Дисциплина

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Изучение и программная реализация методов шифрования. Лабораторные работы

СОДЕРЖАНИЕ

ЦЕЛЬ РАБОТ

Изучить принципы работы традиционных криптографических систем. Зашифровать сообщение с использованием предложенных шифров. Описать постановку задачи и метод её решения на формальном языке.

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования/расшифрования. В соответствии со стандартом ГОСТ 28147-89 под шифром понимают совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом криптографического преобразования.

Ключ - это конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма.

Основной характеристикой шифра является криптостойкость, которая определяет его стойкость к раскрытию методами криптоанализа. Обычно эта характеристика определяется интервалом времени, необходимым для раскрытия шифра.

К шифрам, используемым для криптографической защиты информации, предъявляется ряд требований:

- Достаточная криптостойкость (надежность закрытия данных);
- Простота процедур шифрования и расшифрования;
- Незначительная избыточность информации за счет шифрования;
- Нечувствительность к небольшим ошибкам шифрования и др.

В той или иной мере этим требованиям отвечают:

- шифры перестановок;
- шифры замены;
- шифры гаммирования;
- шифры, основанные на аналитических преобразованиях шифруемых данных.

Шифрование перестановкой заключается в том, что символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста. При достаточной длине блока, и пределах которого осуществляется перестановка, и сложном неповторяющемся порядке перестановки можно достигнуть приемлемой для простых практических приложений стойкости шифра.

Шифрование заменой (подстановкой) заключается в том, что символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены.

Шифрование гаммированиием заключается в том, что символы шифруемою текста складываются с символами некоторой случайной последовательности, именуемой гаммой шифра. Стойкость шифрования определяется в основном длиной (периодом) неповторяющейся части гаммы шифра. Поскольку с помощью ЭВМ можно генерировать практически бесконечную гамму шифра, то данный способ является одним из основных для шифрования информации в автоматизированных системах.

Шифрование аналитическим преобразованием заключается в том, что шифруемый текст преобразуется по некоторому аналитическому правилу (формуле).

Например, можно использовать правило умножения вектора на матрицу, причем умножаемая матрица является ключом шифрования (поэтому ее размер и содержание должны храниться в секрете), а символами умножаемого вектора последовательно служат символы шифруемого текста. Другим примером может служить использование так называемых однонаправленных функций для построения криптосистем с открытым ключом.

Процессы шифрования и расшифрования осуществляются в рамках некоторой криптосистемы. Характерной особенностью симметричной криптосистемы является применение одного и того же секретного ключа как при шифровании, так и при расшифровании сообщений.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТ

Используя традиционные методы шифрования, зашифровать сообщение (по вариантам).

1. Выбрать ключ.
2. Зашифровать сообщение вручную указанным методом.
3. Разработать и написать программу, реализующую указанный метод шифрования и позволяющую расшифровать полученное сообщение.
4. Составить отчет.

СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист с указанием варианта
2. Теоретическое описание метода шифрования.
3. Исходное сообщение
4. Ключ
5. Описание произведенного криптографического преобразования.
6. Криптограмма.
7. Алгоритм разработанной программы.
8. Код программы.
9. Иллюстрация результата работы программы.

ЛАБОРАТОРНАЯ РАБОТА № 1. ОДНОАЛФАВИТНАЯ ПОДСТАНОВКА

Варианты сообщений для шифрования:

