МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению лабораторных работ
по дисциплине
«Методы и средства криптографической защиты информации»
для студентов
Специальности 10.05.03 Информационная безопасность
автоматизированных систем
Специализация «Анализ безопасности информационных систем»

Ставрополь
2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Цель и задачи освоения дисциплины

Целью освоения дисциплины «Методы и средства криптографической защиты информации» является формирование у будущего специалиста по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация «Анализ безопасности информационных систем» понимания основных методов, средств и технологий эффективного взаимодействия и реализации успешной командной работы.
Задачи дисциплины:

– изучение теоретических основ формирования и развития навыков командной работы;
– формирование умений управления групповыми проектами;
– овладение навыками эффективного социального взаимодействия, создания благоприятной и конструктивной атмосферы в команде средствами доступных информационных технологий.

Лабораторная работа №1 Методы криптографического преобразования информации

Наукой, изучающей математические методы защиты информации путем ее преобразования, является **криптология** [kruptoz – тайный, logoz – наука (слово) (греч.)]. Криптология разделяется на два направления – криптографию и криптоанализ.

Под **криптографической защитой информации** понимается такое преобразование исходной информации, в результате которого она становится недоступной для ознакомления и использования лицами, не имеющими на это полномочий.

Известны различные подходы к классификации методов криптографического преобразования информации. По виду воздействия на исходную информацию **методы криптографического преобразования информации** могут быть разделены на четыре группы (рисунок 1).

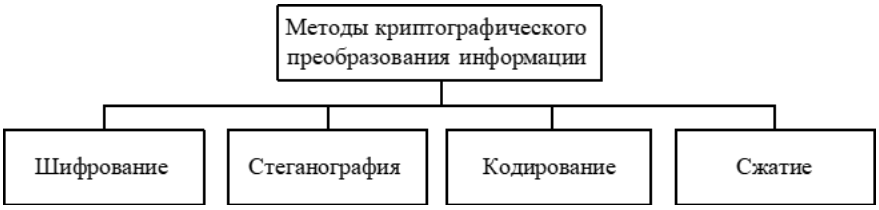

Рисунок 1 – Классификация методов криптографического преобразования информации

Содержание отчета:

- Введение
- Методы классификации криптографического преобразования
- Примеры методов каждой группы
- Сравнительные методы анализа
- Заключение

Контрольные вопросы:

- Чем отличаются криптография и криптоанализ как направления криптологии?
- В чем заключается суть криптографической защиты информации?

- В каких группах можно использовать методы криптографического преобразования информации для предотвращения воздействия на исходные данные?

Лабораторная работа №2 Шифрование информации

Основным видом криптографического преобразования информации в компьютерных системах является шифрование. Под **шифрованием** понимается процесс преобразования открытой информации в зашифрованную (шифротекст) или процесс обратного преобразования зашифрованной информации в открытую. Процесс преобразования открытой информации в закрытую получил название шифрование, а процесс преобразования закрытой информации в открытую – расшифрование (рисунок 2).

Процесс шифрования заключается в проведении обратимых математических, логических, комбинаторных и других преобразований исходной ин- формации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов.

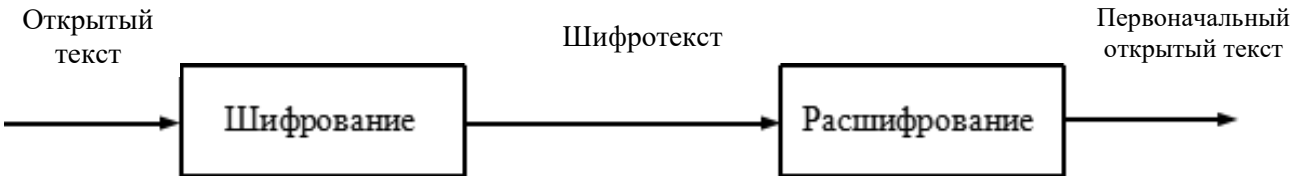

Рисунок 2 – Шифрование и расшифрование

Для шифрования информации используются алгоритм преобразования и ключ. Как правило, алгоритм для определенного метода шифрования является неизменным. Исходными данными для алгоритма шифрования служат информация, подлежащая шифрованию, и ключ шифрования. Ключ – конкретное значение некоторых параметров алгоритма криптографического преобразования, обеспечивающее выбор преобразования из семейства. Он содержит управляющую информацию, которая определяет выбор преобразования на определенных шагах алгоритма и величины операндов, используемые при реализации алгоритма шифрования.

