, ПК-4

4. Установите правильную последовательность этапов работы системы управления ключами шифрования:

А) Генерация ключей.

Б) Распределение ключей между пользователями.

В Хранение ключей в защищенном хранилище

Г) Обновление или отзыв ключей при необходимости.

Правильный ответ: А, Б, В, Г

Компетенции (индикаторы): ПК-1, ПК-4

Задания открытого типа

Задания открытого типа на дополнение

1. Напишите пропущенное слово (словосочетание).

Протокол _____ обеспечивает защиту данных при передаче по сети Интернет путем шифрования трафика между клиентом и сервером.

Правильный ответ: HTTPS.

Компетенции (индикаторы): ПК-1, ПК-4

2. Напишите пропущенное слово (словосочетание).

Метод шифрования, при котором для шифрования и расшифрования используется один и тот же ключ, называется _____ шифрованием.

Правильный ответ: симметричным.

Компетенции (индикаторы): ПК-1, ПК-4

3. Напишите пропущенное слово (словосочетание).

_____ — это метод сокрытия информации внутри других данных, например, в изображениях или аудиофайлах.

Правильный ответ: стеганография.

Компетенции (индикаторы): ПК-1, ПК-4

4. Напишите пропущенное слово (словосочетание).

_____ — это процесс проверки подлинности пользователя, например, с помощью пароля, биометрических данных или одноразового кода.

Правильный ответ: аутентификация.

Компетенции (индикаторы): ПК-1, ПК-4

5. Напишите пропущенное слово (словосочетание).

Алгоритм _____ используется для создания цифровой подписи и обеспечивает проверку подлинности и целостности данных.

Правильный ответ: RSA.

Компетенции (индикаторы): ПК-1, ПК-4

Задания открытого типа с кратким свободным ответом

1. Напишите пропущенное слово (словосочетание).

1. _____ — это вредоносное программное обеспечение, которое блокирует доступ к данным и требует выкуп для их разблокировки.

Правильный ответ: Ransomware / шифровальщик

Компетенции (индикаторы): ПК-1, ПК-4

2. Дайте ответ на вопрос.

Как регулируют защиту персональных данных в РФ?

Правильный ответ: Федеральный закон/Закон о персональных данных/Трудовой кодекс

Компетенции (индикаторы): ПК-1

3. Дайте ответ на вопрос

Назовите основные типы сетевых атак..

Правильный ответ: DDoS-атака, фишинг, SQL-инъекция, Man-in-the-Middle.

Компетенции (индикаторы): ПК-1, ПК-4

4. Дайте ответ на вопрос

Перечислите основные методы аутентификации пользователей.

Правильный ответ: Пароли, биометрические данные, одноразовые коды, сертификаты.

Компетенции (индикаторы): ПК-1

5. Дайте ответ на вопрос

Перечислите основные протоколы, обеспечивающие защиту данных при передаче.

Правильный ответ: HTTPS, SSL/TLS, IPsec, SSH.

Компетенции (индикаторы): ПК-1, ПК-4

Задания открытого типа с развернутым ответом

1. Оцените суммарную максимальную и суммарную минимальную величину ущерба от реализации совокупности следующих угроз:

1) Неумышленные действия (ошибки) персонала;

2) Атаки злоумышленников;

3) Другие угрозы

При этом первая угроза может возникнуть с вероятностью 20% (потери от ее реализации могут составить максимально от 1 млн.руб. до минимально 200 тыс.руб.), а соответствующие финансовые потери от каждой последующей угрозы составляют 40% от соответствующих максимальных и минимальных потерь от реализации предыдущей угрозы. Вероятности второй и третьей угрозы составляют соответственно 10% и 5%.

Привести расширенное описание.

Время выполнения – 60 мин.

Ожидаемый результат:

Для оценки суммарной максимальной и минимальной величины ущерба от реализации совокупности угроз необходимо рассчитать возможные потери для каждой угрозы с учетом их вероятностей и зависимости потерь от предыдущей угрозы. У нас есть три угрозы:

1. Неумышленные действия (ошибки) персонала:

- Вероятность: 20% (0.2).
- Максимальные потери: 1 млн. руб.
- Минимальные потери: 200 тыс. руб.

2. Атаки злоумышленников:

- Вероятность: 10% (0.1).
- Потери составляют 40% от потерь первой угрозы.

3. Другие угрозы: - Вероятность: 5% (0.05).

- Потери составляют 40% от потерь второй угрозы.

Шаг 1: Расчет потерь для каждой угрозы

Угроза 1: Неумышленные действия персонала

- Максимальные потери: $L_1^{max} = 1000000$ руб.
- Минимальные потери: $L_1^{min} = 200000$ руб.

Угроза 2: Атаки злоумышленников

Потери составляют 40% от потерь первой угрозы:

- Максимальные потери: $L_2^{max} = 0{,}4 * L_1^{max} = 0{,}4 * 1000000 = 400000$ руб.
- Минимальные потери: $L_2^{min} = 0{,}4 * L_1^{min} = 0{,}4 * 200000 = 80000$руб.

