УДК 004.056

Сальникова А.А.

студент

5 курс, факультет «Информатика и управление»

КФ МГТУ им. Н.Э. Баумана

Россия, г. Калуга

ОРГАНИЗАЦИЯ ЗАЩИЩЕННОГО ОБМЕНА ИНФОРМАЦИЕЙ

Аннотация:

В данной статье рассмотрены различные подходы к организации защищенного обмена информацией. Представлен анализ способов защиты информации при передаче по электронной почте, в мессенджерах и с помощью физических носителей. Даны рекомендации для повышения защищенности данных от несанкционированного доступа.

Ключевые слова: защита информации, информационная безопасность, коммерческая тайна, безопасный обмен данными.

Salnikova A.A.

student

5 year, faculty "Computer Science and Management"

Bauman MSTU KF

Russia, Kaluga

ORGANIZATION OF PROTECTED EXCHANGE OF MESSAGES

Annotation:

This article discusses various approaches to organizing a secure exchange of information. The analysis of information protection methods during transmission by e-mail, in messengers and using physical media is presented. Recommendations are given to increase data security from unauthorized access.

Keywords: information protection, information security, trade secret, secure data exchange.

Введение. Информационная безопасность предполагает обеспечение защиты данных от хищений или изменений как случайного, так и умышленного характера. Защита информации включает полный комплекс мер по обеспечению целостности и конфиденциальности информации при условии ее доступности для пользователей, имеющих соответствующие права. Особую роль играет эффективная организация безопасного обмена информацией. Каждый способ передачи информации обладает своей спецификой, от которой зависят и применяемые средства защиты передачи данных. Для передачи информации используют электронную почту, мессенджеры и съемные электронные носители [1].

Защита информации передаваемой электронной почтой. Электронная почта – популярный способ для своевременной передачи информации и ведения переговоров. Комплексная защита информации подразумевает обеспечение беспрепятственного получения писем адресатом, без возможности их вскрытия, перехвата, прочтения, распространения и включает:

- Защита от спама. Она осуществляется методом фильтрации конкретных отправителей и методом сортировки сообщений, в результате которого пользователю выдаются только касающиеся заданной тематики.
- Защита от фальшивых адресов. Осуществляется шифрованием с открытыми ключами. Однонаправленная хэш-функция письма шифруется секретным ключом отправителя. Наиболее распространены следующие алгоритмы: SHA, RSA, RC2 и другие. Получатель использует открытый ключ отправителя для расшифровки хэш-функции и сравнивает его с хэш-функцией, рассчитанной по полученному сообщению. Если значения совпадают, то сообщение принадлежит отправителю и не было изменено в пути.

- Защита от перехвата. Осуществляется шифрованием содержимого сообщения или канала, по которому оно передается. При получении несанкционированного доступа к зашифрованному каналу, высока вероятность прочтения или изменения всех сообщений проходящих по нему. Поэтому необходимо инкапсулировать содержимое каждого письма, защитив его от несанкционированного доступа. Наиболее часто используют симметричное шифрование с передачей ключа по второму каналу связи. Например, алгоритм шифрования AES-256 является на сегодняшний день достаточно надежным. Необходимо учитывать, что уровень сложности пароля должен быть не менее 10 символов с использованием латинского алфавита в нижнем и верхнем регистрах, чисел и знаков. Далее пароль от зашифрованного архива передается иным каналом связи адресату. Например, по телефону или смс.

Для увеличения степени защиты используется электронная цифровая подпись (ЭЦП), которая уникальна для каждого документа. В ее основе лежит алгоритм асимметричного шифрования. Данный способ обеспечивает защиту передаваемых данных на высоком уровне.

Распространением сертификатов открытых ключей, участвующих в электронном документообороте, занимается Центр удостоверения открытых ключей. Для генерации электронной подписи и работы с сертификатами используются различные средства криптографической защиты (СКЗИ). Например, КриптоПро и ViPNet CSP [2].

Защита информации в мессенджерах. Популярным способом обмена сообщениями являются мессенджеры, которые предоставляют обмен информацией в режиме реального времени через Интернет: звуковые сигналы, текстовые сообщения, изображения, видео. Для обеспечения безопасного обмена данными в мессенджерах используется сквозное шифрование или end-to-end encryption (E2EE), при котором

ключи шифрования хранятся только на пользовательских устройствах и не отправляются на сервер. Также необходимо учитывать использование надежного протокола шифрования.

Данные сервисы ориентированы на интенсивную онлайновую переписку в виде цепочки коротких сообщений, которые должны отображаться в строго определенном порядке. Для того чтобы не нарушить структуру, предусмотрена прямая и обратная секретность. Она делает невозможным прочтение отправленных ранее и написанных в будущем сообщений, зная только текущий ключ шифрования. Для этого используется многослойное шифрование с переходом от асимметричной к симметричной криптографии и дополнительные ключи с разным временем жизни [3].

Защита информации на внешних носителях. Для хранения и переноса информации с одного компьютера на другие используют внешние носители. К ним относятся магнитные (HDD, HMDD), оптические (CD-ROM, DVD-ROM, Blu-Ray Disc), полупроводниковые (флеш-память, дискеты) и др. Для обеспечения безопасности переносимых данных от НСД существуют следующие способы защиты: шифрование, биометрические системы защиты, двухфакторная аутентификация, защита паролем, физическая защита. Существуют два метода шифрования, позволяющие надежно защитить данные.

Либо шифруется файл (файлы) с использованием одной из многочисленных систем шифрования (GnuPG, TrueCrypt, PGP и т. д.), либо создаётся архив, защищённый паролем. К биометрическим системам защиты информации относятся системы идентификации: по отпечаткам пальцев; по характеристикам речи; по радужной оболочке глаза; по изображению лица; по геометрии ладони руки. Также используются технологии, повышающие стойкость к физическим воздействиям:

повышение ударопрочности накопителей данных (шоковая защита), защита от влаги, экстремальных температур и др. Использование защиты с помощью организации двухфакторной аутентификации пользователя. Необходимо предоставить пароль и цифровой проверочный код [4].

Выводы.

Таким образом, передача данных по электронной почте, через сервисы файлового обмена или с использованием внешних носителей может быть небезопасной. Защита передаваемой информации обеспечивается различными методами и подходами исходя из требуемого уровня безопасности. Наилучшую защиту информации может обеспечить только применение комплексных мер для обеспечения информационной безопасности.

Использованные источники:

1. Информационная безопасность / [Электронный ресурс]. Режим доступа: https://center-yf.ru/data/stat/informacionnaya-bezopasnost.php (дата обращения: 05.10.2019).

2. Защита информации / [Электронный ресурс]. Режим доступа: https://vuzlit.ru/496459/zaschita_informatsii (дата обращения: 15.09.2019).

3. Внукова З.А. Оценка безопасности систем мгновенного обмена сообщениями методом анализа иерархий // Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. 2016. №. 23.

4. Защищенные носители информации / [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki (дата обращения: 11.08.2019).