За многовековую историю использования шифрования информации человечеством изобретено множество методов шифрования, или шифров. Методом шифрования (шифром) называется совокупность обратимых преобразований открытой информации в закрытую в соответствии с алгоритмом шифрования. Большинство методов шифрования не выдержали проверку временем, а некоторые используются и до сих пор. Появление ЭВМ инициировало процесс разработки новых шифров, учитывающих их возможности использования как для шифрования/дешифрования информации, так и для атак на шифр. Атака на шифр (криптоанализ) – это процесс дешифрования закрытой информации без знания ключа и, возможно, при отсутствии сведений об алгоритме шифрования. Процесс восстановления первоначального открытого текста на основе шифрованного без знания ключа называют дешифрованием.

Современные *методы шифрования должны отвечать следующим требованиям*:

- стойкость шифра противостоять криптоанализу (криптостойкость) должна быть такой, чтобы вскрытие его могло быть осуществлено только путем решения задачи полного перебора ключей;
- криптостойкость обеспечивается не секретностью алгоритма шифрования, а секретностью ключа;
- шифротекст не должен существенно превосходить по объему исходную информацию;
- ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации;
- время шифрования не должно быть большим;
- стоимость шифрования должна быть согласована со стоимостью закрываемой информации.

Криптостойкость шифра является его основным показателем эффективности. Она измеряется временем или стоимостью средств, необходимых криптоаналитику для получения исходной информации по

шифротексту, при условии, что ему неизвестен ключ.

Сохранить в секрете широко используемый алгоритм шифрования практически невозможно. Поэтому алгоритм не должен иметь скрытых слабых мест, которыми могли бы воспользоваться криптоаналитики. Если это условие выполняется, то криптостойкость шифра определяется длиной ключа, так как единственный путь вскрытия зашифрованной информации – перебор комбинаций ключа и выполнение алгоритма дешифрования. Таким образом, время и средства, затрачиваемые на криптоанализ, зависят от длины ключа и сложности алгоритма шифрования.

В качестве примера удачного метода шифрования можно привести шифр DES (Data Encryption Standard), применяемый в США с 1978 года в качестве государственного стандарта. Алгоритм шифрования не является секретным и был опубликован в открытой печати. За все время использования этого шифра не было обнародовано ни одного случая обнаружения слабых мест в алгоритме шифрования.

В конце 70-х годов использование ключа длиной в 56 бит гарантировало, что для раскрытия шифра потребуется несколько лет непрерывной работы самых мощных по тем временам компьютеров. Прогресс в области вычислительной техники позволил значительно сократить время определения ключа путем полного перебора. Согласно заявлению специалистов Агентства национальной безопасности США, 56-битный ключ для DES может быть найден менее чем за 453 дня с использованием супер ЭВМ Cray T3D, которая имеет 1024 узла и стоит 30 млн дол. Используя чип FPGA (Field Progammably Gate Array – программируемая вентильная матрица) стоимостью 400 дол., можно восстановить 40-битный ключ DES за 5 часов. Потратив 10000 дол. за 25 чипов FPGA, 40-битный ключ можно найти в среднем за 12 мин. Для вскрытия 56-битного ключа DES при опоре на серийную технологию и затратах в 300000 дол. требуется в среднем 19 дней, а если разработать специальный чип, – то 3 часа. При затратах в 300 млн дол. 56-битные ключи могут быть найдены за 12 с. Расчеты показывают, что в настоящее время для надежного закрытия

информации длина ключа должна быть не менее 90 бит.

Современная криптография включает в себя четыре основные группы криптографических методов защиты информации:

- симметричные криптосистемы;
- асимметричные криптосистемы (криптосистемы с открытым ключом);
- системы электронной цифровой подписи;
- управление ключами.

В *асимметричных криптосистемах* используются два ключа – открытый и секретный, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключ, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Электронной цифровой подписью называется присоединение к тексту его криптографического преобразования, которое позволяет при получении текста другим пользователем проверить авторство и целостность сообще- ния.

