Комплект оценочных материалов по дисциплине
«Технологии защиты информации»

Задания закрытого типа

Задания закрытого типа на выбор правильного ответа

1. *Выберите один правильный ответ.*

Какой из перечисленных методов защиты информации относится к физическим мерам?

А) шифрование данных;

Б) установка антивирусного программного обеспечения;

В) ограничение доступа в серверную комнату;

Г) использование межсетевого экрана.

Правильный ответ: В

Компетенции (индикаторы): ОПК-2

2. *Выберите один правильный ответ.*

Конфиденциальность информации – это …

А) доступность информации для всех пользователей;

Б) защита информации от несанкционированного доступа;

В) целостность информации;

Г) достоверность информации.

Правильный ответ: Б

Компетенции (индикаторы): ОПК-2

3. *Выберите один правильный ответ.*

Метод защиты информации, который обеспечивает ее целостность:

А) резервное копирование;

Б) антивирусная защита;

В) шифрование;

Г) межсетевой экран.

Правильный ответ: А

Компетенции (индикаторы): ОПК-2

4. *Выберите один правильный ответ.*

Вредоносное программное обеспечение – это …

А) программное обеспечение для шифрования данных;

Б) программное обеспечение, предназначенное для нанесения вреда компьютерным системам;

В) программное обеспечение для резервного копирования данных;

Г) программное обеспечение для фильтрации сетевого трафика.

Правильный ответ: Б

Компетенции (индикаторы): ОПК-2

5. *Выберите все правильные варианты ответов.*

Какие из перечисленных методов используются для аутентификации пользователей?

А) пароль;

Б) биометрические данные;

В) цифровая подпись;

Г) межсетевой экран;

Д) хеширование.

Правильный ответ: А, Б, В

Компетенции (индикаторы): ОПК-2

6. *Выберите все правильные варианты ответов.*

Выберите из нижеперечисленных угроз те, которые относятся к вредоносному программному обеспечению:

А) фишинг;

Б) вирусы;

В) троянские программы;

Г) DDoS-атаки;

Д) шпионское программное обеспечение.

Правильный ответ: Б, В, Д.

Компетенции (индикаторы): ОПК-2

Задания закрытого типа на установление соответствия

1. *Установите соответствие между методами защиты информации и их основными функциями*:

1) Шифрование	А) Обеспечение доступности информации
2) Резервное копирование	Б) Защита от вредоносного программного обеспечения
3) Антивирус	В) Обеспечение конфиденциальности
4) Контроль доступа	Г) Ограничение доступа к ресурсам

Правильный ответ

1	2	3	4
В	А	Б	Г

Компетенции (индикаторы): ОПК-2

2. *Установите соответствие между типами атак и их характеристиками:*

1) Фишинг	А) Самовоспроизводящееся вредоносное ПО
2) DDoS-атака	Б) Кража конфиденциальной информации через обман
3) Троянская программа	В) Нарушение доступности сервиса
4) Вирус	Г) Вредоносное программное обеспечение, замаскированное под легитимное

Правильный ответ

1	2	3	4
Б	В	Г	А

Компетенции (индикаторы): ОПК-2

3. *Установите соответствие между компонентами информационной безопасности и их характеристиками:*

1) Конфиденциальность	А) Обеспечение достоверности информации
2) Целостность	Б) Защита от несанкционированного доступа
3) Доступность	В) Обеспечение непрерывной работы сервисов
4) Аутентичность	Г) Подтверждение источника и неизменности информации

Правильный ответ

1	2	3	4
Б	А	В	Г

Компетенции (индикаторы): ОПК-2

4. *Установите соответствие между угрозами информационной безопасности и соответствующими методами защиты:*

1) Фишинг	А) Межсетевой экран
2) DDoS-атака	Б) Антивирусное ПО
3) Вирусная атака	В) Обучение пользователей
4) Несанкционированный доступ	Г) Системы обнаружения вторжений

Правильный ответ

1	2	3	4
В	Г	Б	А

Компетенции (индикаторы): ОПК-2

Задания закрытого типа на установление правильной последовательности

1. *Установите правильную последовательность этапы процесса шифрования данных. Запишите правильную последовательность букв слева направо.*

А) дешифрование данных;

Б) выбор алгоритма шифрования;

В) генерация ключа шифрования;

Г) шифрование данных.

Правильный ответ: Б, В, Г, А

Компетенции (индикаторы): ОПК-2

2. *Установите правильную последовательность этапов жизненного цикла управления доступом. Запишите правильную последовательность букв слева направо.*

А) аутентификация;

Б) отзыв прав доступа;

В) предоставление прав доступа;

Г) авторизация.

