Комплект оценочных материалов по дисциплине
«Безопасность информационных технологий»

Задания закрытого типа

Задания закрытого типа на выбор правильного ответа

1. Выберите один правильный ответ
Что такое кибербезопасность?
А) Процесс создания резервных копий данных.
Б) Защита компьютерных систем и сетей от цифровых атак.
В) Метод шифрования данных для хранения в облаке.
Г) Технология автоматизации процессов в IT-инфраструктуре.
Правильный ответ: Б
Компетенции (индикаторы): ПК-3

2. Выберите один правильный ответ
Какой тип атаки использует поддельные электронные письма для кражи данных?
А) DDoS-атака.
Б) SQL-инъекция
В) Фишинг
Г) Брутфорс-атака.
Правильный ответ: В
Компетенции (индикаторы): ПК-3

3. Выберите один правильный ответ
Какой из перечисленных методов используется для защиты данных от несанкционированного доступа?
А) Шифрование
Б) Дефрагментация диска.
В) Обновление драйверов.
Г) Установка графических редакторов.
Правильный ответ: А
Компетенции (индикаторы): ПК-3

4. Выберите один правильный ответ
Что такое уязвимость нулевого дня (zero-day)?
А) Уязвимость, которая известна только злоумышленникам и еще не устранена разработчиками.
Б) Ошибка в программном обеспечении, которая возникает при первом запуске программы.
В) Уязвимость, которая проявляется только через 24 часа после атаки.

Г) Технология защиты данных, использующая нулевое шифрование.
Правильный ответ: А
Компетенции (индикаторы): ПК-3

Задания закрытого типа на установление соответствия

1. Сопоставьте названия программ и изображения.

Программа		Изображение	
1)	Antivir	А)	
2)	DrWeb	Б)	
3)	Nod 32	В)	
4)	Avast	Г)	

Правильный ответ:

1	2	3	4
Б	Г	А	В

Компетенции (индикаторы):

2. Установите соответствие между типами шифрования и их характеристиками:

Тип шифрования		Характеристика	
1)	Симметричное	А)	Использует один ключ для шифрования и расшифрования.
2)	Асимметричное	Б)	Использует открытый и закрытый ключи для шифрования и расшифрования.
3)	Хэширование	В)	Преобразование данных в уникальный код, который невозможно расшифровать.

4)	Цифровая подпись	Г)	Использование закрытого ключа для подтверждения подлинности данных.

Правильный ответ:

1	2	3	4
А	Б	В	Г

Компетенции (индикаторы): ПК-3

3. Установите соответствие между компонентами информационной безопасности и их описаниями:

	Компонент		Описание
1)	Конфиденциальность	А)	Гарантия того, что данные не будут изменены несанкционированно.
2)	Целостность	Б)	Доступность данных и систем для авторизованных пользователей.
3)	Доступность	В)	Защита данных от несанкционированного доступа.
4)	Аутентификация	Г)	Процесс проверки подлинности пользователя или системы.

Правильный ответ:

1	2	3	4
В	А	Б	Г

Компетенции (индикаторы): ПК-3

4 Установите соответствие между методами защиты и их назначением:

	Метод защиты		Назначение
1)	Антивирусное ПО	А)	Защита данных от несанкционированного доступа.
2)	Шифрование данных	Б)	Фильтрация сетевого трафика для предотвращения атак
3)	Резервное копирование	В)	Обнаружение и блокировка вредоносного программного обеспечения.
4)	Межсетевой экран	Г)	Восстановление данных после потери или повреждения.

Правильный ответ:

1	2	3	4
В	А	Г	Б

Компетенции (индикаторы): ПК-3

Задания закрытого типа на установление правильной последовательности

1. Установите правильную последовательность этапов создания политики информационной безопасности::

А) Разработка правил и процедур

Б) Обучение сотрудников

В) Анализ рисков

Г) Внедрение и мониторинг

Правильный ответ: В, А, Б, Г

Компетенции (индикаторы): ПК-3

2. Установите правильную последовательность действий при реагировании на инцидент информационной безопасности:

А) Восстановление работоспособности

Б) Изоляция затронутых систем

В) Анализ и оценка угрозы.

