Комплект оценочных материалов по дисциплине
«Защита информации»

Задания закрытого типа

Задания закрытого типа на выбор правильного ответа

1. Выберите один правильный ответ
Какие основные угрозы могут быть связаны с технической защитой информации?
А) Вирусы и вредоносные программы
Б) Физическое повреждение оборудования
В) Несанкционированный доступ к данным
Г) Все перечисленное выше
Правильный ответ: Г
Компетенции: УК-1, ПК-2

2. Выберите один правильный ответ
Что такое уровень целостности данных?
А) Способность данных быть доступными только для авторизованных пользователей
Б) Способность данных оставаться неизменными и быть защищенными от несанкционированного изменения
В) Способность данных быть достоверными и точными
Г) Способность данных быть сохраненными и доступными в случае сбоя системы
Правильный ответ: Б
Компетенции: УК-1, ПК-2

3. Выберите один правильный ответ
Что такое антивирусное программное обеспечение?
А) Программное обеспечение для защиты систем от вирусов
Б) Программное обеспечение для шифрования данных
В) Программное обеспечение для контроля доступа
Г) Программное обеспечение для аутентификации пользователей
Правильный ответ: А
Компетенции: УК-1, ПК-2

4. Выберите один правильный ответ
Кто является регулятором в области обеспечения технической защиты информации в
Российской Федерации?
А) Федеральная служба по техническому и экспортному контролю

Б) Федеральная служба безопасности
В) Министерство обороны
Г) Министерство связи и массовых коммуникаций
Правильный ответ: Г
Компетенции: УК-1, ПК-2

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: УК-1, ПК-2

2. Установите правильное соответствие. Каждому элементу левого столбца соответствует только один элемент правого столбца.

Термин		Определение
1) Троян	А)	компьютерный вирус, который для своего размножения использует файловую систему, внедряясь в исполняемые файлы практически любой ОС
2) Файловый вирус	Б)	вредоносная программа, которая маскируется под легальное ПО

3)	Макровирус	В)	компьютерный вирус, добавляющий свой код в макросы для создания документов, электронных таблиц и других файлов данных
4)	Загрузочный вирус	Г)	вирус, который поражает загрузочный сектор жёсткого диска или главную загрузочную запись жёсткого диска

Правильный ответ:

1	2	3	4
Б	А	В	Г

Компетенции: УК-1, ПК-2

3. Установите правильное соответствие. Каждому элементу левого столбца соответствует только один элемент правого столбца.

	Термин		Определение
1)	Физическая защита	А)	метод защиты информации, основанный на преобразовании данных в код различного вида, чтобы информацию нельзя было прочитать, прослушать без расшифровки.
2)	Криптографическая защита	Б)	это меры безопасности, применяемые для защиты вычислительных устройств, а также компьютерных сетей
3)	Компьютерная защита	В)	это комплекс мер, направленных на защиту прав, свобод и законных интересов физических и юридических лиц в различных правовых ситуациях
4)	Юридическая защита	Г)	комплекс мер и средств, направленных на обеспечение безопасности физического состояния объектов, лиц, защиты информации от несанкционированного доступа, вредоносных действий и других угроз

Правильный ответ:

1	2	3	4
Г	А	Б	В

Компетенции: УК-1, ПК-2

4. Установите правильное соответствие. Каждому элементу левого столбца соответствует только один элемент правого столбца.

Термин		Определение
1) Конфиденциальность	А)	состояние, при котором информация либо остаётся неизменной, либо изменения осуществляются только теми, кто имеет на это право
2) Защищенность	Б)	способность системы предоставлять данные и услуги в любое время, независимо от внешних факторов
3) Целостность	В)	способность противостоять угрозам, защита физического и душевного здоровья
4) Доступность	Г)	необходимость предотвращения разглашения, утечки какой-либо информации

Правильный ответ:

1	2	3	4
Г	В	А	Б

Компетенции: УК-1, ПК-2

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: УК-1, ПК-2

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: УК-1, ПК-2

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: УК-1, ПК-2

4. Установите правильную последовательность шагов для обеспечения резервного копирования данных:

А) Выбор метода резервного копирования

Б) Настройка расписания копирования

В) Проверка целостности резервных копий.

Г) Определение критически важных данных.

Правильный ответ: Г, А, Б, В

Компетенции: УК-1, ПК-2

Задания открытого типа

Задания открытого типа на дополнение

1. Напишите пропущенное слово (словосочетание).

Процесс представления информации в виде, удобном для ее хранения и передачи - это _____

Правильный ответ: кодирование.

Компетенции: УК-1, ПК-2

2. Как называется наука о создании безопасных методов связи, о создании стойких (устойчивых к взлому) шифров (тайнописи).

Правильный ответ: криптография.

Компетенции: УК-1, ПК-2

3. Напишите пропущенное слово (словосочетание).

Знаковая система представления и передачи информации - это . _____.

Правильный ответ: язык.

Компетенции: УК-1, ПК-2

4. Полный набор символов, используемый для кодирования, называют:

Правильный ответ: алфавит.

Компетенции: УК-1, ПК-2

5. Напишите пропущенное слово (словосочетание).

Массированная отправка пакетов данных на узлы сети предприятия, с целью их перегрузки и выведения из строя это _____.

Правильный ответ: DOS атака.

Компетенции: УК-1, ПК-2

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: УК-1, ПК-2

2. Дайте ответ на вопрос.

Какие методы используются для предотвращения несанкционированного доступа к данным?

Правильный ответ: Правовые, организационные, технические, аппаратные, программные.

Компетенции: УК-1, ПК-2

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: УК-1, ПК-2

4. Дайте ответ на вопрос

Какие меры помогают защитить данные от фишинговых атак?

Правильный ответ: обучение сотрудников/ использование антифишинговых фильтров/ проверка подлинности сайтов/ использование фильтров

Компетенции: УК-1, ПК-2

5. Дайте ответ на вопрос

Какие технологии используются для шифрования данных?

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

Компетенции: УК-1, ПК-2

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: УК-1, ПК-2 ….

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: УК-1, ПК-2

Экспертное заключение

Представленный комплект оценочных материалов по дисциплине «Защита информации» соответствует требованиям ФГОС ВО.

Предлагаемые формы и средства текущего и промежуточного контроля адекватны целям и задачам реализации основной профессиональной образовательной программы по направлению подготовки: 01.03.02 Прикладная математика и информатика.

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)
1.	Дополнен комплектом оценочных материалов	протокол заседания кафедры компьютерных систем и сетей № 8 от 10.03.2025	С.В. Попов