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)
«12» 03 2025 года

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по учебной дисциплине

«Информационная безопасность»
40.04.01 Юриспруденция
«Юрист в сфере цифровой экономики»

Разработчик:
ст. преп. _____ Зверева О.С.
(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
«Информационная безопасность»

Задания закрытого типа

Задания закрытого типа на выбор правильного ответа

1. Выберите один правильный ответ

Что такое информационная безопасность?

А) Процесс защиты информации от несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения.

Б) Метод создания программного обеспечения для обработки данных.

В) Технология для ускорения передачи данных в сети.

Г) Способ повышения производительности компьютера

Правильный ответ: А

Компетенции (индикаторы):

2. Выберите один правильный ответ

Какой из перечисленных методов является примером двухфакторной аутентификации?

А) Ввод пароля.

Б) Ввод пароля и подтверждение через SMS-код.

В) Шифрование данных

Г) Использование антивирусного программного обеспечения.

Правильный ответ: Б

Компетенции (индикаторы):

3. Выберите один правильный ответ

Что такое социальная инженерия?

А) Метод защиты данных с помощью шифрования.

Б) Способ манипулирования людьми для получения конфиденциальной информации.

В) Технология для создания безопасных сетей.

Г) Процесс резервного копирования данных.

Правильный ответ: Б

Компетенции (индикаторы):

4. Выберите один правильный ответ

Какой из перечисленных методов используется для защиты от вредоносного программного обеспечения?

А) Установка брандмауэра.

Б) Шифрование данных.

В) Резервное копирование

Г) Использование антивирусных программ.

Правильный ответ: Г
Компетенции (индикаторы):

Задания закрытого типа на установление соответствия

1. Установите соответствие между типами угроз и их описаниями:.

Тип угрозы		Описание	
1)	Фишинг	А)	Атака, направленная на перегрузку сервера или сети большим количеством запросов.
2)	DDoS-атака	Б)	Вредоносная программа, способная к самовоспроизведению и распространению
3)	Вирус	В)	Метод манипулирования людьми для получения конфиденциальной информации
4)	Социальная инженерия	Г)	Мошенническая попытка получить личные данные через поддельные письма или сайты.

Правильный ответ:

1	2	3	4
Г	А	Б	В

Компетенции (индикаторы):

2. Установите соответствие между типами защиты и их описаниями:

Тип защиты		Описание	
1)	Антивирусное ПО	А)	Защита данных путем преобразования их в нечитаемый формат.
2)	Брандмауэр	Б)	Программа для обнаружения и удаления вредоносного ПО
3)	Шифрование	В)	Создание копий данных для восстановления в случае потери.
4)	Резервное копирование	Г)	Система для контроля и фильтрации сетевого трафика

Правильный ответ:

1	2	3	4
Б	Г	А	В

Компетенции (индикаторы):

3. Установите соответствие между типами вредоносного ПО и их описаниями:

Тип вредоносного ПО		Описание
1) Вирус	А)	Программа, которая маскируется под легитимное ПО, но выполняет вредоносные действия.
2) Троян	Б)	Вредоносная программа, распространяющаяся через сеть без участия пользователя.
3) Черви	В)	Программа, которая отображает нежелательную рекламу
4) Рекламное ПО	Г)	Вредоносная программа, способная к самовоспроизведению и внедрению в другие файлы.

Правильный ответ:

1	2	3	4
Г	А	Б	В

Компетенции (индикаторы):

4. Установите соответствие между типами аутентификации и их примерами:

Тип аутентификации		Определение
1) Пароль	А)	Использование отпечатка пальца или сканирования лица.
2) Биометрическая аутентификация	Б)	Ввод пароля и подтверждение через SMS-код.
3) Двухфакторная аутентификация	В)	Использование цифрового ключа для подтверждения личности
4) Сертификаты	Г)	Ввод секретного набора символов.

