Давлетов И.Ш.

Обзор и сравнение методов шифрования данных на съёмных носителях информации

Аннотация. Данная статья посвящена исследованию методов шифрования данных на съемных носителях и анализу возможности их применения для безопасного хранения и обмена конфиденциальной информацией. Описания программных и аппаратных средств в данной статье не имеют рекламного характера, а предназначены исключительно для ознакомительных и научных целей.

***Ключевые слова*:** шифрование данных, защита информации, криптография, Flash память.

Введение

В настоящее время большую популярность приобретают USB-устройства флэш-памяти, являющиеся самыми распространенными и удобными запоминающими устройствами, используемые в качестве хранения различного типа данных. Параллельно с этим развиваются средства защиты, специализированные для данных устройств. Наиболее популярным методом защиты информации является шифрование данных с помощью криптографических алгоритмов.

Основная часть

Криптографическая защита данных на носителях информации необходима для предотвращения угроз хищения конфиденциальной информации при хранении и транспортировки данных.

Общая схема применения шифрования данных на съемных носителях показана на рис.1.

На 1 шаге данной схемы происходит передача электронного ключа шифрования (секретного пароля) по закрытому каналу связи от пункта А в пункт В.

На 2 шаге, с помощью ключа и криптографического алгоритма выполняется шифрование информации на USB-устройстве флэш-памяти в пункте А, передача носителя в пункт В и расшифрование информации с помощью ключа, полученного ранее.

На 3 шаге происходит обратный процесс, т.е. съемный носитель с зашифрованными данными передается от пункта В пункт А.

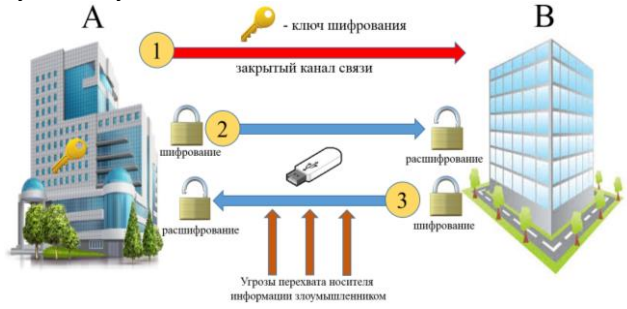

Рис. 1. Схема применения шифрования данных на USB-устройстве флэш-памяти.

Существуют несколько способов защиты данных на съемных носителях информации.

1. Шифрование данных средствами операционной системы.
2. Шифрование данных сторонними программными средствами.
3. Аппаратное шифрование данных с помощью специального модуля, встроенного в съемный носитель.
4. Шифрование данных на USB-устройствах флэш-памяти с помощью отдельных аппаратно-программных средств.

Шифрование данных средствами операционной системы

При исследовании данного способа, были рассмотрены стандартные встроенные средства шифрования данных операционной системы Windows. На сегодняшний день данная операционная система имеет 2 встроенных инструмента защиты данных: EFS (начиная с Windows 2000 и выше [3]) и BitLocker (начиная с Windows 7 и выше).

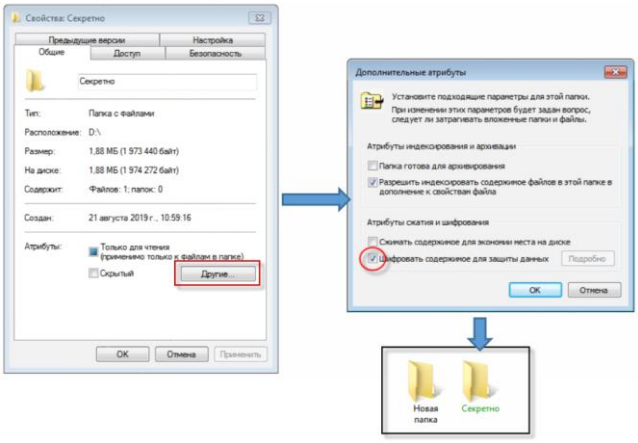

Рис. 2. Порядок шифрования данных с помощью EFS.

EFS (Encrypting File System) - система шифрования данных, реализующая шифрование на уровне файлов в операционных системах Microsoft Windows [1]. Файловая система EFS используется для защиты отдельных файлов на любом диске на уровне пользователя. На рис.2 изображен порядок шифрования данных с помощью EFS.

BitLocker—технология шифрования носителей информации, являющаяся частью операционных систем семейства Microsoft Windows. С помощью BitLocker можно шифровать все файлы на несъемных и съемных носителях. На рис.3 показан порядок использования технологии.

