К. А. Бирюков

СРЕДСТВА БЕЗОПАСНОГО ХРАНЕНИЯ КЛЮЧЕЙ[1]

В подавляющем большинстве многопользовательских защищенных информационных систем (ЗИС), для обеспечения информационной безопасности которых применяются средства криптографической защиты информации (СКЗИ), используется большое количество устройств для хранения ключевой информации (КИ).

Поскольку в настоящее время на рынке предлагается достаточно широкий спектр таких устройств, важнейшей задачей при выборе ключевых носителей для использования в ЗИС является обеспечение оптимального соотношения между уровнем защищенности носителя КИ и его ценой.

Попробуем проанализировать существующие на современном рынке носители КИ с точки зрения уровня защищенности и стоимостных характеристик, сделать вывод о том, существует ли в настоящее время «идеальный» носитель КИ и какие подходы к реализации защитных механизмов позволят приблизить носитель КИ к «идеалу».

Применяемые в настоящее время ключевые хранилища могут быть как относительно универсальными по своему назначению, то есть такими, для которых хранение КИ не является единственной и даже основной функцией, так и специализированными, предназначенными специально для хранения КИ.

К устройствам первого типа можно отнести различные flash-накопители, основной функцией которых является хранение больших (до нескольких десятков и даже сотен гигабайт) объемов данных.

Обычный flash-накопитель не обладает никакими защитными механизмами. Он может быть украден или утерян. Любой человек может получить доступ к данным не нем. Обычный flash-накопитель обладает чаще всего значительным объемом памяти и совместим практически с любым устройством, имеющим USB-порт. Обычный flash-накопитель может быть использован на любом средстве вычислительной техники (СВТ) в любых условиях. Информация хранится на обычном flash-накопителе в открытом виде и может быть легко скопирована и скомпрометирована.

Использование обычного flash-накопителя для хранения КИ принципиально возможно, но нецелесообразно из-за отсутствия механизмов защиты и неоправданно высокой цены, которая является следствием объема памяти, значительно превышающего необходимый для хранения КИ.

Некоторые **flash-накопители** имеют возможность включения защитного механизма в виде **установки PIN-кода** для получения доступа к данным. Безопасность такого носителя, безусловно, выше, чем у обычного flash-накопителя. Не зная PIN-кода, получить доступ к данным на таком носителе значительно сложнее[2]. Однако нередки случаи, когда пользователи хранят свой PIN-код вместе с самим носителем, а иногда и пишут его прямо на нем. Кроме того, потенциальной угрозой может являться и сам пользователь носителя, использующий его не по назначению или с преступным умыслом. Информация, хранящаяся на таком накопителе, может быть скопирована после разблокировки легальным пользователем.

Использование flash-накопителя с защитой в виде PIN-кода для хранения КИ принципиально возможно, но имеет недостатки, связанные с отсутствием механизмов защиты от неаккуратного

[1] Данная работа выполнена в НИЯУ МИФИ при финансовой поддержке Министерства образования и науки Российской Федерации проекта «Создание инженерно-технических решений для высокотехнологичного производства инновационных программно-аппаратных средств защиты информации на базе перспективных высокоскоростных интерфейсов информационного взаимодействия», выполняемого совместно с ООО «ОКБ САПР».

[2] Поскольку в общем случае flash-накопитель — пассивное устройство, реализация проверки PIN-кода для доступа к нему является программной. Это дает возможности, во-первых, для обхода проверки эмуляцией ответа проверяющей программы «PIN-верный», а во вторых, для подбора PIN-кода, так как количество попыток его неверного ввода не ограничено.

или недобросовестного пользователя, довольно низкой защищенностью механизма проверки PIN-кода и, как и в предыдущем случае, неоправданно высокой ценой, которая является следствием объема памяти, значительно превышающего необходимый для хранения КИ.

Программно-аппаратный комплекс (ПАК) «Секрет» обладает значительным объемом памяти, при этом доступ к данным возможен только после ввода PIN-кода и только на тех СВТ, на которых он был предварительно зарегистрирован [1].

