Комплект оценочных материалов по дисциплине
«Безопасность информационных систем автоматизации»

Задания закрытого типа

Задания закрытого типа на выбор правильного ответа

Выберите один правильный ответ

1. Какой из перечисленных принципов является основополагающим при построении безопасности информационных систем автоматизации?

А) принцип абсолютной безопасности

Б) принцип экономической целесообразности

В) принцип полной секретности

Г) принцип универсальности защиты

Правильный ответ: Б

Компетенции (индикаторы) ОПК-2, ОПК-4, ПК-1

2. Какое средство защиты, при разработке безопасности информационных систем автоматизации, относится к техническим методам?

А) межсетевой экран

Б) система обнаружения вторжений

В) физическая охрана помещений

Г) система аутентификации

Правильный ответ: В

Компетенции (индикаторы) ОПК-2, ОПК-4, ПК-1

3. Что такое многофакторная аутентификация?

А) использование нескольких паролей

Б) применение разных методов идентификации

В) двойная проверка пароля

Г) использование биометрии

Правильный ответ: Б

Компетенции (индикаторы) ОПК-2, ОПК-4, ПК-1

4. Что такое принцип наименьших привилегий при разработке безопасности информационных систем автоматизации?

А) пользователь должен иметь только необходимые права

Б) все пользователи имеют одинаковые права

В) администратор имеет максимальные права

Г) система автоматически снижает права при угрозе

Правильный ответ: А

Компетенции (индикаторы) ОПК-2, ОПК-4, ПК-1

Задания закрытого типа на установление соответствия

Установите правильное соответствие.

Каждому элементу левого столбца соответствует только один элемент правого столбца.

1. Установите соответствие между методами защиты информации и их реализациями, при построении системы безопасности информационных систем автоматизации.

Реализация метода защиты	Метод защиты
1) охранные системы, замки, сигнализация	А) физический
2) специальные устройства, датчики, криптографические аппаратные модули	Б) программный
3) межсетевые экраны, антивирусное программное обеспечение, системы обнаружения вторжений	В) аппаратный
4) инструкции по эксплуатации, регламенты, политики безопасности	Г) организационный

Правильный ответ

1	2	3	4
А	В	Б	Г

Компетенции (индикаторы) ОПК-2, ОПК-4, ПК-1

2. Установите соответствие между типом атаки и её описанием:

Описание атаки	Название атаки
1) программа, размножающаяся путем заражения других программ	А) SQL-инъекция
2) внедрение вредоносного кода в базу данных	Б) фишинг
3) кража данных через поддельные сайты	В) DDoS
4) перегрузка серверов большим количеством запросов	Г) вирус

Правильный ответ

1	2	3	4
Г	А	Б	В

Компетенции (индикаторы) ОПК-2, ОПК-4, ПК-1

3. Установите соответствие между методом защиты программного обеспечения и его основным механизмом реализации:

Механизмы реализации	Методы защиты
1) преобразование и запутывание исходного кода программы для затруднения его анализа и реверсивной инженерии	А) обфускация
2) создание виртуальной машины для исполнения защищённого кода в изолированной среде	Б) криптографическая защита
3) применение физических защитных ключей и специализированных модулей безопасности	В) эмуляция
4) использование алгоритмов шифрования для защиты компонентов программы	Г) аппаратная защита

Правильный ответ

1	2	3	4
А	В	Г	Б

Компетенции (индикаторы) ОПК-2, ОПК-4, ПК-1

4. Установите соответствие между криптографическими терминами и их точными определениями

	Термин
1) математический процесс преобразования любого входного сообщения в битовую строку фиксированной длины, которая является уникальным отпечатком исходных данных	А) шифрование
2) документ, который связывает открытый ключ с конкретной личностью или организацией	Б) хеширование
3) метод преобразования информации с использованием криптографических алгоритмов для обеспечения конфиденциальности данных	В) электронная подпись
4) механизм для подтверждения подлинности и целостности электронного документа, использующий пару ключей для создания и проверки подписи	Г) цифровой сертификат

Правильный ответ

1	2	3	4
Б	Г	А	В

Компетенции (индикаторы) ОПК-2, ОПК-4, ПК-1

Задания закрытого типа на установление правильной последовательности

Установите правильную последовательность.
Запишите правильную последовательность букв слева направо.

