Защита информации в компьютерных системах: [монография] / [М.В.Буйневич и др.]; под ред. Е.В.Стельмашонок, И.Н.Васильевой. – СПб: Изд-во СПбГЭУ, 2017. (163 с.) – С.72-85.

2.1. Вопросы практического использования российской криптографии в среде операционных систем Windows

Васильева И.Н.

Криптография является традиционным средством обеспечения конфиденциальности как хранимой, так и передаваемой информации. Однако круг задач, решаемых с использованием криптосистем, гораздо шире: контроль целостности, аутентификация сторон коммуникации, формирование общего секрета, обеспечение невозможности отказа сторон от авторства. Поэтому не удивительно, что большинство современных развитых систем, таких как операционные системы (ОС), web-серверы и СУБД, обладают встроенными криптографическими функциями.

В корпоративной среде аутентификация пользователей и устройств, работа с цифровыми сертификатами и защищенный обмен информации по сети, могут выполняться средствами базового программного обеспечения, например, ОС Windows и поддерживаемыми ею серверными службами [11]. ОС семейства Windows имеют ряд встроенных криптографических средств, поддерживающих локальное шифрование файлов (файловая шифрующая система EFS) и дисков (BitLocker), защищенную сетевую передачу информации (поддержка протоколов TLS и SSL для HTTPS, IPSec), сетевую аутентификацию по протоколу Kerberos, управление сертификатами пользователей, устройств и служб (служба Certification Authority). Некоторые из этих средств допускают настройку, предполагающую выбор криптографических алгоритмов, режимов их работы и длин ключей. Набор доступных криптоалгоритмов зависит от конкретной реализации. К сожалению, популярные криптографические функции, встроенные в ОС Windows, равно как и встроенные реализации сетевых защищенных протоколов по умолчанию не поддерживают выбор отечественных криптоалгоритмов.

Вместе с тем, криптографические методы и средства защиты информации традиционно являются объектом правовых ограничений. Так, средства криптографической защиты информации (СКЗИ), используемые в государственных информационных системах, а также для обеспечения конфиденциальность информации, доступ к которой ограничен федеральными законами РФ, должны быть сертифицированы по соответствующему классу безопасности. Это накладывает ограничения на используемые криптографические системы, а именно, СКЗИ должны реализовывать криптоалгоритмы, описанные российскими стандартами [2-5]. Использование отечественных

криптографических стандартов рекомендовано и в некоторых других случаях, например, в защищенных информационных системах финансово-кредитных учреждений РФ, для формирования квалифицированной цифровой подписи, работы удостоверяющих центров и т.д.

В настоящее время на рынке представлен широкий спектр криптографических решений, поддерживающих отечественную криптографию, – от криптопровайдеров, являющихся, по сути, низкоуровневыми библиотеками криптографических функций, отдельных утилит, надстроек и плагинов, расширяющих функции конкретных приложений или протоколов, до интегральных программно-аппаратных комплексов. Вместе с тем, применение российских СКЗИ зачастую сопряжен с рядом трудностей, вызванных:

- неразвитостью и ограниченностью пользовательского интерфейса и интерфейса администратора;
- непрозрачностью настройки;
- слабой совместимостью, а иногда и явными конфликтами, средств различных производителей между собой, а также и с базовым программным обеспечением, в частности, при его обновлении;
- ограниченной функциональностью по сравнению со встроенными механизмами защиты;
- отсутствием развитой документации по использованию и администрированию;
- слабая техническая поддержка в нестандартных ситуациях.

Стоит также добавить, что внедрение полнофункциональных программно-аппаратных комплексов криптографической защиты является достаточно дорогостоящим решением и может оказаться экономически невыгодным в условиях отсутствии необходимости обязательного выполнения требований регуляторов. Поэтому очень заманчивым было бы применение интегрированных в базовое программное обеспечение криптографических механизмов в сочетании с российскими криптоалгоритмами ГОСТ. Такой подход позволяет использовать привычную среду настройки и управления компонентов Windows с возможностью использования отечественной криптографии.