Таким образом, даже если ПАК «Секрет» будет утерян или украден вместе со своим пользовательским PIN-кодом, то доступ к информации на нем все равно невозможно получить на не зарегистрированном на нем СВТ. Это также помогает предотвратить неправомерное использование информации, находящейся на ПАК «Секрет», легальными пользователями.

Описанное свойство ПАК «Секрет» актуально для хранения КИ, использующейся СКЗИ, так как по требованиям, предъявляемым к организации криптографической защиты информации, КИ допускается использовать только в доверенной среде функционирования СКЗИ, а недобросовестный пользователь или злоумышленник, завладевший ПАК «Секрет» и его пользовательским PIN-кодом, может попытаться использовать КИ где-то еще.

ПАК «Секрет» имеет 3 модификации («Личный Секрет», «Секрет Фирмы», «Секрет Особого Назначения») и может выпускаться как с возможностью шифрования данных на нем, так и без нее.

Защищенное хранение данных — единственная функция ПАК «Секрет». Такими данными может быть, в том числе, и КИ.

Однако использование ПАК «Секрет» для хранения КИ нецелесообразно из-за неоправданно высокой цены, которая является следствием объема памяти, сопоставимого с объемом памяти других flash-накопителей и значительно превышающего необходимый для хранения КИ.

Следует также отметить, что все модификации ПАК «Секрет», за исключением модификации «Секрет Особого Назначения», требуют установки на СВТ, на котором предполагается их использование, специального программного обеспечения.

Теперь рассмотрим устройства, предназначенные специально для хранения КИ.

TM-идентификаторы (TM — Touch Memory) не обладают никакими защитными механизмами, кроме необходимости наличия специального считывающего устройства, свободно продаваемого.

Содержимое TM-идентификаторов можно копировать, поэтому КИ, хранящаяся в устройстве в открытом виде, может быть легко скомпрометирована.

Основное предназначение TM-идентификаторов — двухфакторная аутентификация. Если аутентифицирующей информацией являются не непосредственно хранящиеся в TM-идентификаторе данные, а результат преобразования, которое производится резидентным компонентом безопасности с данными, полученными по разным каналам, то возможность копирования памяти TM-идентификатора не является критичным фактором, в отличие от возможности считывания хранящихся в TM-идентификаторе в открытом виде криптографических ключей.

TM-идентификатор характеризуется низкой ценой, объемом памяти, достаточным для хранения КИ, но не избыточным, как в случае использования различных flash-накопителей, и отсутствием защитных механизмов.

Смарт-карты обычно обладают весьма скромным объемом памяти для данных — десятки килобайт, однако этого достаточно для хранения КИ. Для доступа к данным необходим ввод PIN-кода. Устройство может быть заблокировано после некоторого количества неверных вводов PIN-кода подряд, что делает затруднительным его подбор. Смарт-карты обладают хорошей

совместимостью, так как используют стандартный протокол, но для их использования требуется специальное считывающее устройство — кардридер. Одна из основных проблем смарт-карт — их возможный отказ, так как тонкий пластиковый корпус не может обеспечить надежную защиту при физических воздействиях.

Если злоумышленник завладел и смарт-картой, и ее PIN-кодом, он сможет получить доступ к данным. Легальный пользователь смарт-карты технически может, хотя и не должен, использовать ее вне доверенной среды, при этом PIN-код может быть перехвачен с устройства ввода, ключи могут быть списаны из оперативной памяти или из памяти смарт-карты после разблокировки легальным пользователем.

Хранение КИ — не единственная функция смарт-карты, но она — одна из основных.

Токены могут иметь более широкие возможности по сравнению со смарт-картами. Например, устройство может содержать свою собственную клавиатуру для ввода PIN-кода, что значительно усложняет перехват.

Если злоумышленник завладел и токеном, и необходимым кодом доступа, он сможет получить доступ к данным. Легальный пользователь токена технически может, хотя и не должен, использовать его вне доверенной среды, при этом ключи могут быть списаны из оперативной памяти или прямо из устройства после его разблокировки легальным пользователем.