Номер варианта	Сообщение
1	Однонаправленную хэш-функцию можно построить, используя симметричный блочный алгоритм.
2	При выполнении лабораторных работ разрешается пользоваться конспектами лекций.
3	Экзамен представляет собой ответы на теоретические вопросы.
4	Однонаправленная функция – это основное понятие в криптографии с открытым ключом.
5	После приема подписанного сообщения получатель должен проверить, соответствует ли подпись сообщению.
6	Анализ возможностей подделки подписей называется криптоанализом.
7	Попытка сфальсифицировать подпись или подписанный документ криптоаналитики называют «атака».
8	Более вероятен поиск криптоаналитиком коллизий первого и второго рода.
9	Коллизия первого рода эквивалентна экзистенциальной подделке, а коллизия второго рода – выборочной.
10	Неоспоримая подпись может быть верифицирована только путем непосредственного взаимодействия с подписывающей стороной А.
11	Метод открытой адресации заключается в том, что в массиве таблицы хранятся пары ключ-значение.
12	Для хэш-таблиц есть два основных метода борьбы с коллизиями - это метод цепочек и метод открытой адресации.
13	Самой «опасной» атакой является адаптивная атака на основе выбранных сообщений
14	Защиту информации принято разделять на несколько видов: правовая, техническая, криптографическая, физическая защита информации.
15	Криптографическая защита информации предусматривает защиту информации с помощью ее криптографического преобразования.
16	Под угрозой безопасности данных будем понимать потенциально существующую возможность случайного или преднамеренного действия.
17	Прямые каналы утечки данных, требуют непосредственного доступа к техническим средствам информационной системы и данным
18	Умышленные угрозы преследуют цель нанесения ущерба пользователям сети и подразделяются на активные и пассивные.
19	Механизмы электронной подписи используются для реализации служб аутентификации и защиты от отказов.
20	Механизмы обеспечения аутентификации - различают одностороннюю и взаимную аутентификацию.
21	Неформальными называются такие средства защиты, которые реализуются в результате деятельности людей.
22	В области разработки стандартов работает ряд международных организаций, национальных органов, национальных комиссий.
23	Существует развитая классификация угроз информационной безопасности.
24	Маскировка представляет собой метод защиты данных путем их криптографического закрытия.
25	Аудит системы защиты проводится регулярно через небольшие промежутки времени.

26	Механизмы подстановки трафика используются для реализации службы засекречивания потока данных
27	При построении системы безопасности применяются политики защиты, основанные на требованиях, определяемых направлениями деятельности компании
28	Существует два класса криптосистем: симметричные (одноключевые) и асимметричные (двухключевые).
29	Управление ключами – это информационный процесс, реализующий генерацию, хранение и распределение ключей.
30	Электронная подпись является аналогом собственноручной подписи в предусмотренных законом случаях.
31	У.Диффи и М.Хеллман в 1976 году впервые предложили понятие «электронная цифровая подпись».
32	Процессы шифрования и расшифрования осуществляются в рам-ках некоторой криптосистемы.
33	Стойкость шифрования определяется в основном длиной (периодом) неповторяющейся части гаммы шифра
34	Ключ - это конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных.
35	Проблемы конфиденциальности и целостности информации тесно связаны между собой.

ЛАБОРАТОРНАЯ РАБОТА № 2. МНОГОАЛФАВИТНАЯ ОДНОКОНТУРНАЯ ПОДСТАНОВКА

Варианты сообщений для шифрования:

Номер варианта	Сообщение
1	Закон саморазрушения и закон самосохранения одинаково сильны в человечестве!
2	Информационные активы – это базы данных и файлы данных, системная документация, руководства и инструкции.
3	Активы программного обеспечения – это прикладное программное обеспечение, системное программное обеспечение, и др.
4	Никакой транспорт не будет попутным, если не знаешь, куда идти.
5	Доступность – это свойство информации, при котором субъекты, имеющие законное право доступа к информации, могут это право осуществить.
6	Злоумышленник может пытаться изменить передаваемые сообщения, вставляя в них одни слова, удаляя другие.
7	Понятие «целостность» обозначает одно из свойств информации.
8	Существует весьма развитая классификация угроз информационной безопасности.
9	К понятию «конфиденциальная информация» тесно примыкают понятия «государственная тайна» и «коммерческая тайна».
10	Сегодня имеется множество международных и отечественных наработок в области безопасности и защиты информации.
11	На входящих в те же самые реки притекают в один раз одни, в другой раз другие воды.
12	Конечно, я умный человек, умнее очень многих, но счастье не в этом.
13	Лучшие враги - любимые ученики, лучшая защита от них - новые ученики.
14	Слова так невыразительны, неточны, так ужасно примитивны в сравнении с рисунком, живописью, скульптурой.
15	Протоколы влияют и на возможность поддержания целостности данных.
16	Знать прошлое достаточно неприятно; знать еще и будущее было бы просто невыносимо.
17	Хорошее воспитание не в том, что ты не прольешь соуса на скатерть, а в том, что ты не заметишь, если это сделает кто-нибудь другой.
18	Важной характеристикой Европейских Критериев является отсутствие априорных требований к условиям, в которых должна работать информационная система.
19	История - самый лучший учитель, у которого самые плохие ученики.
20	Протокол позволяет устанавливать защищенное соединение, производить контроль целостности данных и решать различные сопутствующие задачи.
21	Чем более мы размышляем, тем более убеждаемся, что ничего не знаем.
22	Спецификации функций безопасности - это важнейшая часть описания объекта оценки.
23	Язык имеет большое значение еще и потому, что с его помощью мы можем прятать наши мысли.
24	Оптимизм - это страсть утверждать, что все хорошо, когда в действительности все плохо.
25	Говорят, что несчастие хорошая школа, может быть. Но счастье есть лучший университет.
26	Бурное развитие криптографические системы получили в годы первой и второй мировых войн.
27	Криптография представляет собой совокупность методов преобразования данных.

28	Преобразование шифрования может быть симметричным или асимметричным относительно преобразования расшифрования.
29	В симметричной криптосистеме секретный ключ надо передавать отправителю и получателю по защищенному каналу распространения ключей
30	Объектами исследования являются алгоритмы шифрования, алгоритмы электронной подписи и соответствующие стандарты.
31	В асимметричной криптосистеме передают по незащищенному каналу только открытый ключ, а секретный ключ сохраняют на месте его генерации.
32	Существуют два основных современных класса шифров: поточные и блочные шифры.
33	К основным угрозам безопасности относят раскрытие конфиденциальной информации.
34	С точки зрения модели взаимодействия открытых систем, службы и механизмы безопасности могут использоваться на любом из уровней модели.
35	Для использования механизмов шифрования необходима организация специальной службы генерации ключей и их распределения между абонентами.

ЛАБОРАТОРНАЯ РАБОТА № 3. МНОГОАЛФАВИТНАЯ МНОГОКОНТУРНАЯ ПОДСТАНОВКА

Варианты сообщений для шифрования:

Номер варианта	Сообщение
1	Проблемы конфиденциальности и целостности информации тесно связаны между собой.
2	Однонаправленную хэш-функцию можно построить, используя симметричный блочный алгоритм.
3	При выполнении лабораторных работ разрешается пользоваться конспектами лекций.
4	Экзамен представляет собой ответы на теоретические вопросы.
5	Однонаправленная функция – это основное понятие в криптографии с открытым ключом.
6	После приема подписанного сообщения получатель должен проверить, соответствует ли подпись сообщению.
7	Анализ возможностей подделки подписей называется криптоанализом.
8	Попытка сфальсифицировать подпись или подписанный документ криптоаналитики называют «атака».
9	Более вероятен поиск криптоаналитиком коллизий первого и второго рода.
10	Коллизия первого рода эквивалентна экзистенциальной подделке, а коллизия второго рода – выборочной.
11	Неоспоримая подпись может быть верифицирована только путем непосредственного взаимодействия с подписывающей стороной А.
12	Метод открытой адресации заключается в том, что в массиве таблицы хранятся пары ключ-значение.
13	Для хэш-таблиц есть два основных метода борьбы с коллизиями - это метод цепочек и метод открытой адресации.
14	Самой «опасной» атакой является адаптивная атака на основе выбранных сообщений
15	Защиту информации принято разделять на несколько видов: правовая, техническая, криптографическая, физическая защита информации.
16	Криптографическая защита информации предусматривает защиту информации с помощью ее криптографического преобразования.
17	Под угрозой безопасности данных будем понимать потенциально существующую возможность случайного или преднамеренного действия.
18	Прямые каналы утечки данных, требуют непосредственного доступа к техническим средствам информационной системы и данным
19	Умышленные угрозы преследуют цель нанесения ущерба пользователям сети и подразделяются на активные и пассивные.
20	Механизмы электронной подписи используются для реализации служб аутентификации и защиты от отказов.
21	Механизмы обеспечения аутентификации - различают одностороннюю и взаимную аутентификацию.
22	Неформальными называются такие средства защиты, которые реализуются в результате деятельности людей.
223	В области разработки стандартов работает ряд международных организаций, национальных органов, национальных комиссий.
24	Существует развитая классификация угроз информационной безопасности.
25	Маскировка представляет собой метод защиты данных путем их криптографического закрытия.
26	Аудит системы защиты проводится регулярно через небольшие промежутки времени.
27	Механизмы подстановки трафика используются для реализации службы засекречивания потока данных

