УДК 621.391

С. П. ЕВСЕЕВ, канд. техн. наук, ст. науч. сотрудник, доц. кафедры ИС ХНЭУ, Харьков;
О. Г. КОРОЛЬ, аспирант, преподаватель кафедры ИС ХНЭУ, Харьков

ПОРТАТИВНЫЕ СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ

Рассматриваются основные требования, выдвигаемые к аппаратно-программным средствам защиты конфиденциальных данных, проводится сравнительный анализ основных функций портативных аппаратных средств защиты информации категории USB флеш-накопители.

Ключевые слова: конфиденциальные данные, программно-аппаратные средства защиты, USB флеш-накопители.

Постановка задачи. Информация всегда имела стоимость, а сегодня, когда она консолидировано хранится и автоматически обрабатывается, ее стоимость стремительно возрастает. В настоящее время практически каждый человек, работая с информационными технологиями, имеет потребность в защите конфиденциальной информации. Это могут быть как финансовые отчеты, так и конструкторские документы, планы развития предприятия или сведения о корпоративных клиентах, логины и пароли к различным корпоративным или on-line сервисам, не говоря уже о ключах электронной цифровой подписи, в том числе, к системам «клиент-банк». Такая информация уязвима к угрозам разглашения и нуждается в надежной защите от несанкционированного доступа.

Целью статьи является анализ возможностей программно-аппаратных портативных средств обеспечения конфиденциальности информации и определение основных требований, выдвигаемых к функциям средств защиты конфиденциальных данных на примере портативных аппаратных средств защиты информации категории USB флеш-накопители.

Анализ источников угроз конфиденциальности персональных данных. Необходимость обеспечения безопасности персональных данных в наше время – объективная реальность. Кража персональных данных может нанести правообладателю ощутимый материальный ущерб, если речь идет о кредитных картах или информации о сбережениях в банке. Злоумышленники, обладающие достаточными техническими знаниями, похищают реквизиты банковских карт или имитируют сайты финансовых учреждений.

На самом деле зачастую даже трудно установить источник утечки персональных данных (ПД) вследствие высокой информатизации современного общества, основные средства проникновения и кражи представлены на рис. 1.

Рис. 1 – Основные средства проникновения и кражи персональных данных

Кража персональных данных может нанести правообладателю ощутимый материальный ущерб, если речь идет о кредитных картах или информации о сбережениях в банке. Злоумышленники, обладающие достаточными техническими знаниями, похищают реквизиты банковских карт (скиминг) или имитируют сайты финансовых учреждений, чтобы заставить пользователя предоставить свою личную информацию (фишинг). На практике, когда обнаружены уже последствия утечки информации, бывает очень трудно установить источник этой утечки, вследствие высокой информатизации современного общества.

Под угрозами безопасности ПД при их обработке в информационной системе ПД (ИСПД) понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных. Классификация угроз безопасности персональных данных представлена на рис. 2 [1, 2].

Рис. 2 – Классификация угроз безопасности персональных данных

В связи с повсеместным развитием Интернета наиболее часто атаки производятся с использованием уязвимостей протоколов сетевого взаимодействия, основные виды атак представлены на рис. 3.

Проведенный анализ показал, что возросшие технические возможности по сбору и обработке персональной информации, развитие средств электронной коммерции и социальных сетей делают необходимым принятие мер по защите персональных данных. Кража персональных данных может нанести правообладателю ощутимый материальный ущерб, если речь идет о кредитных картах, банковских счетах или информации о сбережениях в банках.