Г) Обнаружение инцидента

Правильный ответ: Г, В, Б, А

Компетенции (индикаторы): ПК-3

3. Установите правильную последовательность этапов шифрования данных:

А) Применение шифрования к данным.

Б) Хранение и управление ключами

В) Генерация ключей.

Г) Выбор алгоритма шифрования

Правильный ответ: Г, В, А, Б

Компетенции (индикаторы): ПК-3

4. Установите правильную последовательность этапов внедрения системы управления информационной безопасностью (СУИБ) по стандарту ISO 27001:

А) Проведение внутреннего аудита.

Б) Разработка политики информационной безопасности.

В) Сертификация системы.

Г) Внедрение мер контроля и процедур.

Правильный ответ: Б, Г, А, В

Компетенции (индикаторы): ПК-3

Задания открытого типа

Задания открытого типа на дополнение

1. Напишите пропущенное слово (словосочетание).

Процесс преобразования данных в нечитаемый формат с целью защиты от несанкционированного доступа называется _____.

Правильный ответ: шифрование.

Компетенции (индикаторы): ПК-3

2. Стандарт, который регулирует управление информационной безопасностью в организации, называется _____.

Правильный ответ: ISO 27001.

Компетенции (индикаторы): ПК-3

3. Напишите пропущенное слово (словосочетание).

Метод атаки, при котором злоумышленник внедряет вредоносный SQL-код для манипуляции с базой данных, называется _____.

Правильный ответ: SQL-инъекция.

Компетенции (индикаторы): ПК-3

4. Напишите пропущенное слово (словосочетание).

Устройство или программа, предназначенная для фильтрации сетевого трафика и предотвращения несанкционированного доступа, называется _____.

Правильный ответ: брандмауэр.

Компетенции (индикаторы): ПК-3

5. Напишите пропущенное слово (словосочетание).

Процесс проверки подлинности пользователя с использованием двух независимых факторов (например, пароля и SMS-кода) называется _____.

Правильный ответ: двухфакторная аутентификация.

Компетенции (индикаторы): ПК-3

Задания открытого типа с кратким свободным ответом

1. Дайте ответ на вопрос.

1. Какие основные принципы лежат в основе защиты информации?

Правильный ответ: Конфиденциальность, . целостность, доступность

Компетенции (индикаторы): ПК-3

2. Дайте ответ на вопрос.

Какие основные цели информационной безопасности?

Правильный ответ: Конфиденциальность, целостность и доступность данных.

Компетенции (индикаторы): ПК-3

3. Дайте ответ на вопрос

Как называется мошенничество, целью которого является получение доступа к конфиденциальным данным пользователей?

Правильный ответ: Фишинг/ Метод социальной инженерии/ Кибермошенничество

Компетенции (индикаторы): ПК-3

4. Дайте ответ на вопрос

Какие меры защиты можно использовать против вредоносного программного обеспечения?

Правильный ответ: Установка антивирусного программного обеспечения, регулярное обновление систем, использование брандмауэров, обучение сотрудников.

Компетенции (индикаторы): ПК-3

5. Дайте ответ на вопрос

Какие технологии используются для шифрования данных?

Правильный ответ: AES/RSA/DES/методы кодирования/ алгоритмы криптографии.

Компетенции (индикаторы): ПК-3

Задания открытого типа с развернутым ответом

1. Зашифровать текст, используя алгоритм на основе задачи об укладке ранца:

Привести расширенное решение.

Время выполнения – 60 мин.

Ожидаемый результат:

Содержательная постановка задачи.

Дано множество предметов различного веса.

Полный вес равен 270, а последовательность весов предметов равна {2, 3, 6, 13, 27, 52, 105, 210}. Самый большой вес – 210. Он меньше 270, поэтому предмет весом 210 кладут в ранец. Вычитают 210 из 270 и получают 60. Следующий наибольший вес последовательности равен 105. Он больше 60, поэтому предмет весом 105 в ранец не кладут. Следующий самый тяжелый предмет имеет вес 52. Он меньше 60, поэтому предмет весом 52 также кладут в ранец. Аналогично проходят процедуру укладки в ранец предметы весом 6 и 2. В результате полный вес уменьшится до 0. Если бы этот ранец был бы использован для дешифрования, то открытый текст, полученный из значения шифртекста 270, был бы равен 10100101_2.