1. Определите правильную последовательность этапов кодирования текстового файла с использованием алгоритма Хаффмана:
А) анализ частотности встречающихся символов
Б) назначение кодовых последовательностей символам
В) построение дерева Хаффмана
Г) формирование таблицы соответствия символов и кодов
Правильный ответ: А, В, Б, Г
Компетенции (индикаторы) ОПК-2, ОПК-4, ПК-1

2. Расположите уровни RAID по возрастанию комплексной производительности чтении и записи:
А) RAID 0
Б) RAID 1
В) RAID 5
Г) RAID 10
Правильный ответ: Б, В, А, Г
Компетенции (индикаторы) ОПК-2, ОПК-4, ПК-1

3. Установите правильную последовательность действий при обнаружении инцидента безопасности информационных систем автоматизации:

А) уведомление руководства

Б) изоляция затронутых систем

В) фиксация доказательств

Г) восстановление работоспособности

Правильный ответ: Б, В, А, Г

Компетенции (индикаторы) ОПК-2, ОПК-4, ПК-1

4. Определите правильную последовательность действий при работе с правами доступа в Linux:

А) установка базовых прав доступа

Б) применение дополнительных битов доступа

В) определение владельца файла

Г) настройка групп доступа

Правильный ответ: В, Г, А, Б

Компетенции (индикаторы) ОПК-2, ОПК-4, ПК-1

Задания открытого типа

Задания открытого типа на дополнение

Напишите пропущенное слово (словосочетание)

1. Процесс систематического выявления и анализа угроз безопасности информационным системам автоматизации называется _____ рисков.
Правильный ответ: оценка
Компетенции (индикаторы) ОПК-2, ОПК-4, ПК-1

2. Процесс преобразования исходного кода программы в менее понятный вид называется _____.
Правильный ответ: обфускация
Компетенции (индикаторы)

3. Процесс преобразования входных данные в уникальную строку фиксированной длины, называется _____ .
Правильный ответ: хэширование
Компетенции (индикаторы) ОПК-2, ОПК-4, ПК-1

4. Регулярное создание копий важных данных с целью их восстановления в случае потери называется _____ копирование.
Правильный ответ: резервное
Компетенции (индикаторы) ОПК-2, ОПК-4, ПК-1

Задания открытого типа с кратким свободным ответом

Напишите пропущенное слово (словосочетание)

1. Для подтверждения подлинности электронного документа используется _____.

Правильный ответ: электронная подпись, цифровая подпись, электронная цифровая подпись цифровой сертификат, криптографический хеш, хэш, цифровой отпечаток, электронная печать

Компетенции (индикаторы) ОПК-2, ОПК-4, ПК-1

2. При передаче конфиденциальных данных через интернет рекомендуется использовать _____ протокол.

Правильный ответ: HTTPS, SFTP, FTPS, SSH, SSL, TLS, TLS, IPSec, VPN

Компетенции (индикаторы) ОПК-2, ОПК-4, ПК-1

3. Для эффективного хранения текстовых данных можно использовать _____.

Правильный ответ: сжатие данных, кодирование Хаффмана, дерево Хаффмана, RLE-сжатие, LZW-алгоритм, архивацию

Компетенции (индикаторы) ОПК-2, ОПК-4, ПК-1

4. Для обеспечения надёжности хранения данных, с целью их защиты от потери при выходе из строя компонентов системы хранения, применяется _____.

Правильный ответ: RAID, RAID-массив, резервное копирование, резервирование, дублирование, зеркалирование, зеркальное отображение, кластерное хранение

Компетенции (индикаторы) ОПК-2, ОПК-4, ПК-1

Задания открытого типа с развернутым ответом

1. Применение алгоритмов ZIP при обеспечении безопасности информационных систем автоматизации. Приведите пример работы алгоритма семейства ZIP.