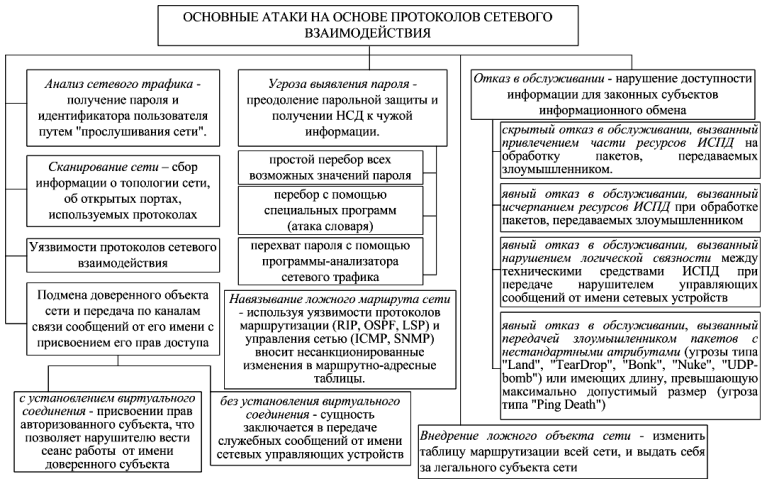

Рис. 3 – Основные виды атак с использованием уязвимостей протоколов сетевого взаимодействия

Классификация элементов комплексной системы защиты конфиденциальных данных. Для обеспечения защиты конфиденциальных (персональных) данных, выделяются три основных типа мер по обеспечению безопасности: организационные, технические и правовые. Их классификация представлена на рис. 4.

Рис. 4 – Основные типы мер по защите персональных данных

Важной составляющей комплексной защиты персональных данных являются технические средства. Условно, их можно разделить на три основных вида (по способу реализации): аппаратные, программные и программно-аппаратные. При этом исключительно аппаратные средства защиты сегодня встречаются очень редко, т.к. для гибкой интеграции аппаратного средства защиты (особенно многоцелевого) в современную ИТ-систему всё равно необходимо специализированное программное обеспечение.

К аппаратным средствам относят комплексы электронных устройств, которые обеспечивают защиту конфиденциальных данных на аппаратном уровне, т. е. реализация защиты осуществляется ресурсами самого периферийного устройства, а не рабочей станции и её программного обеспечения, включая операционную систему (ОС). Программные средства защиты – это совокупность программных компонентов, как правило, реализующих криптографические алгоритмы и обеспечивающих разграничение доступа и предотвращение угроз несанкционированного использования и модификации информации.

На практике, программные средства незаменимы при построении защиты баз персональных данных и систем обработки информации различного назначения, и сложности. Вместе с тем, программные средства, по своей природе, подвержены угрозам взлома и НСД.

Аппаратно-программные средства как правило обеспечивают комплексную защиту данных, что существенно снижает возможность несанкционированного доступа до защищенной области данных, однако, их разработка и реализация требует дополнительных экономических затрат, что существенно увеличивает их стоимость по сравнению с программными средствами.

Примерами реализации аппаратно-программных средств, криптографической защиты конфиденциальной информации являются Armorino (Украина) и InfoWatch CryptoStorage (Россия). Сравнительная характеристика Armorino и InfoWatch Crypto-Storage представлена в таблице.

Решения представлены в виде флеш-накопителей с интегрированным программным обеспечением и предназначены для защищённого хранения и обработки конфиденциальных данных. Данные устройства – наиболее универсальны в обеспечении защиты персональных данных, в случаях, использования и распространения БПД на разных компьютерах.

Разработанная система группой компаний InfoWatch предназначена для защиты конфиденциальной информации пользователя от несанкционированного доступа и предотвращения утечки данных при сохранении операционной системой служебной [3].

Система предоставляет возможность: создавать отдельные защищенные папки в файловой системе NTFS для размещения конфиденциальной информации; создавать виртуальные защищенные диски (защищенные контейнеры) для размещения конфиденциальной информации; защитить всю

информацию на логических разделах жесткого диска, включая системные и загрузочные, на Flash-накопителях, USB устройствах хранения и прочих устройствах класса MassStorage.