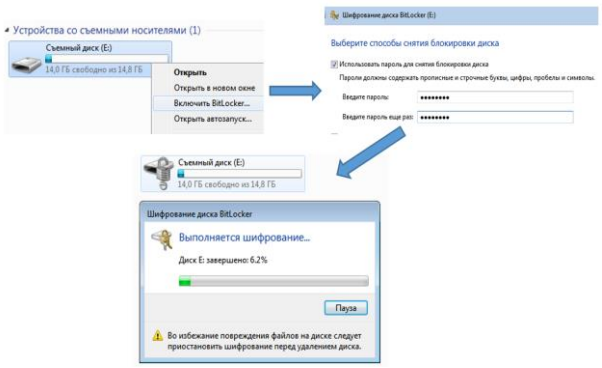

Рис.3. Порядок шифрования данных с помощью BitLocker.

Основные отличия средств шифрования данных EFS от BitLocker представлены в Таблице 1.

Таблица 1.

Отличия EFS от BitLocker

EFS	BitLocker
EFS по отдельности шифрует личные файлы и папки и не шифрует все содержимое диска.	BitLocker выполняет шифрование всех личных и системных файлов на диске с ОС, несъемных и съемных носителях.
EFS шифрует файлы на основе сопоставленной им учетной записи пользователя. При наличии на компьютере нескольких пользователей или групп они могут шифровать собственные файлы независимо друг от друга.	BitLocker не зависит от отдельных учетных записей пользователей, связанных с файлами. BitLocker либо включен, либо отключен, и это применяется для всех пользователей и групп.
EFS не требует и не использует дополнительное оборудование.	BitLocker использует доверенный платформенный модуль - особую микросхему, присутствующую во многих компьютерах, поддерживающую дополнительные функции безопасности для шифрования диска с ОС.
Для использования EFS прав администратора не требуется.	Для включения или отключения шифрования BitLocker на диске с установленной ОС Windows и на съемных дисках необходимо иметь права администратора.

Шифрование данных сторонними программными средствами.

В настоящее время существуют множество программных средств криптографической защиты информации, позволяющие защитить файлы как на жестком диске, так и на съемных носителях.

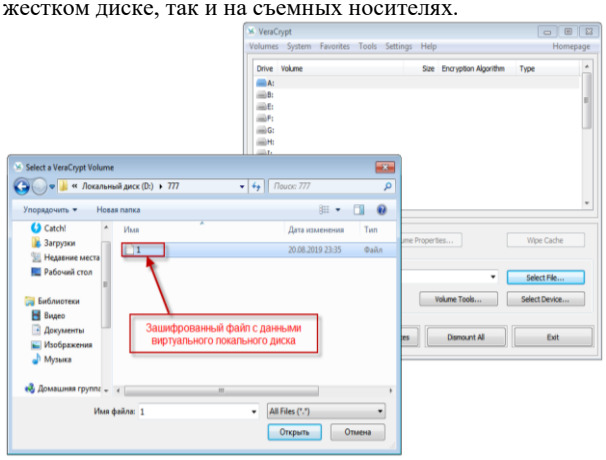

Рис.4. Выбор зашифрованного файла с данными виртуального логического диска.

В данной статье будут рассмотренны самые популярные из них. VeraCrypt (аналог TrueCrypt) — это программное обеспечение, позволяющее создавать виртуальный зашифрованный логический диск, хранящийся в файловой системе как зашифрованный файл (рис.4), который можно хранить на жестком диске, записать на съемный носитель или передать по сети [4]. Перед созданием зашифрованного файла виртуального локального диска имеется возвожность выбора алгоритма шифрования (рис.5).

Монтирование виртуального логического диска производится после успешного ввода пароля (рис.6), который был установлен во время создания зашифрованного файла.

Особенность данной программы является возможность шифрования данных “на лету”, т.е. работа с монтированным виртуальным логическим диском производится точно также как с обычным логическим диском (рис.7) и процесс шифрования будет незаметен для пользователя, имеющего секретный пароль. В данном программном обеспечении также имеется возможность полного шифрования USB flash носителя информации.

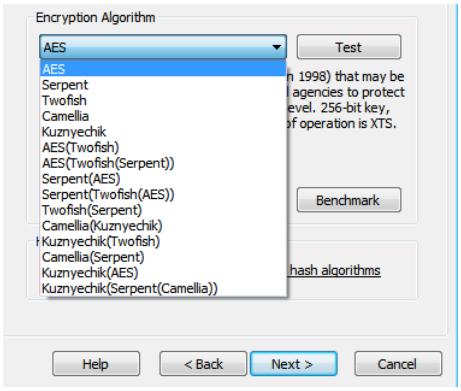

Рис.5. Список алгоритмов шифрования, поддерживаемых программным обеспечением VeraCrypt.

