УДК 004

ШИФРОВАНИЕ ДАННЫХ НА НОУТБУКАХ

Брянцева И.А., студентка 3 курса экономического факультета
Научный руководитель – Голубев С.В., к.э.н., доцент
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *защита, шифрование, модуль, ключ, информация.*

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

Шифрование обеспечивает дополнительный уровень безопасности конфиденциальных данных, защищая файлы на компьютере и передаваемую по сети информацию от посторонних пользователей, шпионов и всех, кому не разрешен доступ к информации конфиденциального характера. Чтобы данные с легкостью не оказались у третьих лиц, необходимо использовать шифрование, т.к. более эффективного способа их защиты пока не существует.

Шифрование необходимо для работы со всеми данными, чувствительными для бизнеса. Такие данные могут обрабатываться и храниться на жестких дисках, переносных устройствах, в электронных письмах, файлах, папках и в других местах. Существует ряд специфических угроз, для своевременного предотвращения которых обязательно требуется использовать шифрование.

В настоящий момент существует ряд специальных программных продуктов, выполняющих шифрование данных на мобильных устройствах и съемных носителях. Эти продукты имеют различные варианты исполнения и могут использоваться как отдельными пользователями, так и организациями в целом. Корпоративные решения позволяют централизованно управлять учетными записями, политиками доступа, ключами шифрования и обеспечивают резервирование и восстановление поврежденных данных. Реализация самого механизма шифрования,

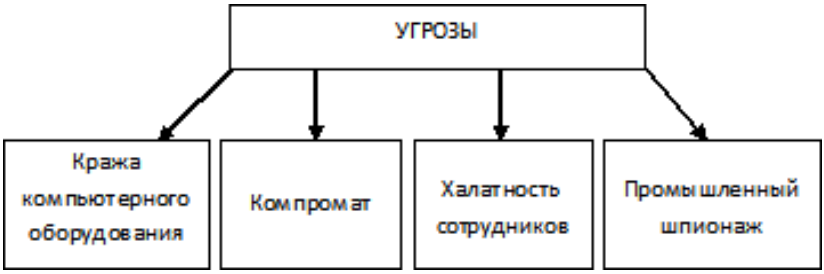

Рисунок 1 - Угрозы безопасности данных

как правило, имеет схожий принцип во всех продуктах – на мобильное устройство устанавливается специальный программный криптографический модуль, который в соответствии с заданными политиками производит шифрование части либо всего жесткого диска, в том числе зашифровываются служебные области и главная загрузочная запись (MBR). Такой вид шифрования не изменяет способ использования мобильных устройств и не оказывает влияния на работу пользователей.

Непосредственно для криптографических преобразований применяются стойкие алгоритмы симметричного шифрования с различными длинами ключей, например AES, 3DES, IDEA, Blowfish или российский ГОСТ 28147. При помощи секретного ключа зашифровываются все сектора жесткого диска, включая данные пользователей, операционную систему и служебные поля. Секретный ключ шифруется на результате хеширования пароля или сертификате пользователя и сохраняется в защищенной загрузочной области криптографического модуля. При включении устройства пользователь должен пройти процедуру аутентификации в криптомодуле. В случае успешной аутентификации модуль загружает специальный драйвер в память устройства и запускает оригинальную операционную систему. С этого момента устройство начитает работать обычным образом, как будто криптографический модуль на нем не установлен. Расшифрование секторов происходит «на лету», прозрачно для пользователя – необходимые данные последовательно обрабатываются драйвером, позволяя операционной системе загружаться и работать в штатном режиме.

Криптографический модуль является полностью независимым от остального программного обеспечения и выступает как отдельная

мини-операционная система на жестком диске устройства. Он контролирует доступ к данным при помощи специализированного драйвера, который является «посредником» между операционной системой и жестким диском. Драйвер зашифровывает каждый участок данных, записанный на диск и расшифровывает данные, считываемые с диска. Если какое-либо приложение пытается обратиться к диску и считать информацию напрямую, минуя драйвер-посредник, то оно обнаружит только зашифрованные данные, в том числе в области расположения временных файлов и в файле подкачки. Если злоумышленник при помощи специальных загрузочных утилит попытается получить доступ к диску похищенного ноутбука в обход криптомодуля, то он обнаружит только набор бит, который не содержит никакой полезной информации.

Защита коммуникаторов происходит несколько иначе – на устройство устанавливается специальное приложение, а также драйверы для аутентификации и шифрования сервисов мобильной операционной системы. Криптографический модуль позволяет предотвратить несанкционированный доступ к содержимому карт памяти, внутренней почтовой базе данных, спискам контактов и обеспечивает безопасное хранение важной информации. Данные на ноутбуке с установленным криптографическим программным обеспечением, становятся надежно защищенными от разглашения даже при хищении самого устройства.

Таким образом, эффективная защита данных подразумевает использование надежных средств шифрования и средств сильной аутентификации. Среди средств пофайлового шифрования, идеально подходящего для пересылки файлов по Интернету, стоит отметить известную программу PGP, которая может удовлетворить практически все запросы пользователя.

Библиографический список

1. Гатчин, Ю.А. Основы криптографических алгоритмов: учебное пособие / Ю.А. Гатчин, А.Г. Коробейников. - СПб.: СПбГИТМО(ТУ), 2012.
2. Коробейников, А.Г. Математические основы криптографии: учебное пособие / А.Г. Коробейников.- СПб: СПб ГИТМО (ТУ), 2013.
3. Ляшенко, И.Н. Линейное и нелинейное программирование / И.Н. Ляшенко. – К.: Высш. школа, 2008.- 369с.
4. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C / Б. Шнайер. - М.: Триумф, 2012.

ENCRYPTION OF DATA ON NOTEBOOKS

Bryantseva I.A.

Key words: *protection, encryption, module, key, information.*

The problem of protecting confidential information from unauthorized access is one of the most topical. This article discusses technologies that reliably protect sensitive data on laptops through encryption and multifactor authentication. As practice shows, this is the most reliable, and sometimes the only, way to ensure the security of information and at the same time the convenience of access to it.