Сравнительная характеристика Armorino и InfoWatch Crypto-Storage

Характеристики	Armorino	InfoWatch CryptoStorage
1	2	3
Несколько разделов, с различным типом доступа.	+	-
Аппаратное шифрование данных стойкими алгоритмами.	+	+
Устойчивость к ошибкам в процессе шифрования	+	+
Поддержка нескольких учетных записей пользователей и возможность управления ними	+	–
Наличие различных ролей доступа таких как “Пользователь”, “Администратор”	+	–
Поддержка работы со всеми типами и версиями ОС	+	+
Удобство и простота в использовании	+	+
Безвозвратное удаление	–	+
Удалённое восстановление данных	–	+

Защита системного диска обеспечивает конфиденциальность: содержимого оперативной памяти, сохраняемого на диске при переходе в спящий (hi-bernate) режим; данных файла дампа памяти (crash dump), сохраняемого на диске в экстренных ситуациях; информации из временных файлов и файлов подкачки; информации на диске при неполном уничтожении файлов пользователя**.**

Для защиты информации применяется механизм прозрачного шифрования на основе блочно-симметричного алгоритма AES [3].

Системой обеспечивается: разграничение доступа к защищенной информации на основе паролей пользователей; многопользовательский доступ к защищаемой информации; возможность размещения одних защищенных объектов внутри других с произвольной глубиной вложенности; предотвращение случайного или умышленного уничтожения защищенных объектов посредством ограничения доступа к этим объектам; работа с защищенными контейнерами и папками, расположенными как на компьютере пользователя, так и на ресурсах локальной сети; возможность переноса защищенных объектов вместе с физическим носителем, на котором объекты расположены, на другой компьютер, на котором также установлена Система. При этом возможность работы с объектами не утрачивается; гарантированное удаление файлов и папок [3].

Проведенный анализ основных функций позволяет выделить недостатки системы:

- отсутствие счетчика попыток авторизации пользователя позволяет злоумышленнику осуществлять “неограниченное” количество попыток подбора ключевых последовательностей. Ключевые последовательности формируются пользователем и их “надежность” зависит от компетентности пользователя в области защиты данных;
- отсутствие возможности, в случае утраты всех паролей доступа к защищенному объекту, восстановить содержимое объекта, может привести к потере конфиденциальной информации;
- невозможность администрирования защищенных областей не обеспечивает защиту от инсайдерских атак на защищенные области других пользователей;
- отсутствует возможность надежной аутентификации пользователей Windows на основе генерации случайного пароля;
- отсутствие возможности использования портативного программного обеспечения требует дополнительных затрат на защиту от вирусных атак защищенных областей системы;
- отсутствие возможности автоматического обновления ПО.

Разработанный компанией Microcrypt Technologies защищенный USB флеш-накопитель “Арморино” позволяет эффективно противодействовать угрозам безопасности, возникающим в корпоративном секторе, и обеспечивает безопасное хранение, обработку и обмен конфиденциальной информации между разными рабочими станциями на платформе Windows. Для обеспечения конфиденциальности информации, устройство применяет высоконадежный блочный симметричный шифр AES-256 и аутентификацию авторизованных пользователей с помощью паролей, количество неудачных попыток аутентификации ограниченно. “Прозрачное” шифрование и проверка паролей реализованы непосредственно в аппаратном обеспечении, позволяя достигнуть высокого уровня защиты без потери быстродействия [1–3]. Дополнительно, этот накопитель может применяться для безопасного хранения некоторого критического программного обеспечения, которое может быть запущено непосредственно с накопителя на любой рабочей станции Windows (“портабельное” программное обеспечение), что позволяет в некоторых случаях повысить степень защиты от вредоносного программного обеспечения.

USB флеш-накопитель “Арморино” вводит гибкую систему управления полномочиями и поддерживает несколько ролей пользователей с разными правами доступа. Для авторизации в рамках любой роли, имеющей привилегированный доступ (“Ограниченный пользователь”, “Привилегированный пользователь” или “Администратор”), необходимо ввести соответствующий пароль. Реализованная система позволяет создать

единую корпоративную политику безопасности, и одновременно решить возможные угрозы, связанные с утратой (забыванием) паролей пользователями и, как следствие, потерей критической информации. Устройство “Арморино” может применяться для надежной аутентификации пользователей Windows. Для этого на хост-систему устанавливается провайдер аутентификации (Windows Logon), позволяющий выполнять вход в систему, подключив устройство и выполнив аутентификацию на пароле “Пользователя” или “Администратора” устройства. Таким образом, пользователю достаточно запомнить лишь пароль доступа к устройству и иметь само устройство.