В единой среде операционной системы Windows, приложения могут обращаться к низкоуровневым реализациям криптографических функций посредством прикладного интерфейса Cryptography Next Generation (CNG) API (Crypto API в старых версиях ОС). Интерфейс CNG API позволяет разграничить прикладной уровень и уровень реализации криптографических функций (рис. 2.1), обеспечив доступ к последнему через набор стандартных функций или интерфейсов.

Поставщиками криптографии в архитектуре CNG API являются криптопровайдеры CSP, что позволяет использовать разные криптографические алгоритмы и различные реализации этих алгоритмов, включая аппаратные.

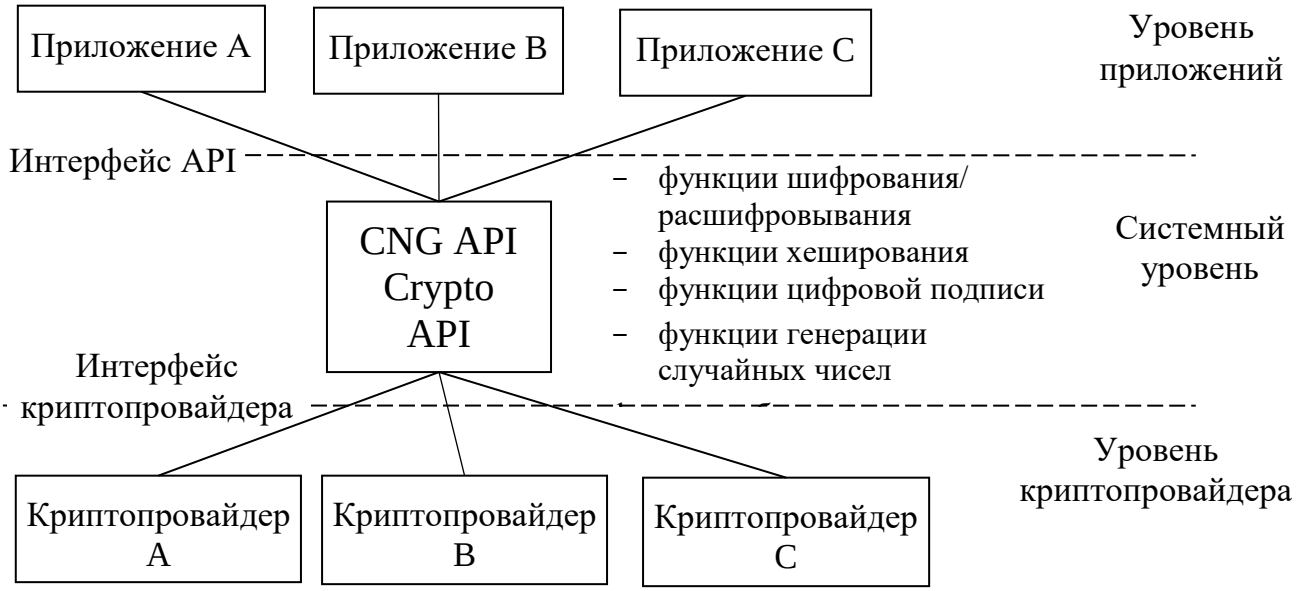

Рис. 2.1. Общая архитектура криптографических интерфейсов API

Криптопровайдер – предоставляющая специальный интерфейс и специальным образом зарегистрированная в ОС библиотека, которая позволяет расширить список поддерживаемых алгоритмов. При этом CNG API поддерживает обращение как к встроенным CSP Windows, так и к криптопровайдерам сторонних производителей. Это позволяет, установив в операционную систему сертифицированный криптопровайдер отечественных производителей (например, КриптоПро CSP, ViPNet CSP и т.п.), строить защищенные системы с поддержкой российской криптографии. Криптопровайдеры де-факто стали стандартом СКЗИ, однако несовершенство предлагаемых ОС Windows механизмов расширения вынуждает разработчиков дополнительно модифицировать высокоуровневые криптобиблиотеки и приложения MS Windows, что требует в некоторых случаях использования дополнительных утилит (например, КриптоПро IPSec, КриптоПро EFS и др).