28	При построении системы безопасности применяются политики защиты, основанные на требованиях, определяемых направлениями деятельности компании
29	Существует два класса криптосистем: симметричные (одноключевые) и асимметричные (двухключевые).
30	Управление ключами – это информационный процесс, реализующий генерацию, хранение и распределение ключей.
31	Электронная подпись является аналогом собственноручной подписи в предусмотренных законом случаях.
32	У.Диффи и М.Хеллман в 1976 году впервые предложили понятие «электронная цифровая подпись».
33	Процессы шифрования и расшифрования осуществляются в рам-ках некоторой криптосистемы.
34	Стойкость шифрования определяется в основном длиной (периодом) неповторяющейся части гаммы шифра
35	Ключ - это конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных.

ЛАБОРАТОРНАЯ РАБОТА № 4. МНОГОАЛФАВИТНАЯ ПОДСТАНОВКА ПО ТАБЛИЦЕ ВИЖЕНЕРА

Варианты сообщений для шифрования:

Номер варианта	Сообщение
1	Для использования механизмов шифрования необходима организация специальной службы генерации ключей и их распределения между абонентами.
2	Закон саморазрушения и закон самосохранения одинаково сильны в человечестве!
3	Информационные активы – это базы данных и файлы данных, системная документация, руководства и инструкции.
4	Активы программного обеспечения – это прикладное программное обеспечение, системное программное обеспечение, и др.
5	Никакой транспорт не будет попутным, если не знаешь, куда идти.
6	Доступность – это свойство информации, при котором субъекты, имеющие законное право доступа к информации, могут это право осуществить.
7	Злоумышленник может пытаться изменить передаваемые сообщения, вставляя в них одни слова, удаляя другие.
8	Понятие «целостность» обозначает одно из свойств информации.
9	Существует весьма развитая классификация угроз информационной безопасности.
10	К понятию «конфиденциальная информация» тесно примыкают понятия «государственная тайна» и «коммерческая тайна».
11	Сегодня имеется множество международных и отечественных наработок в области безопасности и защиты информации.
12	На входящих в те же самые реки притекают в один раз одни, в другой раз другие воды.
13	Конечно, я умный человек, умнее очень многих, но счастье не в этом.
14	Лучшие враги - любимые ученики, лучшая защита от них - новые ученики.
15	Слова так невыразительны, неточны, так ужасно примитивны в сравнении с рисунком, живописью, скульптурой.
16	Протоколы влияют и на возможность поддержания целостности данных.
17	Знать прошлое достаточно неприятно; знать еще и будущее было бы просто невыносимо.
18	Хорошее воспитание не в том, что ты не прольешь соуса на скатерть, а в том, что ты не заметишь, если это сделает кто-нибудь другой.
19	Важной характеристикой Европейских Критериев является отсутствие априорных требований к условиям, в которых должна работать информационная система.
20	История - самый лучший учитель, у которого самые плохие ученики.
21	Протокол позволяет устанавливать защищенное соединение, производить контроль целостности данных и решать различные сопутствующие задачи.
22	Чем более мы размышляем, тем более убеждаемся, что ничего не знаем.
23	Спецификации функций безопасности - это важнейшая часть описания объекта оценки.
24	Язык имеет большое значение еще и потому, что с его помощью мы можем прятать наши мысли.
25	Оптимизм - это страсть утверждать, что все хорошо, когда в действительности все плохо.
26	Говорят, что несчастие хорошая школа, может быть. Но счастье есть лучший университет.
27	Бурное развитие криптографические системы получили в годы первой и второй мировых войн.
28	Криптография представляет собой совокупность методов преобразования данных.
29	Преобразование шифрования может быть симметричным или асимметричным относительно преобразования расшифрования.

