Титулка

Зміст

[Список сокращений и условных обозначений 4](#_Toc511677823)

[Словарь терминов 5](#_Toc511677824)

[Введение 8](#_Toc511677825)

[1 Уровни информационной безопасности 10](#_Toc511677826)

[Теоретические ведомости 10](#_Toc511677827)

[Задания 10](#_Toc511677828)

[Ход работы 10](#_Toc511677829)

[Вопросы для самоконтроля 10](#_Toc511677830)

[2 Локальная защита устройств 11](#_Toc511677831)

[Теоретические ведомости 11](#_Toc511677832)

[Задания 11](#_Toc511677833)

[Ход работы 11](#_Toc511677834)

[Вопросы для самоконтроля 11](#_Toc511677835)

[3 Мировые стандарты безопасности 12](#_Toc511677836)

[Теоретические ведомости 12](#_Toc511677837)

[Задания 12](#_Toc511677838)

[Ход работы 12](#_Toc511677839)

[Вопросы для самоконтроля 12](#_Toc511677840)

[4 Методы сокрытия информации 13](#_Toc511677841)

[Теоретические ведомости 13](#_Toc511677842)

[Задания 13](#_Toc511677843)

[Ход работы 13](#_Toc511677844)

[Вопросы для самоконтроля 13](#_Toc511677845)

[5 Сжатие и Архивация данных 14](#_Toc511677846)

[Теоретические ведомости 14](#_Toc511677847)

[Задания 14](#_Toc511677848)

[Ход работы 14](#_Toc511677849)

[Вопросы для самоконтроля 14](#_Toc511677850)

[6 Cisco. Часть 1 15](#_Toc511677851)

[Теоретические ведомости 15](#_Toc511677852)

[Задания 15](#_Toc511677853)

[Ход работы 15](#_Toc511677854)

[Вопросы для самоконтроля 15](#_Toc511677855)

[7 Cisco. Часть 2 16](#_Toc511677856)

[Теоретические ведомости 16](#_Toc511677857)

[Задания 16](#_Toc511677858)

[Ход работы 16](#_Toc511677859)

[Вопросы для самоконтроля 16](#_Toc511677860)

[8 анализ данных 17](#_Toc511677861)

[Теоретические ведомости 17](#_Toc511677862)

[Задания 17](#_Toc511677863)

[Ход работы 17](#_Toc511677864)

[Вопросы для самоконтроля 17](#_Toc511677865)

[Додаток А 18](#_Toc511677866)

[Додаток Б 19](#_Toc511677867)

1. Список сокращений и условных обозначений
2. Словарь терминов

**Открытый (исходный) текст** — данные (не обязательно текстовые), пере­даваемые без использования криптографии.

**Шифротекст, шифрованный (закрытый) текст** — данные, полученные после применения криптосистемы.

**Шифр, криптосистема** — совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты.

**Символ** — это любой знак, в том числе буква, цифра или знак препинания. **Алфавит** — конечное множество используемых для кодирования информации символов. Стандартный алфавит может быть изменён или дополнен символами. **Ключ** — параметр шифра, определяющий выбор конкретного преобразования данного текста. В современных шифрах криптографическая стойкость шифра це­ликом определяется секретностью ключа (принцип Керкгоффса).

**Шифрование** — процесс нормального применения криптографического преобразования открытого текста на основе алгоритма и ключа, в результате ко­торого возникает шифрованный текст.

**Расшифровывание** — процесс нормального применения криптографиче­ского преобразования шифрованного текста в открытый.

**Асимметричный шифр, двухключевой шифр, шифр с открытым ключом** — шифр, в котором используются два ключа, шифрующий и расшифро­вывающий. При этом, зная лишь ключ зашифровывания, нельзя расшифровать сообщение, и наоборот.

**Открытый ключ** — тот из двух ключей асимметричной системы, который свободно распространяется. Шифрующий для секретной переписки и расшифро­вывающий — для электронной подписи.

**Секретный ключ, закрытый ключ** — тот из двух ключей асимметричной системы, который хранится в секрете. Криптоанализ — наука, изучающая мате­матические методы нарушения конфиденциальности и целостности информации.

**Система шифрования (шифрсистема)** — это любая система, которую мо­жно использовать для обратимого изменения текста сообщения с целью сделать его непонятным для всех, кроме адресата.

**Криптостойкостью** — это характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т.е. способность противостоять криптоанализу).

**Криптоаналитик** — учёный, создающий и применяющий методы крипто­анализа. Криптография и криптоанализ составляют криптологию, как единую науку о создании и взломе шифров (такое деление привнесено с запада, до этого в СССР и России не применялось специального деления).