Рассмотрим далее совместное использование службы сертификации MS Windows (Certification Authority, CA) и криптопровайдера КриптоПро CSP, как продукт одного из наиболее авторитетных отечественных производителей с сфере разработки СКЗИ (компании КриптоПро). Отметим, что альтернативой использованию CA

для управления сертификатами является установка удостоверяющего центра КриптоПро УЦ. В таком случае работа с сертификатами будет осуществляться через интерфейс продуктов КриптоПро.

Служба сертификации CA является основой развертывания корпоративной инфраструктуры открытых ключей PKI и осуществляет выпуск и управление сертификатами пользователей, компьютеров, служб и устройств в локальной сети предприятия, что позволяет на ее основе осуществлять аутентификацию, локальное шифрование и защищенный сетевой обмен данными. Поэтому важным этапом является планирование инфраструктуры PKI, что предполагает, в частности получение ответа на вопрос о необходимости внедрения в корпоративной среде:

- защищенных механизмов сетевой аутентификации на основе сертификатов, в том числе с использованием смарт-карт;
- защищенных сетевых протоколов (SSL/TLS, IPsec);
- защищенных запросов чтения и записи данных в Active Directory с помощью Secure LDAP;
- защищенной электронной почты с возможностью шифрования и/или подписания сообщений;
- подписание программного кода приложений или документов;
- управление шифрующей файловой системой EFS.

Планирование самой службы CA предполагает, исходя из анализа существующей сетевой инфраструктуры и политики безопасности компании, определение:

- иерархической структуры корневых и подчиненных центров сертификации в сети предприятия;
- криптографических алгоритмов;
- сроков действия сертификатов;
- возможности централизованной архивации и восстановления закрытых ключей,
- возможности автоматической регистрации и обновления сертификатов и т.п.

Процесс установки службы сертификации CA, поддерживающей сертификаты с российскими криптоалгоритмами, в целом следует стандартной процедуре, однако следует обратить внимание на следующие моменты:

- использование настраиваемых шаблонов сертификатов, позволяющих выбрать российские криптоалгоритмы, доступно только в версиях Enterprise/ Datacenter операционной системы Windows Server не ниже 2003;

- в системе должен быть предварительно установлен криптопровайдер КриптоПро CSP;
- должен быть выбран тип установки CA Enterprise (Предприятие);
- при создании нового ключа сертификата CA в окне настроек криптографии следует выбрать в качестве поставщика служб шифрования (CSP) отечественный криптопровайдер и включить флаг Allow administrator interaction when the private key is accessed by the CA (Разрешить взаимодействие с администратором, если ЦС обращается к закрытому ключу).

Последнее необходимо, так как отечественные криптопровайдеры используют для создания ключей биометрический генератор случайных последовательностей, что требует выполнения определенных действий со стороны пользователя.

Кроме того, установке CA может предшествовать настройка групповой политики домена, а также настройка межсетевого экрана. Например, если планируется управление сертификатами файловой шифрующей системы EFS на компьютерах домена, может быть предложена следующая процедура развертывания службы сертификации:

1. Настройка групповой политики безопасности, запрещающей использование файловой шифрующей системы EFS на компьютерах домена (ветвь Computer Configuration/ Policies/ Widows Settings/ Security Settings/ Public Key Policies/ EFS File System – Конфигурация компьютера/ Политики/ Конфигурация Windows/ Параметры безопасности/ Политики открытого ключа/ Шифрующая файловая система EFS).

2. Установка криптопровайдера КриптоПро CSP и утилиты КриптоПро EFS на сервере и клиентских компьютерах.