30	В симметричной криптосистеме секретный ключ надо передавать отправителю и получателю по защищенному каналу распространения ключей
31	Объектами исследования являются алгоритмы шифрования, алгоритмы электронной подписи и соответствующие стандарты.
32	В асимметричной криптосистеме передают по незащищенному каналу только открытый ключ, а секретный ключ сохраняют на месте его генерации.
33	Существуют два основных современных класса шифров: поточные и блочные шифры.
34	К основным угрозам безопасности относят раскрытие конфиденциальной информации.
35	С точки зрения модели взаимодействия открытых систем, службы и механизмы безопасности могут использоваться на любом из уровней модели.

ЛАБОРАТОРНАЯ РАБОТА № 5. ПРОСТАЯ ПЕРЕСТАНОВКА

Варианты сообщений для шифрования:

Номер варианта	Сообщение
1	Ключ - это конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных.
2	Проблемы конфиденциальности и целостности информации тесно связаны между собой.
3	Однонаправленную хэш-функцию можно построить, используя симметричный блочный алгоритм.
4	При выполнении лабораторных работ разрешается пользоваться конспектами лекций.
5	Экзамен представляет собой ответы на теоретические вопросы.
6	Однонаправленная функция – это основное понятие в криптографии с открытым ключом.
7	После приема подписанного сообщения получатель должен проверить, соответствует ли подпись сообщению.
8	Анализ возможностей подделки подписей называется криптоанализом.
9	Попытка сфальсифицировать подпись или подписанный документ криптоаналитики называют «атака».
10	Более вероятен поиск криптоаналитиком коллизий первого и второго рода.
11	Коллизия первого рода эквивалентна экзистенциальной подделке, а коллизия второго рода – выборочной.
12	Неоспоримая подпись может быть верифицирована только путем непосредственного взаимодействия с подписывающей стороной А.
13	Метод открытой адресации заключается в том, что в массиве таблицы хранятся пары ключ-значение.
14	Для хэш-таблиц есть два основных метода борьбы с коллизиями - это метод цепочек и метод открытой адресации.
15	Самой «опасной» атакой является адаптивная атака на основе выбранных сообщений
16	Защиту информации принято разделять на несколько видов: правовая, техническая, криптографическая, физическая защита информации.
17	Криптографическая защита информации предусматривает защиту информации с помощью ее криптографического преобразования.
18	Под угрозой безопасности данных будем понимать потенциально существующую возможность случайного или преднамеренного действия.
19	Прямые каналы утечки данных, требуют непосредственного доступа к техническим средствам информационной системы и данным
20	Умышленные угрозы преследуют цель нанесения ущерба пользователям сети и подразделяются на активные и пассивные.
21	Механизмы электронной подписи используются для реализации служб аутентификации и защиты от отказов.
22	Механизмы обеспечения аутентификации - различают одностороннюю и взаимную аутентификацию.
23	Неформальными называются такие средства защиты, которые реализуются в результате деятельности людей.
24	В области разработки стандартов работает ряд международных организаций, национальных органов, национальных комиссий.
25	Существует развитая классификация угроз информационной безопасности.
26	Маскировка представляет собой метод защиты данных путем их криптографического закрытия.
27	Аудит системы защиты проводится регулярно через небольшие промежутки времени.

