студентов специальности 1 – 96 01 01 «Таможенное дело» – Мн.: БНТУ, 2008. С. 27-30.

УДК 003.26

КРИПТОГРАФИЯ КАК НАУКА. ТИПЫ КРИПТОСИСТЕМ

Пантюк И.Д., Редковская Д.А.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

Без использования криптографии преодоление таких проблемных задач информационной безопасности, как конфиденциальность и целостность, аутентификация и неотказуемость, было бы на сегодняшний день немыслимо. [1]

Криптография – это дисциплина, которая занимается вариантами предоставления конфиденциальности, единообразия, аутентификации и шифрования информации. Исконно криптография трудилась над алгоритмами шифрования данных. Она обратимо преобразует открытый текст в шифротекст на основе тайного кода, либо же ключа. Классическая криптография является фрагментом неизменяемой криптосистемы, в которой шифрование и дешифрование проделываются с помощью одного и того же секретного ключа. Шифрование снабжают те, кто осуществляет подобные операции, например, банки и социальные сети. Другими словами, это функция кибербезопасности в сфере цифровых транзакций. Сегодня данные настолько ценны, что кибербезопасность сравнима с человеческой жизнью. В важных аспектах они сопряжены косвенно.

Дабы сделать зашифрованную информацию криптографически защищённой, криптосистемы могут неоднократно пользоваться примитивами, которые являются условно простыми преобразованиями. В качестве примитивов могут использоваться замены, перестановки, циклические шаги, гаммы и т. д. [2]

Фундаментальной доступной криптографической технологией является шифрование, которое кодирует информацию таким образом, что её невозможно дешифровать без подходящего ключа. Криптография – это форма шифрования, при которой код знают исключительно отправитель и адресат информации, в этом случае передаваемые данные остаются набором символов для остальных, которые невозможно перевести на другие языки.

В цифровых технологиях криптография важна как для защиты конфиденциальных данных, так и в качестве инструмента ради борьбы с

пиратством и распространением информации об интеллектуальной собственности.

Основные типы криптографии:

• *шифры транспозиции*, где перестановка символов шифруемого текста осуществляется в соответствии с определённым правилом;

• *шифры замены*, когда символы шифруемого текста сменяются символами такого же или иного алфавита по определённой схеме;

• *гамма-шифры*, где символы шифруемого текста комбинируются с символами в случайной последовательности, называемой гаммой;

• *шифры, базирующиеся на аналитических преобразованиях*, в которых документ, подлежащий шифрованию модифицируется в соответствии с определённым аналитическим правилом, математической формулой.

В зависимости от характера шифрования общераспространённые криптосистемы разделяются на два типа: *симметричные*, шифрование скрытым ключом и *асимметричные* шифрование открытым ключом.

1. Симметричные криптосистемы применяют один и тот же секретный ключ как для шифрования так и для дешифрования блоков данных.

В симметричных криптосистемах, либо как их ещё называют, в криптосистемах с секретным ключом, информация шифруется и расшифровывается с помощью одного ключа – секретного ключа. Расшифровка ключа шифрования приводит к рассекречиванию всех оберегаемых сообщений. До изобретения асимметричных систем шифрования были исключительно симметричные системы шифрования. Ключ алгоритма обязан держаться в секрете двумя сторонами, то есть отправителем и получателем, и выбираться ими до начала коммуникации. [3]

2. Асимметричные схемы шифрования применяют два разных ключа, открытый и закрытый, в блоке шифрования и блоке дешифрования.

Асимметричные криптосистемы ещё известны как криптосистемы с открытым ключом. В этих системах с открытым ключом используются два математически объединённых ключа – открытый ключ и закрытый ключ. Данные шифруются с помощью открытого ключа, который является общедоступным, и расшифровывается с поддержкой закрытого ключа, который известен исключительно получателю сообщения. [4]

В случае симметричных криптосистем шифратор отправителя и дешифратор получателя используют один ключ, который находится в секрете и передаётся от отправителя к получателю по каналу, свободному от наружного вмешательства. В асимметричных системах ключ шифрования хранится в точке генерации, а открытый ключ передаётся по открытому каналу.

Необходимость в сертификации криптографических алгоритмов и многофункциональной сопоставимости между различными пользователями привела к созданию криптографических стандартов.

Литература

1. Основы криптографии / А. П. Алферов [и др.]. – М: Гелиос АРВ, 2022. – С. 3.

2. Прохорова, О.В. Информационная безопасность и защита информации: учебник / О.В. Прохорова. – Самара: СГАСУ, 2014.– С. 40.

3. Краснова, А. К. Криптография как наука. Типы криптосистем / А. К. Краснова ; науч. рук. И. А. Ковалькова // НИРС-76 [Электронный ресурс] : материалы научно-практической конференции студентов и курсантов, Минск, 23 апреля 2020 г. / Белорусский национальный технический университет ; редкол.: Е. С. Голубцова (отв. ред.), О. В. Веремейчик, Г. М. Бровка. – Минск : БНТУ, 2020. – С.38.

4. Ковалькова, И.А. Криптографические методы обеспечения информационной безопасности. / Наука – образованию, производству, экономике. Материалы 10-ой международной научно-технической конференции в 4-х томах. Том 4. Минск, БНТУ, 2012 г.

ВЛИЯНИЕ КОМПЬЮТЕРНЫХ СЕТЕЙ НА ЧЕЛОВЕКА

Перевозникова Д. Д., Гайдученко А. А.
Научный руководитель: ст. преподаватель Галай Т. А.
Белорусский национальный технический университет

Компьютерные сети в наше время активно развиваются, но многие из них основаны на излучении электромагнитной энергии. Это уже привело к ухудшению состояния электромагнитного поля нашей Земли. Неоспоримым так же является тот факт, что человек практически в каждый момент своей жизни находится под влиянием электромагнитного поля.

Первое, что нужно определить – что же такое компьютерные сети. Самой подходящей формулировкой является: совокупность технических средств, способных передавать информацию из одной точки в другую, которые объединяются общими сетевыми ресурсами. Существует несколько разновидностей компьютерных сетей, таких как локальные сети (LAN), глобальные сети (WAN), городские сети (MAN) и т.д. Каждый тип сети имеет свои особенности и сферу применения. В современном мире компьютеры присутствуют на любом, даже самом маленьком предприятии. Как показывает практика, чем крупнее организация, тем большей компьютерной системы требуется для ее правильного функционирования.

Возвращаясь, к проблеме, можно сказать, что она достаточно актуальна. Так как количество людей, использующих компьютерные технологии,