Пример дешифрования на основе задачи об укладке ранца

Шифрограмма (нераспределенный вес ранца, S)	Закрытый ключ (вес предмета, M_i)	Открытый текст (бинарный множитель, b_i)

270	210	1
60	105	0
60	52	1
8	27	0
8	13	0
8	6	1
2	3	0
2	2	1

Открытый ключ представляет собой не сверхвозрастающую (нормальную) последовательность. Он формируется на основе закрытого ключа и, как принято считать, не позволяет легко решить задачу об укладке ранца. Для его получения все значения закрытого ключа умножаются на число m по модулю n. Значение модуля n должно быть больше суммы всех чисел последовательности (например, n = 420 [2+3+6+13+27+52+105+210 = 418]). Множитель m должен быть взаимно простым числом с модулем n (например, m = 31). Результат построения нормальной последовательности (открытого ключа) представлен в следующей таблице.

Пример получения открытого ключа

Закрытый ключ, d_i	2	3	6	13	27	52	105	210
Открытый ключ, $e_i = (d_i*m) \bmod n = (d_i*31) \bmod 420$	62	93	186	403	417	352	315	210

Для зашифрования открытый текст сначала преобразуется в бинарный вид и разбивается на блоки, по размерам равные числу элементов последовательности (ключа). Затем, считая, что единица указывает на присутствие элемента последовательности в ранце, а ноль – на его отсутствие, вычисляются полные веса ранцев – по одному ранцу для каждого блока открытого текста.

В качестве примера возьмем открытый текст «АБРАМОВ», символы которого представим в бинарном виде в соответствии с кодировкой Windows 1251. Результат зашифрования с помощью открытого ключа e = {62, 93, 186, 403, 417, 352, 315, 210} представлен в следующей таблице.

Пример зашифрования

Открытый текст		Сумма весов	Шифрограмма (вес ранца), C
Символ	Bin-код		
А	1100 0000	62+93	155
Б	1100 0001	62+93+210	365
Р	1101 0000	62+93+403	558
А	1100 0000	62+93	155

М	1100 1100	62+93+417+352	924
О	1100 1110	62+93+417+352+315	1239
В	1100 0010	62+93+315	470

Правильный ответ: 155, 365, 558,155,924, 1239, 470

Компетенции (индикаторы): ПК-3

2. Зашифровать текст, используя алгоритм RSA:

Привести расширенное решение.

Время выполнения – 60 мин.

Ожидаемый результат:

Шифрование:

Выбираем простые числа:

p= 3, q=11

Вычисляем модуль $n = p \cdot q = 3 \cdot 11 = 33$

Вычисляем функцию Эйлера от модуля n : $\varphi(N) = (p-1)(q-1) = = 2 \cdot 10 = 20.$

4. Выбираем открытую экспоненту e=7

5. Определяем закрытую экспоненту d: $d * e = 1\big(mod\varphi(N)\big) \Longrightarrow d = 3$

Будем шифровать сообщение RSA, пусть букве А соответствует цифра 1, В – 2, С - 3 и т.д., тогда:

R=18; S=19; A=1;

Открытый ключ: $(e, n) = (7{,}33)$

$$C_1 = (18^7) mod 33 = 6$$
$$C_2 = (19^7) mod 33 = 13$$
$$C_3 = (1^7) mod 33 = 1$$

Правильный ответ: 6,13,1

Компетенции (индикаторы): ПК-3

Экспертное заключение

Представленный комплект оценочных материалов по дисциплине «Безопасность информационных технологий» соответствует требованиям ФГОС ВО.

Предлагаемые оценочные материалы адекватны целям и задачам реализации основной профессиональной образовательной программы по направлению подготовки 09.04.03 Прикладная информатика.

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

Разработанные и представленные для экспертизы оценочные материалы рекомендуются 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)
1.	Дополнен комплектом оценочных материалов	протокол заседания кафедры компьютерных систем и сетей № 8 от 10.03.2025	С.В. Попов