28	Механизмы подстановки трафика используются для реализации службы засекречивания потока данных
29	При построении системы безопасности применяются политики защиты, основанные на требованиях, определяемых направлениями деятельности компании
30	Существует два класса криптосистем: симметричные (одноключевые) и асимметричные (двухключевые).
31	Управление ключами – это информационный процесс, реализующий генерацию, хранение и распределение ключей.
32	Электронная подпись является аналогом собственноручной подписи в предусмотренных законом случаях.
33	У.Диффи и М.Хеллман в 1976 году впервые предложили понятие «электронная цифровая подпись».
34	Процессы шифрования и расшифрования осуществляются в рам-ках некоторой криптосистемы.
35	Стойкость шифрования определяется в основном длиной (периодом) неповторяющейся части гаммы шифра

ЛАБОРАТОРНАЯ РАБОТА № 6. ПЕРЕСТАНОВКА, УСЛОЖНЕННАЯ ПО ТАБЛИЦЕ

Варианты сообщений для шифрования:

Номер варианта	Сообщение
1	С точки зрения модели взаимодействия открытых систем, службы и механизмы безопасности могут использоваться на любом из уровней модели.
2	Для использования механизмов шифрования необходима организация специальной службы генерации ключей и их распределения между абонентами.
3	Закон саморазрушения и закон самосохранения одинаково сильны в человечестве!
4	Информационные активы – это базы данных и файлы данных, системная документация, руководства и инструкции.
5	Активы программного обеспечения – это прикладное программное обеспечение, системное программное обеспечение, и др.
6	Никакой транспорт не будет попутным, если не знаешь, куда идти.
7	Доступность – это свойство информации, при котором субъекты, имеющие законное право доступа к информации, могут это право осуществить.
8	Злоумышленник может пытаться изменить передаваемые сообщения, вставляя в них одни слова, удаляя другие.
9	Понятие «целостность» обозначает одно из свойств информации.
10	Существует весьма развитая классификация угроз информационной безопасности.
11	К понятию «конфиденциальная информация» тесно примыкают понятия «государственная тайна» и «коммерческая тайна».
12	Сегодня имеется множество международных и отечественных наработок в области безопасности и защиты информации.
13	На входящих в те же самые реки притекают в один раз одни, в другой раз другие воды.
14	Конечно, я умный человек, умнее очень многих, но счастье не в этом.
15	Лучшие враги - любимые ученики, лучшая защита от них - новые ученики.
16	Слова так невыразительны, неточны, так ужасно примитивны в сравнении с рисунком, живописью, скульптурой.
17	Протоколы влияют и на возможность поддержания целостности данных.
18	Знать прошлое достаточно неприятно; знать еще и будущее было бы просто невыносимо.
19	Хорошее воспитание не в том, что ты не прольешь соуса на скатерть, а в том, что ты не заметишь, если это сделает кто-нибудь другой.
20	Важной характеристикой Европейских Критериев является отсутствие априорных требований к условиям, в которых должна работать информационная система.
21	История - самый лучший учитель, у которого самые плохие ученики.
22	Протокол позволяет устанавливать защищенное соединение, производить контроль целостности данных и решать различные сопутствующие задачи.
23	Чем более мы размышляем, тем более убеждаемся, что ничего не знаем.
24	Спецификации функций безопасности - это важнейшая часть описания объекта оценки.
25	Язык имеет большое значение еще и потому, что с его помощью мы можем прятать наши мысли.
26	Оптимизм - это страсть утверждать, что все хорошо, когда в действительности все плохо.
27	Говорят, что несчастие хорошая школа, может быть. Но счастье есть лучший университет.
28	Бурное развитие криптографические системы получили в годы первой и второй мировых войн.
29	Криптография представляет собой совокупность методов преобразования данных.

