НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

«МЭИ»

ИНЖЕНЕРНО-ЭКОНОМИЧЕСКИЙ ИНСТИТУТ

Кафедра безопасности и информационной технологии

Направление подготовки бакалавриата

10.03.01 «Информационная безопасность»

Учебная практика № 2

Криптографические системы защиты

Студент группы ИЭ-40-20 Ле К.З.

Дата: 08/05/2021

Москва, 2021 г

Содержание

1 Введение **1**

2 Исследовательно-аналическая часть **1**

2.1 Что такое криптография и её назначения в области информационной безопасности 1

2.2 Основные понятия криптографических систем и требования к ним 2

2.3 Разделы криптографии 3

1 Введение

Криптография появилась очень долго раньше, чтобы обслужить в войнах. Она использовала простую математику но очень эффективно для защиты информации. Когда компьютер и сети родились, криптография использовалась для защиты данные, но теперь сложные математические понятия используют, благодаря возможностей компьютеров.

2 Исследовательно-аналическая часть

2.1 Что такое криптография и её назначения в области информационной безопасности

Что такое криптография? - это область науки, которая использует математику для защиты информация

Когда передавать данные на сетях, мы заботимся о

- безопасности: если A хочет передать информации в B, но не хочет другие знают, тогда A использует криптографию, чтобы трансфомировать обычные данные в данные, которые не могут читать

- авторизации: А хочет знает, послал ли В эти информации, или другой человек С послал но скажет себя В

2.2 Основные понятия криптографических систем и требования к ним

Основные понятия криптографического системы:

- Шифрование - преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом.
- Дешифрование - обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный
- Ключ - информация, необходимая для беспрепятственного шифрования и дешифрования текстов

Требования к криптосисемам:

- зашифрованное сообщение должно поддаваться чтению только при наличии ключа;
- число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;
- число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей, должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычис-лений);
- знание алгоритма шифрования не должно влиять на надежность защиты;
- незначительное изменение ключа должно при водить к существенному изменению вида зашифрованного сообщения даже при использовании

одного и того же ключа;

- структурные элементы алгоритма шифрования должны быть неизменными;
- дополнительные биты, вводимые в сообщение в процесс е шифрования, должен быть полностью и надежно скрыты в шифрованном тексте;
- длина шифрованного текста должна быть равной длине исходного текста;
- не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования;
- любой ключ из множества возможных должен обеспечивать надежную защиту информации;
- алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования

2.3 Разделы криптографии

- **Симметричные криптосистемы** использует один и тот же ключ и для шифрования, и для расшифровывания. Алгоритм и ключ выбирается заранее и известен обеим сторонам. Сохранение ключа в секретности является важной задачей для установления и поддержки защищённого канала связи
- **Асимметричные криптосистемы** использует два разных ключа: один для шифрования (который также называется открытым), другой для расшифровывания (называется закрытым). Данные ключи связанны друг с другом определенным математическим образом
- **Системы электронной подписи** - это присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении

текста другим пользователем проверить авторство и подлинность сообщения

- **Системы управления ключами** - это информационные системы, целью которых является составление и распределение ключей между пользователями информационной системы