Правильный ответ: А, Г, В, Б

Компетенции (индикаторы): ОПК-2

3. *Установите правильную последовательность этапов жизненного цикла криптографического ключа. Запишите правильную последовательность букв слева направо.*

А) уничтожение ключа;

Б) генерация ключа;

В) распределение ключа;

Г) хранение и использование ключа.

Правильный ответ: Б, В, Г, А

Компетенции (индикаторы): ОПК-2

4. *Установите правильную последовательность этапов процесса шифрования сообщения. Запишите правильную последовательность букв слева направо.*

А) дешифрование;
Б) генерация ключа;
В) шифрование;
Г) передача зашифрованного сообщения;
Д) исходное сообщение.
Правильный ответ: Д, Б, В, Г, А
Компетенции (индикаторы): ОПК-2

Задания открытого типа

Задания открытого типа на дополнение

1. *Напишите пропущенное словосочетание.*
_____ – свойство системы обеспечивать своевременный беспрепятственный доступ правомочных (авторизованных) субъектов к интересующей их информации или осуществлять своевременный информационный обмен между ними.
Правильный ответ: доступность информации
Компетенции (индикаторы): ОПК-2

2. *Напишите пропущенное словосочетание.*
Под _____ понимается любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).
Правильный ответ: персональными данными
Компетенции (индикаторы): ОПК-2

3. *Напишите пропущенное слово.*
_____ – наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.
Правильный ответ: криптография
Компетенции (индикаторы): ОПК-2

Задания открытого типа с кратким свободным ответом

1. *Напишите пропущенное слово.*
Идентификация – процесс распознавания сущностей путем присвоения им уникальных _____.
Правильный ответ: меток/идентификаторов/логинов
Компетенции (индикаторы): ОПК-2

2. *Напишите пропущенное слово.*

Аутентификация – проверка _____ сущности предъявленному ею идентификатору.

Правильный ответ: соответствия/подлинности

Компетенции (индикаторы): ОПК-2

3. *Напишите пропущенное слово (словосочетание).*

Хеш-функция – легко вычислимая функция, преобразующая исходное сообщение произвольной длины (прообраз) в _____, для которой(ого) не существует эффективного алгоритма поиска коллизий.

Правильный ответ: сообщение фиксированной длины/хеш-образ

Компетенции (индикаторы): ОПК-2

4. *Напишите пропущенное словосочетание.*

_____ – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией, и которая используется для определения лица, подписывающего информацию.

Правильный ответ: электронная цифровая подпись/цифровая подпись

Компетенции (индикаторы): ОПК-2

Задания открытого типа с развернутым ответом

1. Практическое задание.

Тема: «Криптографические методы защиты информации»

Задание: объясните, как работают симметричные и асимметричные криптографические методы. В чем их различия и преимущества? Приведите примеры использования каждого метода.

Время выполнения – 20 мин.

Ожидаемый результат:

Симметричные методы используют один ключ для шифрования и расшифрования, асимметричные – два ключа (открытый и закрытый).

Различия: скорость, управление ключами, области применения.

Преимущества:

симметричные – простота реализации (всего один пароль), быстрая скорость зашифровки и дешифровки;

асимметричные – безопасный обмен ключами, упрощенная процедура хранения пароля (отсутствие необходимости передавать кому-то закрытый ключ).

Примеры:

симметричные – AES, ГОСТ 28147-89, 3DES;

асимметричные – RSA, DSA, Диффи-Хелмана.

Критерии оценивания:

Правильный ответ должен содержать: в качестве основных результатов – полнота и точность объяснения принципов работы симметричных и асимметричных методов; указание минимум двух различий между данными методами и их преимуществ из предложенных в ожидаемом результате; наличие минимум одного примера данных криптографических методов из предложенных в ожидаемом результате.

Компетенции (индикаторы): ОПК-2

2. Практическое задание.

Тема: «Шифр двойной перестановки»

Задание. Зашифровать текст «КРИПТОГРАФИЯ» методом двойной перестановки, используя таблицу 3x5, сначала переставляя строки по ключу «213», а затем столбцы по ключу «41523». Записать развернутый ответ в текстовом виде.

Время выполнения – 20 мин.

Ожидаемый результат:

1) Записываем текст в таблицу:

К Р И П Т

О Г Р А Ф

И Я _ _ _

2) Переставляем строки по ключу «213»:

О Г Р А Ф

К Р И П Т

И Я _ _ _

3) Переставляем столбцы по ключу «41523»:

А О Ф Г Р

П К Т Р И

_ И _ Я _

4) Выписываем текст по строкам. Зашифрованный текст: «АОФГРПКТРИ_И_Я_».

Компетенции (индикаторы): ОПК-2

2. Практическое задание.