Управление ключами – это процесс системы обработки информации, вырабатывающий и распределяющий ключи (открытые и секретные) между пользователями.

Далее данные группы методов будут рассмотрены подробнее.

Содержание отчета:

- Введение
- Принцип работы шифрования
- Понятие криптостойкости
- Современные методы криптографической защиты
- Заключение

Контрольные вопросы:

- В чём заключаются различия между шифрованием и расшифрованием?
- От чего зависит криптостойкость шифра, и почему длина ключа играет решающую роль?

- Какие группы методов криптографической защиты информации достигаются в современной криптографии?

Лабораторная работа №3 Стеганография

В отличие от других методов криптографического преобразования информации, методы **стеганографии** позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации. В компьютерных системах практическое использование стеганографии только начинается, но проведенные исследования показывают ее перспективность. В основе всех методов стеганографии лежит маскирование закрытой информации среди открытых файлов. Обработка мультимедийных файлов в компьютерных системах открыла практически неограниченные возможности перед стеганографией.

Существует несколько методов скрытой передачи информации. Одним из них является простой метод скрытия файлов при работе в операционной системе MS DOS. За текстовым открытым файлом записывается скрытый двоичный файл, объем которого много меньше текстового файла. В конце текстового файла помещается метка EOF (комбинация клавиш Ctrl и Z). При обращении к этому текстовому файлу стандартными средствами ОС считывание прекращается по достижению метки EOF, и скрытый файл остается недоступен. Для двоичных файлов никаких меток в конце файла не предусмотрено. Конец такого файла определяется при обработке атрибутов, в которых хранится длина файла в байтах. Доступ к скрытому файлу может быть получен, если файл открыть как двоичный. Скрытый файл может быть зашифрован. Если кто-то случайно обнаружит скрытый файл, то зашифрованная информация будет воспринята как сбой в работе системы.

Графическая и звуковая информации представляются в числовом виде. Так, в графических объектах наименьший элемент изображения может

кодироваться одним байтом. В младшие разряды определенных байтов изображения в соответствии с алгоритмом криптографического преобразования помещаются биты скрытого файла. Если правильно подобрать алгоритм преобразования и изображение, на фоне которого помещается скрытый файл, то человеческому глазу практически невозможно отличить полученное изображение от исходного. Очень сложно выявить скрытую информацию и с помощью специальных программ. Наилучшим образом для внедрения скрытой информации подходят изображения местности: фотоснимки со спутников, самолетов и т.п. С помощью средств стеганографии могут маскироваться текст, изображение, речь, цифровая подпись, зашифрованное сообщение. Комплексное использование стеганографии и шифрования многократно повышает сложность решения задачи обнаружения и раскрытия конфиденциальной информации.

Содержание отчета:

- Общее представление о стеганографии
- Методы раскрытия информации в компьютерных технологиях
- Использование полученных файлов для раскрытия данных
- Преимущества и сложность поиска скрытых данных
- Заключение и перспективы применения стеганографии

Контрольные вопросы:

- В чем принципиальные отличия стеганографии от криптографии?
- Как раскрыта информация о вреде графических или звуковых файлов?
- Почему сочетание стеганографии и шифрования считается особенно надёжным способом защиты информации?

Лабораторная работа №4 Кодирование информации

Содержанием процесса **кодирования информации** является замена

смысловых конструкций исходной информации (слов, предложений) кодами. В качестве кодов могут использоваться сочетания букв, цифр, букв и цифр. При кодировании и обратном преобразовании используются специальные таблицы или словари. Кодирование информации целесообразно применять в системах с ограниченным набором смысловых конструкций. Такой вид криптографического преобразования применим, например, в командных линиях автоматизированных систем управления. Недостатками кодирования конфиденциальной информации является необходимость хранения и распространения кодировочных таблиц, которые необходимо часто менять, чтобы избежать раскрытия кодов статистическими методами обработки перехваченных сообщений.

Содержание отчета:

- Понятие кодирования информации и его особенности
- Типы кодов и способы замены смысловых конструкций
- Применение кодирования в автоматизированных компьютерных управлениях
- Недостатки, методы и риски при использовании кодировочных таблиц
- Выводы о применимости шифрования как криптографических методов

Контрольные вопросы:

- Чем отличается кодирование информации от шифрования?
- В чем преимущества и недостатки использования кодировочных таблиц?
- Почему кодирование рекомендуется использовать в домашних условиях с ограниченным набором команд?