Угроза 3: Другие угрозы

Потери составляют 40% от потерь второй угрозы:

- Максимальные потери: $L_3^{max} = 0{,}4 * L_2^{max} = 0{,}4 * 400000 = 160000$руб.
- Минимальные потери: $L_3^{min} = 0{,}4 * L_2^{min} = 0{,}4 * 80000 = 32000$руб.

Шаг 2: Расчет ожидаемых потерь для каждой угрозы

Ожидаемые потери рассчитываются как произведение вероятности угрозы на соответствующие потери.

Угроза 1:

- Ожидаемые максимальные потери: $E_1^{\max} = P_1 * L_1^{\max} = 0{,}2 * 1000000 = 200000$ руб.

- Ожидаемые минимальные потери: $E_1^{\min} = P_1 * L_1^{\min} = 0{,}2 * 200000 = 40000$ руб.

Угроза 2:

- Ожидаемые максимальные потери: $E_2^{\max} = P_2 * L_2^{\max} = 0{,}1 * 400000 = 40000$ руб.

- Ожидаемые минимальные потери: $E_2^{\min} = P_2 * L_2^{\min} = 0{,}1 * 80000 = 8000$ руб.

Угроза 3:

- Ожидаемые максимальные потери: $E_3^{\max} = P_3 * L_3^{\max} = 0{,}05 * 160000 = 8000$руб.

- Ожидаемые минимальные потери: $E_3^{\min} = P_3 * L_3^{\min} = 0{,}05 * 32000 = 1600$руб.

Шаг 3: Расчет суммарных ожидаемых потерь

Суммарные ожидаемые потери рассчитываются как сумма ожидаемых потерь от всех угроз.

Суммарные максимальные потери:

$$E_{total}^{\max} = E_1^{\max} + E_2^{\max} + E_3^{\max} = 200000 + 40000 + 8000 = 248000$$

Суммарные минимальные потери:

$$E_{total}^{\min} = E_1^{\min} + E_2^{\min} + E_3^{\min} = 40000 + 8000 + 1600 = 49600$$

Правильный ответ: Суммарная максимальная величина ущерба от реализации совокупности угроз составляет 248 000 рублей, а суммарная минимальная величина ущерба — 49 600 рублей.

Компетенции (индикаторы): ПК-1, ПК-4

2. Рассчитайте, во сколько раз разнятся времена раскрытия пароля при использовании в пароле только символов стандартной клавиатуры (256 символов) или только всех букв русского алфавита, если длина пароля в первом случае составляет пять символов, во втором случае – десять символов. При этом время ввода пароля во втором случае в два раза больше, чем в первом.:

Привести расширенное решение.

Время выполнения – 60 мин.

Ожидаемый результат:

Для расчета разницы во времени раскрытия пароля необходимо учитывать:

1. Количество возможных комбинаций пароля.

2. Время ввода пароля.

Исходные данные:

1. Первый случай:

- Используются символы стандартной клавиатуры (256 символов).

- Длина пароля: 5 символов.

- Время ввода пароля: t_1.

2. Второй случай:

- Используются только буквы русского алфавита (33 буквы).

- Длина пароля: 10 символов.

- Время ввода пароля: $t_2 = 2*t_1$.

Шаг 1: Расчет количества возможных комбинаций

Первый случай:

Количество возможных комбинаций для пароля из 5 символов при использовании 256 символов:

$$N_1 = 256^5$$

Второй случай:

Количество возможных комбинаций для пароля из 10 символов при использовании 33 букв:

$$N_2 = 33^{10}$$

Шаг 2: Расчет времени раскрытия пароля

Время раскрытия пароля пропорционально количеству возможных комбинаций и времени ввода одной попытки.

Первый случай:

Время раскрытия пароля:

$$T_1 = N_1 * t_1 = 256^5 * t_1$$

Второй случай:

Время раскрытия пароля:

$$T_2 = N_2 * t_2 = 33^{10} * 2t_1$$

Шаг 3: Расчет отношения времен раскрытия

Необходимо найти отношение $\frac{T_2}{T_1}$:

$$\frac{T_2}{T_1} = \frac{33^{10} * 2t_1}{256^5 * t_1} = \frac{33^{10} * 2}{256^5}$$

Упростим выражение:

$$\frac{T_2}{T_1} = 2 * \left(\frac{33^{10}}{256^5} \right)$$

Шаг 4: Вычисление численного значения

1. Вычислим 256^5:

$$256^5 = \left(2^8\right)^5 = 2^{40} \approx 1{,}1 * 10^{12}$$

2. Вычислим 33^{10}:

$$33^{10} \approx 1{,}5 * 10^{15}$$

3. Подставим значения в формулу:

$$\frac{T_2}{T_1} = 2 * \left(\frac{1{,}5 * 10^{15}}{1{,}1 * 10^{12}} \right) \approx 2 * 1363{,}6 \approx 2727{,}2$$

Правильный ответ: Время раскрытия пароля во втором случае (10 символов из 33 букв) примерно в 2727 раз больше, чем в первом случае (5 символов из 256 символов стандартной клавиатуры).

Компетенции (индикаторы): ПК-1, ПК-4

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.

Председатель учебно-методической
комиссии института компьютерных
систем и информационных технологий Ветрова Н.Н.

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)