Золотарева И.В, к.э.н., доцент кафедры «Экономическая безопасность, учет и право» ДГТУ, Ростов-на-Дону, Россия;

Городинская И.Ю., студент 5 курса кафедры «Экономическая безопасность, учет и право» ДГТУ, Ростов-на-Дону, Россия;

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация. В статье рассматриваются методы криптографической защиты информации. Методы криптографической защиты информации − это специальные методы шифрования, кодирования или иного преобразования информации, которые делают ее содержимое недоступным без представления ключа криптограммы и обратного преобразования. Криптографическая защита, несомненно, является наиболее надежным методом защиты, поскольку сама информация защищена напрямую и к ней нет доступа.

Ключевые слова: криптография; шифрование; сжатие; кодирование; стенография; защита информации.

Zolotareva I. V., PhD, Associate Professor of the Department of "Economic Security, Accounting and Law", DSTU, Rostov-on-Don, Russia;

Gorodinskaya I. Yu.,5 year student of the Department of economic security, accounting and law of the DSTU, Rostov-on-Don, Russia;

CRYPTOGRAPHIC METHODS OF INFORMATION PROTECTION

Annotation. The article discusses the methods of cryptographic protection of information. Methods of cryptographic protection of information are special methods of encryption, encoding or other transformation of information that make its contents inaccessible without presenting the cryptogram key and reverse transformation. Cryptographic protection is undoubtedly the most reliable method

of protection, since the information itself is protected directly and there is no access to it.

Keywords: cryptography; encryption; compression; encoding; shorthand; information protection.

Сегодня самым надежным методом шифрования для передачи информационных данных на большие расстояния является именно криптографическая защита информации.

Криптография— это наука, изучающая и описывающая модели информационной безопасности. Она позволяет решить многие проблемы, связанные с информационной безопасностью сети:

1) конфиденциальность;
2) аутентификацию;
3) контроль;
4) целостность взаимодействующих участников.

Основная цель криптографической защиты информации − гарантировать конфиденциальность и защиту данных информации компьютерных сетей в процессе передачи по сети между пользователями системы.

Защита конфиденциальной информации, основанная на криптографической защите, шифрует информационные данные с помощью обратимых преобразований, каждое из которых описывается ключом и порядком, которые определяют порядок его применения.

Важным элементом криптографической защиты информации является ключ, отвечающий за выбор преобразования и последовательность его выполнения.

Классификация криптографических методов преобразования информации по типу воздействия на выходные данные включает следующие виды (рисунок 1.1):

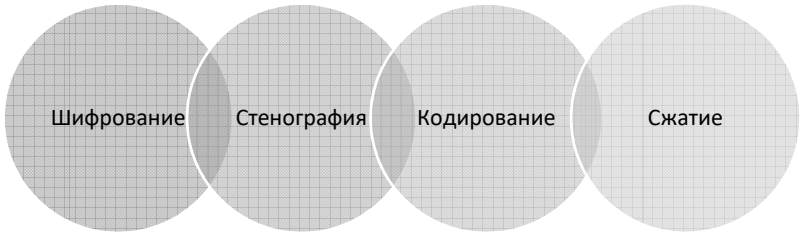

Рисунок 1.1 – Классификация методов криптографического преобразования информации

Шифрование

Шифрование включает изменение исходного кода с помощью логических, математических, комбинаторных и других операций. В результате таких преобразований выходные данные принимают форму хаотически расположенных символов (чисел, букв и т. д.) и кодов двоичной системы.

Инструментами создания шифра служат ключ и алгоритм преобразования.

Шифрование − это основной криптографический метод изменения данных на компьютерах. Чтобы иметь возможность эффективно бороться с крипто − атаками (атаки на шифры, криптоанализ), методы шифрования должны соответствовать ряду требований (рисунок 1.2):

Рисунок 1.2 – Требования методов шифрования

Эффективность шифрования определяется криптографической стойкостью шифра. Единицей измерения этого показателя может быть:

время; стоимость инструментов, необходимых криптоаналитику для расшифровки без знания ключа.

На рисунке 1.3 изображен механизм работы простейшей криптосистемы:

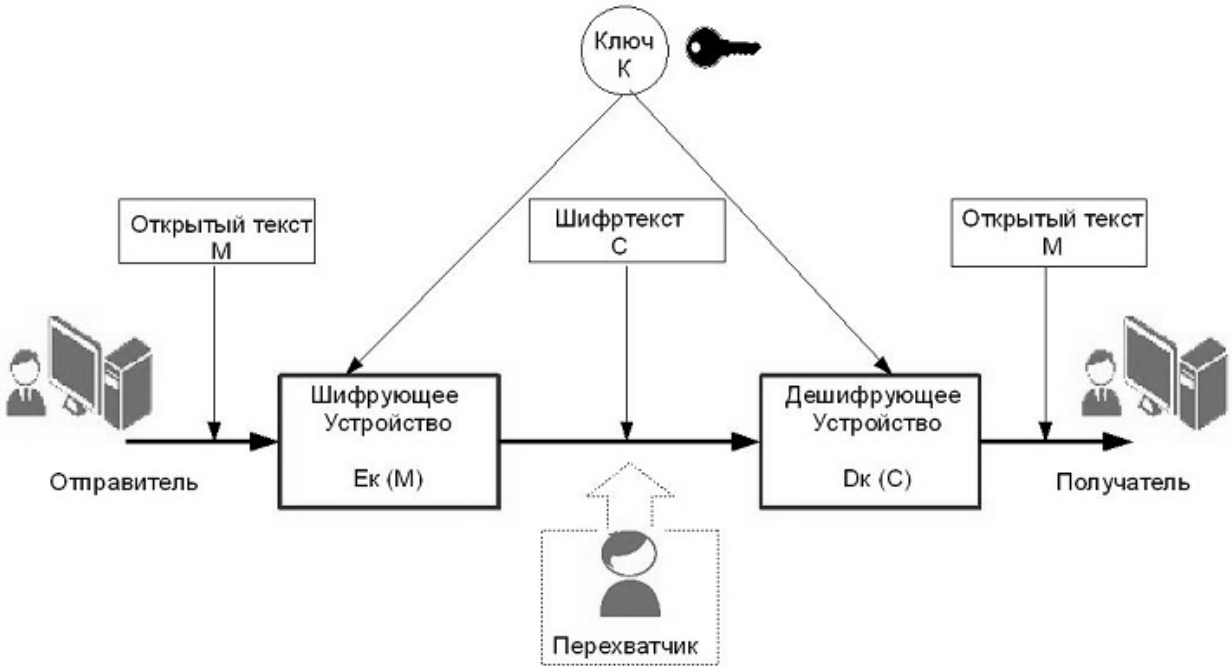

Рисунок 1.3 – Механизм работы криптосистемы

В этой модели отправитель создает сообщение с открытым исходным кодом (M), которое передается законному адресату по незащищенному каналу. Канал находится под контролем злоумышленника, который пытается перехватить и выпустить сообщение. Чтобы не дать перехватчику расшифровать переданные данные, отправитель защищает их с помощью обратимого преобразования (Ek (C)), а затем получает зашифрованный текст (C). Он отправляет его получателю. Адресат получает зашифрованный текст, раскрывает секретное сообщение с помощью дешифратора (Dk (C)) и получает исходный текст (M).

Ек — один из алгоритмов преобразования, К — это критпографический ключ, который определяет выбор алгоритма, подходящего для конкретного шифрования.

Стенография

Этот метод, единственный среди криптографических методов, позволяет скрыть не только информацию, но и сам факт их хранения и передачи. Сокращение основано на маскировании конфиденциальных данных между общедоступными файлами. Другими словами, закрытая информация скрывается, а вместо нее создаются дубликаты.

Кодирование

Преобразование данных с использованием этой техники основано на принципе замены слов и фраз исходного кода кодами. Закодированные данные могут отображаться в виде буквенных, цифровых или буквенно-цифровых комбинаций. Для кодирования и декодирования используются словари или специальные таблицы.

Рассмотренный метод подходит для использования в системах с небольшим набором семантических структур. Обратной стороной кодирования является то, что вам необходимо хранить и распространять кодовую книгу, а также часто менять ее, чтобы избежать нежелательного рассекречивания информации.

Сжатие

Этот метод − сокращение объема исходной информации. Концепция сжатия классифицируется как криптографическая с некоторыми оговорками. С одной стороны, сжатые данные требуют обратного преобразования, чтобы их можно было прочитать. С другой стороны, широко доступны инструменты сжатия и обратного преобразования, поэтому этот метод ненадежен с точки зрения информационной безопасности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Криптографическая защита информации : учебное пособие / А. В. Яковлев, А. А. Безбогов, В. В. Родин, В. Н. Шамкин; ТГТУ, 2020, 140 с.
2. Криптографические методы защиты информации : учебник и практикум для академического бакалавриата / И. Н. Васильева. — Москва : Издательство Юрайт, 2016. — 349 с.
3. Цифровая стеганография / ГрибунинВадим Геннадьевич М.:Солон-Пресс, 2016. - 589 с.
4. Криптографическая защита информации. Богомолов С.А. Библиотечка студента. От простого к сложному. Персональный компьютер. – Москва, 2015 – 24 с.

References:

1. Cryptographic protection of information : textbook / A.V. Yakovlev, A. A. Bebog, V. V. Rodin, V. N. Shamkin; TSTU, 2020, 140 p.
2. Cryptographic methods of information protection : textbook and workshop for academic undergraduate / I. N. Vasilyeva. - Moscow : Yurayt Publishing House, 2016. - 349 p.
3. Digital steganography / GribuninVadim Gennadievich M.:Solon-Press, 2016. - 589 p.
4. Cryptographic protection of information. Bogomolov S.A. Student's library. From simple to complex. Personal computer. - Moscow, 2015 - 24 p.