Правильный ответ:

1	2	3	4
Г	А	Б	В

Компетенции (индикаторы):

Задания закрытого типа на установление правильной последовательности

1. Установите правильную последовательность этапов обработки инцидента информационной безопасности:

А) Анализ и расследование.
Б) Обнаружение инцидента.
В) Устранение последствий.
Г) Составление отчета.
Правильный ответ: Б, А, В, Г
Компетенции (индикаторы):

2. Установите правильную последовательность этапов жизненного цикла информации:
А) Хранение.
Б) Уничтожение.
В) Сбор.
Г) Обработка.
Правильный ответ: В, Г, А, Б
Компетенции (индикаторы):

3. Установите правильную последовательность этапов создания цифровой подписи:
А) Хэширование данных.
Б) Шифрование хэша с использованием закрытого ключа.
В) Передача данных и подписи получателю.
Г) Проверка подписи с использованием открытого ключа.
Правильный ответ: А, Б, В, Г
Компетенции (индикаторы):

4. Установите правильную последовательность этапов реагирования на утечку данных:
А) Идентификация утечки.
Б) Блокировка утечки.
В) Оценка ущерба.
Г) Уведомление заинтересованных сторон.
Правильный ответ: А, Б, В, Г
Компетенции (индикаторы):

Задания открытого типа

Задания открытого типа на дополнение

1. Напишите пропущенное слово (словосочетание).
Брандмауэр используется для контроля и _____ сетевого трафика на основе заданных правил.
Правильный ответ: фильтрации.
Компетенции (индикаторы):

2. Напишите пропущенное слово (словосочетание).

Процесс шифрования включает преобразование данных с использованием _____, передачу зашифрованных данных и их расшифровку..

Правильный ответ: ключа.

Компетенции (индикаторы):

3. Напишите пропущенное слово (словосочетание).

Основные принципы информационной безопасности включают конфиденциальность, _____ и доступность.

Правильный ответ: целостность.

Компетенции (индикаторы):

4. Напишите пропущенное слово (словосочетание).

Основные типы вредоносного ПО включают вирусы, _____, черви и рекламное ПО.

Правильный ответ: трояны.

Компетенции (индикаторы):

5. Напишите пропущенное слово (словосочетание).

Социальная инженерия — это метод мошенничества, при котором злоумышленники манипулируют _____ для получения конфиденциальной информации.

Правильный ответ: людьми.

Компетенции (индикаторы):

Задания открытого типа с кратким свободным ответом

1. Дайте ответ на вопрос.

Как регулируют защиту персональных данных в РФ?

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

Компетенции (индикаторы):

2. Дайте ответ на вопрос.

Какие меры должен предпринять юрист для защиты конфиденциальной информации?

Правильный ответ: шифрование, двухфакторной аутентификация, антивирусное ПО, обучение сотрудников.

Компетенции (индикаторы):

3. Дайте ответ на вопрос

Какие последствия могут наступить за нарушение законодательства о персональных данных?

Правильный ответ: Штраф/приостановление деятельности/возмещение ущерба/уголовная ответственность.

Компетенции (индикаторы):

4. Дайте ответ на вопрос

Какие меры ответственности предусмотрены за утечку персональных данных?

Правильный ответ: Административные штрафы/ гражданско-правовая ответственность /уголовная ответственность.

Компетенции (индикаторы):

5. Дайте ответ на вопрос

Что такое коммерческая тайна и как она защищается?

Правильный ответ: информация, которая имеет ценность для бизнеса и защищается с помощью режима коммерческой тайны.

Компетенции (индикаторы):

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): ….

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): ….

Экспертное заключение

Представленный фонд оценочных средств (далее – ФОС) по дисциплине «Информационная безопасность» соответствует требованиям ФГОС ВО.

Предлагаемые формы и средства текущего и промежуточного контроля адекватны целям и задачам реализации основной профессиональной образовательной программы по направлению подготовки: 40.04.01 Юриспруденция.

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)