30	Преобразование шифрования может быть симметричным или асимметричным относительно преобразования расшифрования.
31	В симметричной криптосистеме секретный ключ надо передавать отправителю и получателю по защищенному каналу распространения ключей
32	Объектами исследования являются алгоритмы шифрования, алгоритмы электронной подписи и соответствующие стандарты.
33	В асимметричной криптосистеме передают по незащищенному каналу только открытый ключ, а секретный ключ сохраняют на месте его генерации.
34	Существуют два основных современных класса шифров: поточные и блочные шифры.
35	К основным угрозам безопасности относят раскрытие конфиденциальной информации.

ЛАБОРАТОРНАЯ РАБОТА № 7. ГАММИРОВАНИЕ

Варианты сообщений для шифрования:

Номер варианта	Сообщение
1	Стойкость шифрования определяется в основном длиной (периодом) неповторяющейся части гаммы шифра
2	Ключ - это конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных.
3	Проблемы конфиденциальности и целостности информации тесно связаны между собой.
4	Однонаправленную хэш-функцию можно построить, используя симметричный блочный алгоритм.
5	При выполнении лабораторных работ разрешается пользоваться конспектами лекций.
6	Экзамен представляет собой ответы на теоретические вопросы.
7	Однонаправленная функция – это основное понятие в криптографии с открытым ключом.
8	После приема подписанного сообщения получатель должен проверить, соответствует ли подпись сообщению.
9	Анализ возможностей подделки подписей называется криптоанализом.
10	Попытка сфальсифицировать подпись или подписанный документ криптоаналитики называют «атака».
11	Более вероятен поиск криптоаналитиком коллизий первого и второго рода.
12	Коллизия первого рода эквивалентна экзистенциальной подделке, а коллизия второго рода – выборочной.
13	Неоспоримая подпись может быть верифицирована только путем непосредственного взаимодействия с подписывающей стороной А.
14	Метод открытой адресации заключается в том, что в массиве таблицы хранятся пары ключ-значение.
15	Для хэш-таблиц есть два основных метода борьбы с коллизиями - это метод цепочек и метод открытой адресации.
16	Самой «опасной» атакой является адаптивная атака на основе выбранных сообщений
17	Защиту информации принято разделять на несколько видов: правовая, техническая, криптографическая, физическая защита информации.
18	Криптографическая защита информации предусматривает защиту информации с помощью ее криптографического преобразования.
19	Под угрозой безопасности данных будем понимать потенциально существующую возможность случайного или преднамеренного действия.
20	Прямые каналы утечки данных, требуют непосредственного доступа к техническим средствам информационной системы и данным
21	Умышленные угрозы преследуют цель нанесения ущерба пользователям сети и подразделяются на активные и пассивные.
22	Механизмы электронной подписи используются для реализации служб аутентификации и защиты от отказов.
23	Механизмы обеспечения аутентификации - различают одностороннюю и взаимную аутентификацию.
24	Неформальными называются такие средства защиты, которые реализуются в результате деятельности людей.
25	В области разработки стандартов работает ряд международных организаций, национальных органов, национальных комиссий.
26	Существует развитая классификация угроз информационной безопасности.
27	Маскировка представляет собой метод защиты данных путем их криптографического закрытия.

28	Аудит системы защиты проводится регулярно через небольшие промежутки времени.
29	Механизмы подстановки трафика используются для реализации службы засекречивания потока данных
30	При построении системы безопасности применяются политики защиты, основанные на требованиях, определяемых направлениями деятельности компании
31	Существует два класса криптосистем: симметричные (одноключевые) и асимметричные (двухключевые).
32	Управление ключами – это информационный процесс, реализующий генерацию, хранение и распределение ключей.
33	Электронная подпись является аналогом собственноручной подписи в предусмотренных законом случаях.
34	У.Диффи и М.Хеллман в 1976 году впервые предложили понятие «электронная цифровая подпись».
35	Процессы шифрования и расшифрования осуществляются в рам-ках некоторой криптосистемы.