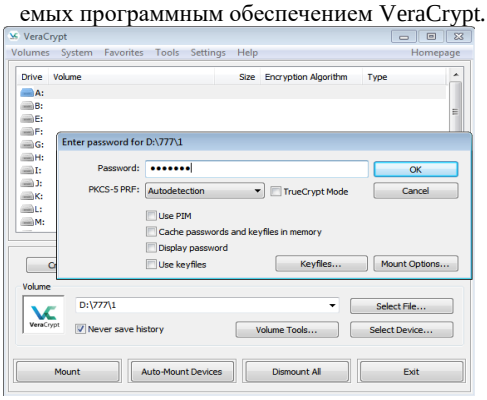

Рис.6. Ввод пароля для монтирования виртуального логического диска.

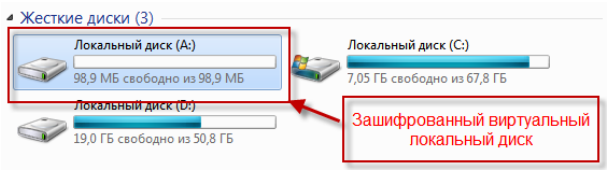

Рис.7. Смонтированный в систему зашифрованный виртуальный локальный диск

Современные архиваторы файлов также имеют возможность шифрования данных с установкой пароля. Например, в архиваторе WinRar доступна функция шифрования архива с использованием алгоритма AES (Advanced Encryption Standard (AES), также известный как Rijndael - симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США [5].) с длиной ключа 256 бит. Расшифрование происходит путём

ввода секретного пароля, установленного при шифровании [6].

Шифрование данных сторонними программными средствами в большинстве случаев требует установки пользовательского пароля, на основе которого генерируется криптографический ключ. В настоящее время парольная защита является наиболее распространенной, прежде всего, благодаря своему единственному достоинству – простоте использования.

Однако, парольная аутентификация имеет множество недостатков. В отличие от случайно формируемых криптографических ключей, пароли, установленные пользователем возможно подобрать из-за достаточно небрежного отношения большинства пользователей к формированию пароля.

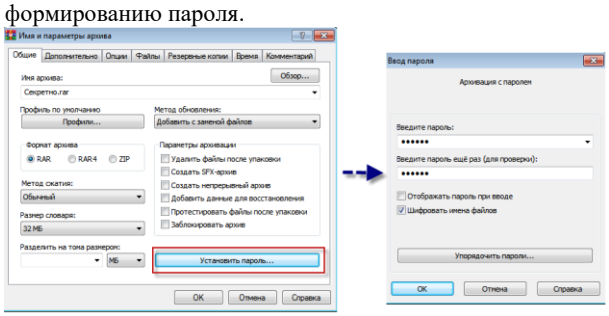

Рис.8. Процесс установки пароля для защиты данных и шифрования при архивировании в программном обеспечении WinRar

Часто встречаются случаи выбора пользователями легко предугадываемых паролей. Кроме этого при вводе пароля появляется угроза его перехвата с помощью так называемых кейлоггеров (Кейло́ггер (англ. keylogger, key — клавиша и logger — регистрирующее устройство) — программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя — нажатия клавиш на клавиатуре компьютера, движения и нажатия клавиш мыши и т. д. [7]).

Аппаратное шифрование данных с помощью специального модуля, встроенного в съемный носитель. На сегодняшний день существуют съёмные носители со встроенными модулями шифрования. В данных устройствах пароль (криптографический ключ) вводится с помощью встроенного интерфейса. Стоить отметить, что в некоторых подобных устройствах имеются несколько профилей ограничения доступа: только чтение, чтение и запись, доступ к определенному разделу памяти, режим администратора и т.п. Одним из представителей USB флеш-памяти со встроенным аппаратным шифрованием является устройство datAshur Pro фирмы iStorage (рис.9). Данное устройство способно шифровать данные по криптографическому стандарту AES с длиной ключа 256 бит. Поддерживается совместимость с операционными системами Windows, Mac, Linux, Android и iOS [8].

Рис.9. Защищенный флэш-накопитель iStorage datAshur Pro

Из достоинств можно выделить удобство в использовании, отсутствие потребности установки дополнительного программного обеспечения, поддержку защиты от перебора паролей. Из недостатков стоит отметить довольно высокую стоимость данного устройства.