Лабораторная работа №5 Сжатие информации

Сжатие информации может быть отнесено к методам криптографического преобразования информации с определенными оговорками. Целью сжатия является сокращение объема информации. В то же время сжатая информация не может быть прочитана или использована без обратного преобразования. Учитывая доступность средств сжатия и обратного преобразования, эти методы нельзя рассматривать как надежные средства криптографического преобразования информации. Даже если держать в секрете алгоритмы, то они могут быть сравнительно легко раскрыты статистическими методами обработки. Поэтому сжатые файлы конфиденциальной информации подвергаются последующему шифрованию. Для сокращения времени целесообразно совмещать процесс сжатия и шифрования информации.

В некоторых источниках стеганография, кодирование и сжатие информации относятся к отраслям знаний, смежных с криптографией, но не входящих в нее.

Содержание отчета:

- Предложение сокращения информации и его целей
- Особенности и способы алгоритмов сжатия
- Ограничения сокращения как средства защиты данных
- Комбинирование сжатия и шифрования в приложении ИБ
- Выводы: сжатие играет роль вспомогательного метода в криптографии.

Контрольные вопросы:

- Почему расширение информации не считается полноценным методом криптографической защиты?
- В каких случаях сжатие информации может повысить безопасность данных?
- Зачем объединяют процессы сжатия и шифрования?

Лабораторная работа №6 Традиционные методы шифрования

К традиционным (классическим) методам шифрования относятся шифры перестановки, шифры простой и сложной замены, а также некоторые их модификации и комбинации. Комбинации шифров перестановок и шифров замены образуют все многообразие применяемых на практике симметричных шифров.

Шифры перестановки. При шифровании перестановкой символы шифруемого текста переставляются по определенному правилу в пределах блока этого текста. Шифры перестановки являются самыми простыми и, вероятно, самыми древними шифрами.

Шифрующие таблицы. В качестве ключа в шифрующих таблицах используются: размер таблицы, слово или фраза, задающие перестановку, особенности структуры таблицы.

Шифры простой замены. При шифровании заменой (подстановкой) символы шифруемого текста заменяются символами того же или другого алфавита с заранее установленным правилом замены. В шифре простой замены каждый символ исходного текста заменяется символами того же алфавита по одному правилу на всем протяжении текста. Часто шифры простой замены называют шифрами одноалфавитной подстановки.

Система шифрования Цезаря. Шифр Цезаря является частным случаем шифра простой замены (одноалфавитной подстановки). Свое название этот шифр получил по имени римского императора Гая Юлия Цезаря, который использовал этот шифр при переписке.

Система шифрования Вижинера. Система Вижинера подобна такой системе шифрования Цезаря, у которой ключ подстановки меняется от буквы к букве. Этот шифр многоалфавитной замены можно описать таблицей шифрования, называемой таблицей (квадратом) Вижинера. На рисунках 9 и 10 показаны таблицы Вижинера для русского и английского алфавитов соответственно. Таблица Вижинера используется как для шифрования, так и для расшифрования. Она имеет два входа:

- верхнюю строку подчеркнутых символов, используемую для считывания

очередной буквы исходного открытого текста;

- крайний левый столбец ключа.

Последовательность ключей обычно получают из числовых значений букв ключевого слова. При шифровании исходного сообщения его выписывают в строку, а под ним записывают ключевое слово (или фразу).

Если ключ оказался короче сообщения, то его циклически повторяют. В процессе шифрования находят в верхней строке таблицы очередную букву исходного текста и в левом столбце очередное значение ключа. Очередная буква шифротекста находится на пересечении столбца, определяемого шифруемой буквой, и строки, определяемой числовым значением ключа.

Содержание отчета:

- Общие сведения о классических методах шифрования
- Шифры перестановки: принципы и примеры (в том числе таблицы)
- Шифры простых замен: шифр Цезаря
- Шифр Вижинера: устройство и работа таблиц шифрования
- Выводы об эффективности и уязвимости классических методов

Контрольные вопросы:

- В чем заключаются выводы между перестановками и заменами шифров?
- Как работает шифр Цезаря и в чем его уязвимость?
- Почему шифр Вижинера считается более устойчивым, чем шифр Цезаря?