“Armorino” поддерживает до четырех разделов на одном USB-устройстве:

CD-ROM – раздел предназначен для хранения и запуска программного обеспечения управления устройством. Для считывания информации и запуска программных приложений аутентификация не нужна.

Общий (Public) – раздел предназначен для временного хранения и переноса “открытой” информации, не требующей надежной защиты от разглашения.

Личный (Private) – раздел предназначен для хранения и переноса конфиденциальной информации. Для доступа к этому разделу требуется аутентификация. Все данные, загруженные на этот раздел, хранятся во флеш-памяти устройства в зашифрованном виде.

Скрытый (Hidden) – раздел может использоваться для хранения конфиденциальной информации, требующей особенно тщательной защиты, в том числе в условиях угрозы присутствия на рабочей станции вредоносного ПО. Для доступа к этому разделу требуется аутентификация. Все данные, загруженные на этот раздел, хранятся во флеш-памяти устройства в зашифрованном виде.

Устройство может быть использовано четырьмя классами пользователей в соответствии с уровнем привилегий:

Гость – пользователь без привилегий (анонимный пользователь), может считывать информацию и запускать на выполнение программное обеспечение с CD ROM раздела, а так же считывать/записывать информацию на Общий раздел. Аутентификация не требуется;

Ограниченный Пользователь – оператор получает этот уровень полномочий после успешной аутентификации на пароле “Ограниченного Пользователя”. Ограниченный Пользователь имеет все права Гостя, а также доступ к защищенной информации на Личном разделе. Разрешение записи информации на Личный и Общий разделы зависит от текущего состояния флагов «Защищен от записи» этих разделов и полномочий, предоставленных Ограниченному Пользователю;

Уполномоченный Пользователь – оператор получает этот уровень полномочий после успешной аутентификации на пароле “Уполномоченного

Пользователя". Уполномоченный Пользователь имеет все права Ограниченного Пользователя, а также доступ к защищенной информации на Защищенном разделе. Разрешение записи информации на Личный и Общий разделы зависит от текущего состояния флагов "Защищен от записи" этих разделов и полномочий, предоставленных Уполномоченному Пользователю;

Администратор – оператор получает этот уровень полномочий после успешной аутентификации на пароле Администратора. Уровень полномочий Администратора дает все права Уполномоченного Пользователя и добавляет к ним право конфигурирования всех параметров безопасности накопителя [4].

Для сброса текущего уровня полномочий, с которым выполнена авторизация, необходимо сделать Выход для соответствующего профиля. Устройство "Арморино" поддерживает возможность корпоративной настройки и дальнейшего менеджмента устройства на Корпоративной консоли администрирования. Корпоративная консоль позволяет выполнять следующие функции администрирования устройства:

- начальную инициализацию устройства, включая установку пароля "Администратора", политики безопасности паролей и возможность дистанционного восстановления устройства;
- изменение конфигурации устройства (тип дистанционного восстановления и политика паролей);
- восстановление устройства без потери защищенных данных (при непосредственном подключении);
- вычисление "одноразового пароля" для дистанционного восстановления устройства без потери защищенных данных;
- "сбрасывание" ключа защиты CD-ROM раздела;
- сервисные функции.

Дополнительно, устройство позволяет создавать на его "скрытом" разделе "скрытые защищенные хранилища". Каждое такое хранилище ассоциируется с некоторым сертифицированным приложением, которое создает и использует такое хранилище для хранения собственных секретных данных (в большинстве случаев, ключевой информации).

Создавать и использовать "скрытые защищенные хранилища" может лишь приложение сертифицированное компанией-разработчиком.