Время выполнения – 30 мин

Ожидаемый результат:

Алгоритмы ZIP – это не только удобный инструмент сжатия информации, но и важным элемент обеспечения безопасности информационных систем автоматизации. Исторически ZIP-архиваторы развились с алгоритмов шифрования, и со временем развились до более совершенных решений. Современные ZIP-архиваторы поддерживают такие мощные алгоритмы шифрования с длиной ключа 128 и 256-битным шифрованием.

При использовании ZIP-алгоритмов в системах автоматизации важно понимать их ограничения. Прежде всего, это уязвимость к методам перебора ключей, относительно невысокая скорость шифрования и возможность восстановления данных при определенных условиях. Именно поэтому ZIP-защита должна рассматриваться как один из элементов комплексной системы безопасности, а не как единственное решение.

С точки зрения программирования информационных систем, ZIP-алгоритмы следует применяются как часть комплексной системы защиты данных:

– шифрование данных при передаче между компонентами системы;

– защита резервных копий информации;

– сжатие конфиденциальных данных перед хранением;

– обеспечение целостности данных через встроенные механизмы проверки.

Пример работы алгоритма ZIP.

Представим данные для защиты в виде строки:

«AAABBBCCCCDDDEEE»

Первый этап – поиск повторяющихся последовательностей: «AAA» – три «A» подряд, «BBB» – три «B» подряд, «CCCC» - четыре «C» подряд, «DDD» – три «D» подряд, «EEE» – три «E» подряд.

Второй этап – кодирование. Заменяем каждую последовательность на символ + количество повторений: «A3B3C4D3E3». Получаем, что исходная длина – 15 символов, а кодированная длина – 9 символов. Таким образом, экономия составила 6 символов (40%).

Критерии оценивания:

– дано описание ZIP алгоритмов;

– в общем охарактеризованы преимущества и недостатки ZIP алгоритмов;

– приведен наглядный пример работы ZIP алгоритмов;

– ответ имеет четкую структуру.

Компетенции (индикаторы) ОПК-2, ОПК-4, ПК-1

2. Как работает метод шифрования перестановкой с использованием гиперкуба Гамильтона, и в чем заключаются его основные преимущества и недостатки по сравнению с другими методами криптографической защиты информации?

Время выполнения – 30 мин

Ожидаемый результат:

Метод шифрования перестановкой с использованием гиперкуба Гамильтона представляет собой усовершенствованный метод простой перестановки. Используются вершины гиперкуба для записи символов шифруемого текста. Считывание зашифрованного текста происходит по маршрутам Гамильтона.

Покажем пример реализации.

Пусть есть открытый текст: «ПРИМЕР»

Используем маршрут Гамильтона: 4-0-2-3-1-5-7-6

Разобьем текст на блоки по 8 символов (недостающие заполним пробелами):

«ПРИМЕР__»

Зашифруем по маршруту (4-0-2-3-1-5-7-6):

```
0 1 2 3 4 5 6 7
П Р И М Е Р _ _
4 0 2 3 1 5 7 6
Е П И М Р Р _ _
```

Обратный маршрут (1-4-2-3-0-5-6-7):

```
0 1 2 3 4 5 6 7
Е П И М Р Р _ _
1 4 2 3 0 5 6 7
П Р И М Е Р _ _
```

Преимущества метода перестановки с использованием гиперкуба Гамильтона заключаются в высокой стойкости шифрования благодаря усложненным перестановкам, возможность применения нескольких маршрутов для повышения сложности взлома, относительная простота реализации, возможность создания большого количества ключей.

Недостатком метода можно считать ограниченный размер ключа (8 символов), при использовании фиксированных маршрутов возможно их выявление, требует большего объема вычислений по сравнению с простой перестановкой, сложность обработки больших объемов данных.

По сравнению с простой перестановкой: более стойкий, но сложнее в реализации

По сравнению с современными алгоритмами: уступает в криптостойкости

Данный метод можно оценивать как промежуточный этап развития криптографических методов между простой перестановкой и более сложными алгоритмами шифрования. Он обеспечивает приемлемый уровень защиты при относительно простой реализации.

Критерии оценивания:

– дана краткая характеристика гиперкуба Гамильтона;

– приведены основные преимущества гиперкуба Гамильтона;

– приведены основные недостатки гиперкуба Гамильтона;

– ответ имеет четкую структуру.