Лабораторная работа №7 Методы криптографического преобразования информации

Американский стандарт шифрования данных DES. Стандарт шифрования данных DES (Data Encryption Standard) опубликован в 1977 г. Национальным бюро стандартов США. Он предназначен для защиты от несанкци-

онированного доступа к важной, но не секретной информации в государственных и коммерческих организациях США.

- Основные достоинства алгоритма DES:
- используется только один ключ длиной 56 бит;
- относительная простота алгоритма обеспечивает высокую скорость обработки;
- достаточно высокая стойкость алгоритма.

Алгоритм DES основан на комбинировании методов подстановки и перестановки и состоит из чередующейся последовательности блоков перестановки и подстановки. DES осуществляет шифрование 64-битовых блоков данных с помощью 64-битового ключа, в котором значащими являются 56 бит (остальные 8 бит – проверочные биты для контроля на четность). Расшифрование в DES является операцией, обратной шифрованию, и выполняется путем повторения операций шифрования в обратной последовательности.

Содержание отчета:

- История создания и назначения алгоритма DES
- Структура алгоритма: подстановки, перестановки, длина переключателя.
- Процесс шифрования и расшифрования в DES
- Достоинства и недостатки алгоритма DES
- Заключение: актуальность DES в современных условиях

Контрольные вопросы:

- В чем заключается принцип работы алгоритма DES и какова его структура?
- Каковы основные преимущества DES и почему он был принят в качестве стандарта?
- Почему длина ключа DES в современных условиях считается недостаточной?

Лабораторная работа №8 Электронная цифровая подпись

При обмене электронными документами по сети связи возникает проблема аутентификации автора документа и самого документа, т. е. установления подлинности автора и отсутствия изменений в полученном документе. В обычной (бумажной) информатике эти проблемы решаются за счет того, что информация в документе и рукописная подпись автора жестко связаны с физическим носителем (бумагой). В электронных документах на машинных носителях такой связи нет.

Электронная цифровая подпись (ЭЦП) используется для аутентификаюции текстов, передаваемых по телекоммуникационным каналам. Функционально она аналогична обычной рукописной подписи и обладает ее основными достоинствами:

- удостоверяет, что подписанный текст исходит от лица, поставившего подпись;
- не дает самому этому лицу возможности отказаться от обязательств, связанных с подписанным текстом;
- гарантирует целостность подписанного текста.

Цифровая подпись представляет собой относительно небольшое количество дополнительной цифровой информации, передаваемой вместе с подписываемым текстом. Система ЭЦП включает две процедуры: 1) постановки подписи; 2) проверки подписи. В процедуре постановки подписи используется секретный ключ отправителя сообщения, в процедуре проверки подписи – открытый ключ отправителя.

Содержание отчета:

- Проблема аутентификации электронных документов
- Предложение и назначение электронной цифровой загрузки
- Механизм работы ЭЦП: срабатывание и проверка
- используемые ключи и криптографическая основа

- Значение и применение ЭЦП в информационной безопасности

Контрольные вопросы:

- Какую задачу решает электронная цифровая подпись при передаче электронных документов?
- Чем ЭЦП отличается от обычной рукописной приставки и в чем ее преимущества?
- Какие ключи использовались в процедурах создания и проверки ЭЦП?

Лабораторная работа №9. Криптоанализ и методы взлома шифров

Криптоанализ — это наука о методах взлома шифров и исследования уязвимостей криптографических систем. В отличие от криптографии, которая занимается созданием защищенных алгоритмов, криптоанализ направлен на их разрушение или обход. Понимание методов криптоанализа позволяет улучшить стойкость шифров и разрабатывать более надежные системы защиты информации.

Основные методы криптоанализа:

- Атака полного перебора (Brute Force) — проверка всех возможных ключей.
- Атака по известному открытому тексту (Known Plaintext Attack) — использование пар "открытый текст — шифротекст".
- Атака по выбранному открытому тексту (Chosen Plaintext Attack) — злоумышленник может зашифровать любой текст.
- Атака на основе временных задержек (Timing Attack) — анализ времени выполнения операций.
- Дифференциальный и линейный криптоанализ — методы взлома блочных шифров (например, DES).