Тема: «Криптоанализ зашифрованного сообщения»

Задание. Выполнить криптоанализ сообщения, зашифрованного по алгоритму «двойных перестановок». При этом нужно учитывать, что сначала были переставлены столбцы, затем строки. Исходное зашифрованное сообщение «АВАРНСЧАА_НЕДВЕДЕРПЕОЙ_ИС».

Записать развернутый ответ в текстовом виде.

Время выполнения – 45 мин.

Ожидаемый результат:

Длина зашифрованного сообщения – 24 символа.

Возможные размеры таблицы: 4x6, 6x4, 3x8, 8x3.

Предположим, что использовалась таблица 6x4.

Записываем зашифрованный текст в таблицу 6x4:

А В А Р
Н С Ч А
А _ Н Е
Д В Е Д
Е Р П Е
О Й _ И

Необходимо восстановить исходный порядок строк. Предположим, что после перестановки строк получилась следующая последовательность:

Д В Е Д
А _ Н Е
Е Р П Е
Н С Ч А
А В А Р
О Й _ И

Теперь необходимо восстановить исходный порядок столбцов. Предположим, что после перестановки столбцов получилась следующая последовательность:

Д Е В Д
А Н _ Е
Е П Р Е
Н Ч С А
А Р В А
О _ Й И

Читаем текст по строкам: «ДЕВДАН_ЕПЕРЕНЧСААРВАО_ЙИ».

Убираем символы подчеркивания и получаем «ДЕВДАНЕПЕРЕНЧСААРВАОЙИ».

Полученный текст «ДЕВДАНЕПЕРЕНЧСААРВАОЙИ» не имеет особого смысла, но содержит фрагменты, похожие на слова.

Так как размер таблицы и порядок строк и столбцов предполагался, то результат может не соответствовать действительности.

Попробуем другой порядок строк и столбцов.

Предположим, что порядок строк был таким:

Д В Е Д
Е Р П Е
А _ Н Е
О Й _ И
Н С Ч А
А В А Р

Предположим, что порядок столбцов был таким:

Д Е В Д
Е П Р Е
А Н _ Е

О _ Й И
Н Ч С А
А Р В А

Читаем текст по строкам: «ДЕВДЕПРАН_ЕО_ЙИНЧСААРВА».

Убираем символы подчеркивания и получаем «ДЕВДЕПРАНЕОЙИНЧСААРВА».

Как видно, этот результат уже лучше, и содержит фрагменты слов.

Если предположить, что в сообщении есть слово «ВРЕД», то можно попробовать другой порядок столбцов.

Предположим, что порядок столбцов был таким:

В Р Е Д
П Е Р Е
Н _ А Е
Й И _ О
С Ч А Н
Р А В А

Читаем текст по строкам: «ВРЕДПЕРЕН_АЕЙИ_ОСЧАНРАВА».

Убираем символы подчеркивания и получаем «ВРЕДПЕРЕНАЕЙИОСЧАНРАВА».

Этот результат уже лучше, и содержит слово «ВРЕД».

Если предположить, что в сообщении есть слово «ОПАСНОСТЬ», то можно попробовать другой порядок строк.

Предположим, что порядок строк был таким:

В Р Е Д
П Е Р Е
С Ч А Н
Р А В А
Н _ А Е
Й И _ О

Читаем текст по строкам: «ВРЕДПЕРЕСЧАНРАВАН_АЕЙИ_О».

Убираем символы подчеркивания и получаем «ВРЕДПЕРЕСЧАНРАВАНАЕЙИО».

Этот результат уже лучше, и содержит фрагменты слов «ВРЕД», «ПЕРЕ», «ОПАСНОСТЬ».

Если предположить, что в сообщении есть слово «ИНФОРМАЦИЯ», то можно попробовать другой порядок столбцов.

Предположим, что порядок столбцов был таким:

И Н Ф О
Р М А Ц
Б Е З О
П А С Н
Ь _ _ _

Читаем текст по строкам: «ИНФОРМАЦИЯБЕЗОПАСНОСТЬ».

Этот результат уже лучше, и содержит слова «ИНФОРМАЦИЯ» и «БЕЗОПАСНОСТЬ».

Ответ: исходное сообщение: «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ».

Критерии оценивания:

При помощи любых возможных способов анализа частоты букв, поиска возможных слов и фраз, а также интуиции и предположений получить исходное сообщение, представленное в ответе ожидаемого результата.

Компетенции (индикаторы): ОПК-2

Экспертное заключение

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

Предлагаемые оценочные материалы адекватны целям и задачам реализации основной профессиональной образовательной программы по направлению подготовки 09.03.02 Информационные системы и технологии.

Виды оценочных средств, включенные 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 Н.Н. Ветрова

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	В фонд оценочных средств добавлен комплект оценочных материалов	26.02.2025 г., №14	 А.И. Горбунов