Компетенции (индикаторы) ОПК-2, ОПК-4, ПК-1

3. Обратимое XOR-шифрование данных со случайной гаммой. Укажите основные преимущества и недостатки данного метода. Какие требования предъявляются к случайной гамме.

Время выполнения – 30 мин

Ожидаемый результат:

Обратимое XOR-шифрование со случайной гаммой представляет собой симметричный криптографический метод, где над исходными данными выполняется действие исключающего или с последовательностью случайных битов (гаммой) той же длины.

Алгоритм шифрования сводится к следующему: генерация случайной гаммы той же длины, что и исходные данные, преобразование данных в битовую последовательность, применение операции «исключающего или» между битами исходного сообщения и гаммы, сохранение гаммы и зашифрованных данных.

Алгоритм дешифрования возможен только с применением гаммы шифрования:

Преимущества метода: простота реализации, возможность аппаратной реализации, высокая скорость шифрования/дешифрования, идеальная криптографическая стойкость при правильном использовании, обратимость операции

Недостатки метода: необходимость хранения/передачи гаммы, уязвимость при повторном использовании гаммы, зависимость от качества генератора случайных чисел.

Требования к случайной гамме: должна быть действительно случайной, должна быть не короче исходных данных, должна использоваться только один раз, должна быть надежно защищена.

Данный метод является основой для многих современных потоковых шифров и часто используется в комбинации с другими криптографическими примитивами для обеспечения надежной защиты данных.

Критерии оценивания:

– дана краткая характеристика XOR-шифрованию;

– приведены основные преимущества XOR-шифрования;

– приведены основные недостатки XOR-шифрования;

– приведены основные требования к гамме;

– ответ имеет четкую структуру.

Компетенции (индикаторы) ОПК-2, ОПК-4, ПК-1

4. Как работает алгоритм Хаффмана для сжатия данных, и какие факторы влияют на эффективность этого метода? Опишите пошаговый процесс построения оптимального кодового дерева, объясните принципы префиксного кодирования.

Время выполнения – 30 мин

Ожидаемый результат:

Метод Хаффмана представляет собой эффективный алгоритм сжатия данных, основанный на построении оптимального префиксного кода.

Процесс построения оптимального: сбор статистики частот встречаемости символов, построение бинарного дерева кодирования, формирование кодов переменной длины, преобразование исходного сообщения в сжатый вид.

Пошаговый процесс построения дерева Хаффмана:

– создание списка узлов, где каждый узел представляет символ и его частоту;

– выбор двух узлов с наименьшими частотами;

– создание нового узла-родителя с суммой частот;

– повторение шагов б) и в) до получения корневого узла;

– формирование кодов путем обхода дерева.

Особенности префиксного кодирования:

– ни один код не может быть префиксом другого;

– часто встречающиеся символы получают короткие коды;

– редкие символы получают длинные коды;

– гарантирует однозначное декодирование.

Преимущества алгоритма Хаффмана: высокая эффективность сжатия, простота реализации, гарантированная оптимальность.

Основные недостатки алгоритма Хаффмана: необходимость передачи таблицы кодов, сложность обновления при адаптивном кодировании, ограниченная эффективность при равномерном распределении символов, сложность алгоритма обработки бит данных переменной длины.

Метод Хаффмана остается одним из фундаментальных алгоритмов сжатия данных благодаря своей эффективности и универсальности. Он часто используется как отдельный метод или в составе более сложных алгоритмов сжатия, обеспечивая оптимальное кодирование при правильном применении.

Критерии оценивания:

– дана краткая характеристика алгоритма Хаффмана;

– приведены основные преимущества алгоритма Хаффмана;

– приведены основные недостатки алгоритма Хаффмана;

– ответ имеет четкую структуру.

Компетенции (индикаторы) ОПК-2, ОПК-4, ПК-1

Экспертное заключение

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

Предлагаемые оценочные материалы адекватны целям и задачам реализации основной профессиональной образовательной программы по направлению подготовки 15.04.04 Автоматизация технологических процессов и производств.

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 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	В фонд оценочных средств добавлен комплект оценочных материалов	25.02.2025 г., №14	А.В. Колесников