Содержание отчета:

- Понятие криптоанализа и его роль в информационной безопасности.
- Основные методы атак на шифры.
- Примеры уязвимых алгоритмов и способы их взлома.
- Методы защиты от криптоаналитических атак.
- Практическое применение криптоанализа в тестировании шифров.

Контрольные вопросы:

- Чем отличается криптография от криптоанализа?
- Какие виды атак на шифры вы знаете?
- Почему атака полного перебора не всегда эффективна?
- Как дифференциальный криптоанализ применяется для взлома DES?
- Какие меры защиты могут предотвратить криптоаналитические атаки?

Лабораторная работа №10. Хеширование и защита паролей

Хеширование — это процесс преобразования данных произвольной длины в фиксированную строку (хеш) с помощью математических функций. Хеш-функции используются для проверки целостности данных, хранения паролей и цифровых подписей.

Основные свойства хеш-функций:

- Детерминированность — одинаковые входные данные дают одинаковый хеш.
- Односторонность — сложно восстановить исходные данные по хешу.
- Устойчивость к коллизиям — сложно найти два разных входа с одинаковым хешем.

Применение в защите паролей:

- Пароли хранятся в виде хешей (например, MD5, SHA-256, bcrypt).
- Использование "соли" (salt) для защиты от атак по радужным таблицам.

Содержание отчета:

- Принципы работы хеш-функций.
- Алгоритмы хеширования (MD5, SHA-1, SHA-256, bcrypt).
- Уязвимости старых хеш-функций.
- Методы атак на хеши (радужные таблицы, перебор).
- Современные методы защиты паролей.

Контрольные вопросы:

- Почему пароли хранят в виде хешей, а не в открытом виде?
- Что такое "соль" (salt) и зачем она нужна?
- Чем SHA-256 безопаснее MD5?
- Как работают радужные таблицы?
- Какие алгоритмы хеширования рекомендуются для паролей в 2024 году?

Лабораторная работа №11. Современные алгоритмы шифрования (AES, RSA)

Современные криптографические алгоритмы обеспечивают конфиденциальность, целостность и аутентификацию данных. AES (Advanced Encryption Standard) — симметричный алгоритм, а RSA — асимметричный. Они широко применяются в интернет-безопасности, VPN, SSL/TLS.

AES:

- Блочный шифр (128/192/256 бит).
- Быстрое шифрование больших объемов данных.
- Используется в HTTPS, Wi-Fi (WPA2), архиваторах.

RSA:

- - Основан на сложности факторизации больших чисел.
- - Используется для цифровых подписей и шифрования ключей.

Содержание отчета:

- Принципы симметричного (AES) и асимметричного (RSA) шифрования.
- Математические основы RSA (простые числа, модульная арифметика).
- Режимы работы AES (ECB, CBC, GCM).
- Уязвимости и атаки на AES и RSA.
- Практическое применение в защите данных.

Контрольные вопросы:

- В чем разница между симметричным и асимметричным шифрованием?
- Почему AES считается безопасным?
- Как работает алгоритм RSA?
- Какие атаки возможны на RSA?
- Где применяются AES и RSA в реальных системах?

Лабораторная работа №12. Квантовая криптография

Квантовая криптография использует законы квантовой механики для защиты информации. Основной метод — квантовое распределение ключей (QKD), которое теоретически невозможно взломать без обнаружения.

Принципы:

- Принцип неопределенности Гейзенберга — нельзя измерить квантовое состояние без его изменения.
- Квантовая запутанность — позволяет обнаруживать подслушивание.

Протокол BB84:

- Первый алгоритм квантовой криптографии.
- Использует поляризацию фотонов для передачи ключа.

Содержание отчета:

- Основы квантовой механики в криптографии.
- Протоколы квантового распределения ключей (BB84, E91).
- Угрозы квантовых компьютеров для классических шифров.
- Современные разработки в квантовой криптографии.

Контрольные вопросы:

- Как квантовая криптография обеспечивает безопасность?
- В чем суть протокола BB84?
- Почему квантовые компьютеры опасны для RSA?
- Какие физические носители используются в QKD?
- Какие есть ограничения у квантовой криптографии?