**УДК 004.056.057**

# ЗАЩИТА КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ В НОУТБУКАХ

***Борзило В.В., студентка 4 курса экономического факультета***
***Научный руководитель – Голубев С.В., к.э.н., доцент***
***ФГБОУ ВО Ульяновский гАУ***

***Ключевые слова:*** *конфиденциальная информация, несанкционированный доступ, защита данных, шифрование, криптоконтейнер.*

*В данной работе рассмотрим защиту конфиденциальной информации от несанкционированного доступа в ноутбуках. Для того чтобы защитить информацию от несанкционированного доступа, применяются технологии шифрования. Однако у пользователей, не обладающих надлежащими знаниями о методах шифрования, может возникнуть ложное ощущение, будто все чувствительные данные надежно защищены, так же изучим основные технологии шифрования данных.*

Проблема защиты конфиденциальной информации от несанкционированного доступа является одной из самых злободневных и часто встречаемых в нашем современном мире. В этой статье рассмотрены технологии, надежно защищающие чувствительные данные на ноутбуках с помощью шифрования и многофакторной аутентификации. Как показывает практика, это самый надежный, и единственный способ, позволяющий обеспечить безопасность информации и одновременно удобство доступа к ней.

Одной из самых опасных и основных угроз на сегодняшний день является несанкционированный доступ к информации. Проблема усиливается тем, что за неавторизованным доступом к конфиденциальной информации часто следует проникновение и ее кража. В результате такой комбинации двух чрезвычайно опасных угроз убытки разных деятельности компании могут возрасти в несколько раз (в зависимости от ценности похищенных данных). Таким образом, помимо защиты конфиденциальной информации от несанкционированного доступа необходимо оберегать и сам физический носитель.

Для того чтобы защитить информацию от несанкционированного доступа к нашим данным, применяются технологии шифрования. Од-

нако у пользователей, которые не обладают надлежащими знаниями о методах шифрования, могут возникнуть ложное ощущение, будто все чувствительные данные надежно защищены.

Общие требования к решениям по защите данных на ноутбуках.

• Обеспечение защиты конфиденциальных данных от:

– несанкционированного доступа по сети предприятия;

– несанкционированного доступа через сеть Интернет;

– несанкционированного физического доступа к оборудованию.

• Сокрытие факта наличия и расположения на ноутбуке или сервере конфиденциальных данных.

• Обеспечение защиты данных на съёмных носителях.

• Разграничение прав пользователей на доступ к защищённой информации.

• Обеспечение надёжной процедуры подтверждения прав пользователей.

• Обеспечение непрерывного доступа к защищаемым данным для легальных пользователей.

• Обеспечение простоты и удобства использования системы защиты для пользователя.

• Обеспечение централизованного управления системой защиты данных.

• Обеспечение соответствия требованиям регуляторов.

Применение средств шифрования решает задачу ограничения доступа к конфиденциальной информации - никто посторонний, получив доступ к Вашему компьютеру или серверу, не сможет прочитать закрытые данные. Для злоумышленника зашифрованный диск не отличается от любого другого неформатированного диска. Он не может ни прочесть данные, хранящиеся на нём, ни использовать их против Вас. Используемые современные алгоритмы шифрования с большой длиной ключа гарантируют надёжную защиту и стойкость к взлому даже при помощи высокопроизводительной вычислительной техники.

Основные требования к шифрованию данных:

• Стойкость защиты должна быть такой, чтобы секретность данной информации не нарушалась даже в том случае, когда злоумышленнику становится известен метод шифрования.

• Используемый алгоритм шифрования не должен иметь слабых мест, которыми могли бы воспользоваться криптоаналитики.

• Ключ шифрования должен быть недоступен для злоумышлен-

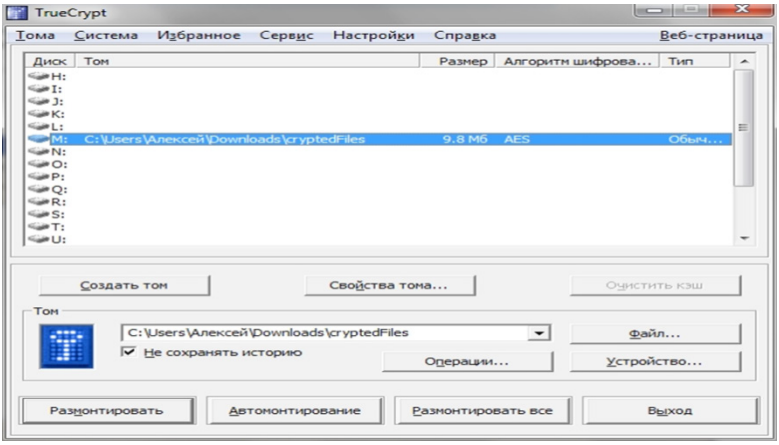


**Рисунок 1 - Криптоконтейнер**

ника. Несоблюдение принципов безопасного использования ключей шифрования может поставить под угрозу защищённость информации, даже при том, что в системе будут реализованы самые криптостойкие алгоритмы.

• Шифрование должно происходить максимально «прозрачно» для пользователя - пользователь не замечает процесса зашифрования и расшифрования данных во время работы.

• Система должна быть максимально устойчива к случайным ошибкам и неправильным действиям пользователей.

Для решения этой задачи используются криптоконтейнеры. По сути, криптоконтейнер - это отдельный файл или целый раздел на диске, содержащий в себе в зашифрованном виде некоторые документы. Таким образом, чтобы эффективно защитить данные и иную информацию, недостаточно их просто зашифровать. Необходимо позаботиться о том, чтобы копии секретной информации не «утекли» во временные и swap-файлы, а также в другие «потайные места» операционной системы, где они уязвимы для злоумышленника.

*Библиографический список*

1. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: монография / Л.Л. Ефимова, С.А. Кочерга. - М.:

ЮНИТИ-ДАНА, 2015. - 239с.
2. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин.- М.: ДМК, 2014. - 702с.

## PROTECTING SENSITIVE DATA IN LAPTOPS

***Borzilo V.V.***

***Key words:*** *confidential information ,unauthorized access, data protection, encryption, crypto container.*

*In this paper, we will consider protecting confidential information from unauthorized access in laptops.To protect information from unauthorized access, encryption technologies are used.However, users who do not have proper knowledge of encryption methods may experience a false impression that all sensitive data is securely protected, as well as learn the basic technologies of data encryption.*