Шифрование данных на USB-устройствах флэш-памяти с помощью отдельных аппаратно-программных средств. Данный метод организации защиты информации на USB флеш-памяти применяется без использования персонального компьютера, т.е. шифрование происходит с помощью отдельного аппаратно-программного устройства, в большинстве случаев выполненного на базе микрокомпьютеров или микропроцессорных технологий, с помощью которых можно реализовать несколько способов использования аппаратуры шифрования (рис.10).

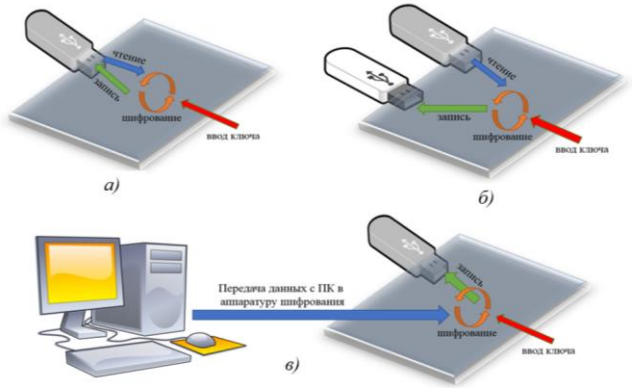

Рис.10. Способы использования аппаратуры шифрования данных на USB флэш-памяти.

Шифрование данных на съемном носителе информации непосредственно на самом носителе, т.е. вместо открытых (незащищенных) данных, на эти же области памяти, после считывания и криптографического преобразования, записываются зашифрованные данные (рис.10, а).

1. Считывание незащищенных данных с одного съемного носителя, криптографическое преобразование и запись зашифрованной информации в другой носитель (рис.10, б).

2. Передача незащищенной информации с персонального компьютера аппаратуре шифрования, выполнение криптографического преобразования и запись зашифрованной информации на съёмный носитель (рис.10, в).

Отдельные аппаратно-программные средства шифрования имеют следующие достоинства:

возможность внедрения разнообразных технологий ввода криптографического ключа, которые, по сравнению с парольной защитой, увеличивают стойкость ключа к перебору;

при разработке своих аппаратно-программных средств, появляется возможность внедрения любых криптографических алгоритмов шифрования;

автономность работы, т.е. независимость процесса шифрования от персонального компьютера.

Недостатками являются сложность и стоимость разработки подобных устройств.

Заключение. Выполненное исследование в данной статье показало, что самым надежным способом шифрования данных на съемных носителях является использование своих аппаратно-программных разработок при правильном использовании криптографических алгоритмов. Это утверждение обоснованно тем, что имеется потенциальная Back-Door (Бэкдор, backdoor (от англ. back door — «чёрный ход», буквально «задняя дверь») — дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным. Основной целью бэкдора является скрытное и быстрое по-

лучение доступа к данным, в большинстве случаев — к защищённым. Например, бэкдор может быть встроен в алгоритм шифрования. [9]) угроза со стороны производителей программных и аппаратных средств шифрования данных, т.е. производитель может намеренно внедрить специальный код в программном обеспечении, который приведет к появлению уязвимостей в алгоритме шифрования и позволит получить несанкционированный доступ к данным.

Использованная литература

1. Шифрованная файловая система – Википедия [электронный ресурс]: https://ru.wikipedia.org/wiki/Шифрованная_файловая_система
2. BitLocker — Википедия [электронный ресурс]: https://ru.wikipedia.org/wiki/BitLocker
3. В.Ю. Мельников. Исследование методов защиты операционных систем и данных. Учебное пособие. Москва: МГТУ имени Н.Э. Баумана. 2017. – 100 с.
4. VeraCrypt User's Guide. Version 1.0e. Инструкция. 2017. – 151 с.
5. Advanced Encryption Standard — Википедия [электронный ресурс]: https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard
6. Кейлогер — Википедия [электронный ресурс]: https://ru.wikipedia.org/wiki/Кейлогер
7. Архиватор WinRAR, инструкции [электронный ресурс]: http://winrar-full.com/kak-postavit-parol-na-arhiv.html
8. Secure USB flash drive datAshur Pro 3.0. Инструкция. 2017. – 15 с.
9. Бэкдор — Википедия [электронный ресурс]: https://ru.wikipedia.org/wiki/ Бэкдор

Давлетов Ислам Шухратович – научный сотрудник научно-исследовательской лаборатории Военного института информационно-коммуникационных технологий и связи.

Davletov I. Sh.

Overview and comparison of data encryption methods on removable information media

Annotation. This article is devoted to the study of data encryption methods on removable media and the analysis of the possibility of their use for the secure storage and exchange of confidential information. The descriptions of software and hardware in this article are not of an advertising nature, but are intended solely for educational and scientific purposes.

Key words: data encryption, information protection, cryptography, Flash memory.