**Криптографическая атака** — попытка криптоаналитика вызвать откло­нения в атакуемой защищённой системе обмена информацией. Успешную криптографическую атаку называют взлом или вскрытие.

**Дешифрование (дешифровка)** — процесс извлечения открытого текста без знания криптографического ключа на основе известного шифрованного. Тер­мин дешифрование обычно применяют по отношению к процессу криптоанализа шифротекста (криптоанализ сам по себе, вообще говоря, может заключаться и в анализе криптосистемы, а не только зашифрованного ею открытого сообщения).

**Криптографическая стойкость** — способность криптографического алго­ритма противостоять криптоанализу.

**Имитозащита** — защита от навязывания ложной информации. Другими словами, текст остаётся открытым, но появляется возможность проверить, что его не изменяли ни случайно, ни намеренно. Имитозащита достигается обычно за счет включения в пакет передаваемых данных имитовставки.

**Имитовставка** — блок информации, применяемый для имитозащиты, за­висящий от ключа и данных.

**Электронная цифровая подпись(электронная подпись)** — асимметри­чная имитовставка (ключ защиты отличается от ключа проверки). Другими словами, такая имитовставка, которую проверяющий не может подделать.

**Центр сертификации** — сторона, чья честность неоспорима, а открытый ключ широко известен. Электронная подпись центра сертификации подтверждает подлинность открытого ключа.

**Хеш-функция** — функция, которая преобразует сообщение произвольной длины в число («свёртку») фиксированной длины. Для криптографической хеш- функции (в отличие от хеш-функции общего назначения) сложно вычислить обратную и даже найти два сообщения с общей хеш-функцией.

1. Введение

Цель практических работ состоит в изучении основных концепций информационной безопасности(ИБ), понимание уровней ИБ и целей. Определение угроз на аппаратном и сетевом уровнях.

**Первая работа** изучить основные понятия и уровни ИБ, составляющие ИБ и виды информационных угроз. После чего подготовиться к тестированию по заданным аспектам. На занятии разобрать ситуацию по варианту или предложенную руководителем.

**Вторая работа** данная работа предполагает настройку устройства, предположительно компьютера. В практическом занятии студент должен провести настройку компьютера, целью является защита от самых распространённых ошибок допускаемыми системными администраторами небольших фирм. После чего протестировать и оформить результаты в отчёт.

**Третья работа** проведение семинара предполагает ознакомить студента с основными стандартами информационной безопасности. Изучить сервисы и механизмы защиты. Так же предполагает разбор нескольких ситуаций из примеров или предложенные студентами.

**Четвёртая работа** ознакомиться с одним из методов криптографического преобразования информации, а именно стеганографией. Рассмотреть примеры сокрытия данных в файле, использование шумов и стохастической модуляции. Реализовать преобразование одним из методов.

**Пятая работа** разделена на две части. Первая, предполагает изучение методов сжатия данных. Изучение алгоритма Хаффмана и Лемпеля-Зива, реализация сжатия больших текстов и оценка актуальности. Вторая, рассматривает архивацию данных, как объект защиты целостности. Ознакомление с возможностями архивации и различными реализациями.

**Шестая работа** является базовой по настройке и работе в сетях, рассматривается вариант «белой», безопасной сети, её подключение и общая настройка прав. Работы выполняются в среде Cisco. Можно использовать другое ПО, если оно предоставляет требуемый функционал.

**Седьмая работа** – это продолжение шестой работы, где студент должен будет реализовать безопасное подключение всей сети к мировой сети Интернет.

**Восьмая работа** настроена на исследование анализа больших потоков данных, прослушивание сети. Тут нужно будет дописать

# Уровни информационной безопасности

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

1. Криптография и её роль в обществе.
2. Объяснить цель и задачи криптографии.
3. Пояснить какие бывают криптографические методы.
4. Виды криптографии и их классификация.
5. Отличие симметричных и асимметричный шифров.
6. Пояснить что такое исходный текст, шифр, ключ.
7. Принцип подбора ключа в симметричных криптосистемах.
8. Принцип работы симметричных шифров. Приведите примеры.
9. Принцип работы асимметричных шифров. Приведите примеры.
10. Шифры одиночной перестановки и перестановки по ключевому слову. Шифр Гронфельда.
11. Шифры двойной перестановки. Шифрование с помощью магического квадрата.

# Локальная защита устройств

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

# Мировые стандарты безопасности

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

# Методы сокрытия информации

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

# Сжатие и Архивация данных

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

# Cisco. Часть 1

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

# Cisco. Часть 2

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

# Анализ данных

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

1. Додаток А
2. Додаток Б