Доступ к данным скрытого хранилища возможен лишь после аутентификации "Администратора" или "Уполномоченного пользователя". Права доступа "Пользователя" к хранилищу приложения могут быть ограничены и определяются вовремя его создания. Накопители семейства "Арморино" позволяют изменить концепцию обеспечения конфиденциальности от "защиты отдельных файлов" до "портативного защищенного офиса в кармане рубашки" [4].

Устройство Armorino может применяться для надежной аутентификации пользователей Windows. Для этого в хост систему устанавливается провайдер

аутентификации (Windows Logon), позволяющий выполнять вход в систему, подключив устройство и выполнив аутентификацию на пароле Пользователя или Администратора устройства. Таким образом, пользователю достаточно запомнить только пароль доступа к устройству и иметь само устройство. В сравнении с простой парольной аутентификацией Windows, применение устройства Armorino позволяет значительно повысить уровень защиты учетных записей пользователей при сохранении удобства аутентификации. Это достигается благодаря установке случайного пароля для учетной записи Windows, а также блокированию устройства после исчерпания ограниченного количества (не более 15) неудачных попыток аутентификации на нем. Программная среда Armorino поддерживает расширение стандартных возможностей устройства благодаря дополнительному программному обеспечению. Внешнее ПО может использовать Armorino в качестве защищенного хранилища ключевой и другой информации. Для этого достаточно интегрировать во внешнее ПО Plugin библиотеку для работы с Armorino. Устройство поддерживает тесную интеграцию с “PortableApps.com”, что позволяет непосредственно из основного интерфейса программы выполнять инсталляцию указанного “портативного” ПО на Личный раздел устройства. “Портативное” ПО, установленное на Личном разделе, все свои данные хранит исключительно на Личном разделе, что обеспечивает необходимый уровень конфиденциальности. Особенно это актуально для почтовых клиентов, браузеров и различных чат и voice-клиентов, а также другого коммуникационного ПО [4].

Выводы. Проведенный анализ технических средств защиты конфиденциальных данных показал, что в условиях рынка информационных технологий России и Украины следует отдавать предпочтение аппаратно-программным средствам защиты информации, поскольку программные средства часто подвергаются взлому ПО, что приводит к возможности изменить уникальность его кода и использованию в личных целях. Таким образом, программные средства не в полной мере могут обеспечить достаточный уровень защиты конфиденциальных данных. Разработанный украинской компанией “Микрокрипт Текнолоджис” защищенный портативный USB флеш-накопитель удовлетворяет современным требованиям по обеспечению комплексной защиты данных.

Список литературы: **1**. *Евсеев С. П.* Портативные средства обеспечения конфиденциальности информации / *С. П. Евсеев, С. А. Головашич, О. Г. Король* // Науково-технічний журнал «Сучасний захист інформації». № 2. – 2012. – С. 43–52. **2.** Защита персональных данных. [Електронний ресурс]. – Режим доступу до ресурсу : http://www.iso27000.ru/ chitalnyi-zai/zaschita-personalnyh-dannyh/zaschita-personalnyh-dannyh [Електронний ресурс]. – Режим доступу до ресурсу : http://www.infowatch.ru/sites/default/files/products/cs/cryptostorage_user_guide_ru.pdf. **3.** CryptoStorage 2.1. Руководство пользователя **4.** Руководство пользователя “Захищений USB флеш-накопичувач-Armorhino”.

Надійшла до редколегії 05.02.2013

УДК 621.391

Портативные средства криптографической защиты конфиденциальных данных / С. П. Евсеев, О. Г. Король // Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології. – Х. : НТУ «ХПІ», 2013. – № 62 (1035). – С. 61–69. – Бібліогр.: 7 назв.

Розглядаються основні вимоги, висунуті до апаратно-програмних засобів захисту конфіденційних даних, проводиться порівняльний аналіз основних функцій портативних апаратних засобів захисту інформації категорії USB флеш- накопичувачі.

Ключові слова: персональні дані, захист персональних даних, програмно-апаратні засоби захисту.

The main demands made to the hardware and software tools for protecting sensitive data, a comparative analysis of the main features of portable hardware data protection category USB flash drives.

Keywords: sensitive data, software and hardware protection, USB flash drives.