Токены обладают небольшим объемом памяти для данных, которого достаточно для хранения КИ, характеризуются невысокой стоимостью и хорошей совместимостью, хотя обычно для работы с токеном необходима установка драйверов.

Хранение КИ — это не единственная и не основная функция токенов. Их основное назначение, как и ТМ-идентификаторов, — двухфакторная аутентификация.

Типичными представителями семейства токенов являются eToken [2], RuToken [3] и ШИПКА-лайт Slim [4].

Анализ существующих типов ключевых хранилищ показал отсутствие на современном рынке устройства, имеющего «идеальное» или, по крайней мере, оптимальное соотношение между уровнем защищенности и ценой.

Помимо этого, даже если ЗИС достаточно надежно защищена различными техническими и программными средствами, то специализированное ключевое хранилище, содержащее секретный криптографический ключ, будучи изъято из ЗИС, остается защищенным максимум PIN-кодом. Это создает угрозу компрометации секретного криптографического ключа при утере или краже хранилища КИ вместе с его PIN-кодом, а также если легальный пользователь хранилища КИ является злоумышленником.

Данные проблемы можно решить, используя носитель КИ, который не будет функционировать и предоставлять доступ к криптографическому ключу где-либо, кроме как в своей (своих) ЗИС. Для этого такой носитель КИ должен обладать функцией, определяющей, на каком именно СВТ пытаются его использовать.

Данное устройство, так называемый идеальный токен, совместит в себе преимущества классического токена (дешевизна, универсальность, надежность) и ПАК «Секрет», который позволяет предотвращать неправомерное использование информации, находящейся на ПАК «Секрет», легальными пользователями.

Для создания такого устройства оптимальным видится соединение в одном решении функциональности устройств ШИПКА-лайт Slim и ПАК «Личный Секрет» по следующим причинам:

- ШИПКА-лайт Slim и ПАК «Личный Секрет» разработаны одной компанией (ЗАО «ОКБ САПР»), что упростит и удешевит процесс интеграции;

- для применения в качестве ключевого носителя избыточны собственные криптографические функции, реализованные в других версиях устройств ШИПКА и делающие их более дорогостоящими;
- сетевое управление ключевыми носителями (аналогично ПАК «Секрет Фирмы») также избыточно в рамках решаемой задачи;
- необходимость предварительной установки программного обеспечения на СВТ, требующее административных прав и являющееся основным ограничением ПАК «Личный Секрет» по сравнению с ПАК «Секрет Особого Назначения», не имеет решающего значения в ситуации с ключевыми носителями и идентификаторами, которые в любом случае должны применяться только на тех СВТ, на которых функционируют СКЗИ и/или средства защиты информации от несанкционированного доступа, требующие административных прав при установке;
- реализация схемы доступа, используемой ПАК «Личный Секрет», возможна на базе существующего устройства ШИПКА-лайт Slim без изменения его аппаратной составляющей, в то время как реализация схемы, используемой ПАК «Секрет Особого Назначения», потребует создания новой аппаратной базы, что повлечет за собой дополнительные временные и трудозатраты и в конечном счете приведет к повышению цены устройства.

Создание и применение «идеальных токенов» должно повысить уровень защищенности ЗИС за счет более безопасного хранения КИ без значительного роста стоимости используемого парка носителей КИ.

СПИСОК ЛИТЕРАТУРЫ:

1. ПАК «Секрет». Документация. URL: http://www.prosecret.ru/documentation.html (дата обращения: 24.08.2013).
2. USB-ключи и смарт-карты eToken. Раздел каталога. URL: http://www.aladdin-rd.ru/catalog/etoken/ (дата обращения: 24.08.2013).
3. Рутокен (RuToken). Раздел каталога. URL: http://www.rutoken.ru/products/all/ (дата обращения: 24.08.2013).
4. ПСКЗИ «ШИПКА». Документация. URL: http://www.shipka.ru/documentation.html (дата обращения: 24.08.2013).