Здесь стоит отметить, что не все компоненты Windows позволяют осуществлять выбор криптопровайдера с помощью шаблонов безопасности. В таких случаях должны быть установлены дополнительные утилиты КриптоПро, использующиеся совместно с криптопровайдером. Такие утилиты фактически представляют собой надстройку над механизмами реализации этого компонента (например, EFS) в операционной системе.

3. Установка на сервере центра сертификации CA с выбором российских криптографических алгоритмов. При установке кроме службы центра сертификации Certification Authority может быть также установлена служба Certification Authority Web Enrollment (Служба регистрации в центре сертификации через Интернет).

Использование службы Web Enrollment может быть полезно при работе с сертификатами вне домена (когда работа с консолью mmc недоступна). Вместе с тем, эта служба имеет ряд ограничений, в частности, через web-интерфейс сложно получить сертификаты со значениями параметров, отличными от заданных в шаблоне. Кроме того, не поддерживается работа с шаблонами V3 (Windows Server 2008 Enterprise).

4. Настройка шаблонов сертификатов. Перед выдачей сертификатов следует настроить шаблоны, на основе которых они будут создаваться. Шаблоны сертификатов настраиваются в оснастке центра сертификации. Необходимо выбрать те шаблоны, которые соответствуют планируемым сервисам безопасности, например, для использования шифрования EFS следует создать дубликат и настроить параметры шаблонов EFS Basic (Базовое шифрование EFS) и EFS Recovery Agent (Агент восстановления EFS). Для использования российских криптоалгоритмов следует создать копии указанных шаблонов, выбрав legacy-тип, то есть шаблон V2 (Windows Server 2003 Enterprise).

Следует отметить, что CNG позволяет разработчикам запрашивать алгоритмы, не указывая поставщиков алгоритмов. Шаблоны V3 содержат предопределенные перечни алгоритмов (цифровой подписи, шифрования с открытым ключом, хэширования) и не предоставляют возможности выбора криптопровайдера. Поэтому для целей использования отечественной криптографии шаблоны V3 не подходят. Настройка шаблонов V2 для этих целей так же имеет ряд особенностей:

- создание экспортируемых ключей не поддерживается – следует отключить флаг Allow private key to be exported (Разрешить экспортировать закрытый ключ);
- поскольку отечественный стандарт ГОСТ Р 34.10–2012 определяет цифровую подпись на эллиптических кривых с ключами размером 512 или 1024 бит, в шаблоне требуется установить минимально возможный размер ключа (512 бит);

Правильность указания этих параметров определяет возможность выбора отечественных CSP в качестве поставщиков криптоалгоритмов, в противном случае они не будут отображены в списке доступных криптопровайдеров.

Для каждого шаблона следует настроить политику выдачи, указав группы или пользователи, имеющие доступ к шаблону. Для запроса и получения сертификатов достаточно дать права Enroll (Заявка) и, возможно, AutoEnroll (Автоматическая подача заявок).

Право на автоматическую подачу заявок является дополнительным к праву заявки, то есть не будет действовать без него. Следует также

отметить, что автоматическая регистрация для сертификатов на основе настраиваемых шаблонов сертификатов с поддержкой российской криптографии будет действовать только при соблюдении следующих условий:

- для шаблона указана необходимость запроса пользователя при создании сертификата (установлен флаг Prompt the user during enrollment – Запрашивать пользователя во время регистрации);
- в домене включена групповая политика автоматической регистрации сертификатов (ветвь User configuration/ Policies/ Widows Settings/ Security Settings/ Public Key Policies/ Certificate Services Client - Auto-Enrollment – Конфигурация пользователя/ Политики/ Конфигурация Windows/ Параметры безопасности/ Политики открытого ключа/ Клиент служб сертификации: автоматическая регистрация, дополнительно следует установить флаг Update certificates that use certificate templates – Обновлять сертификаты, использующие шаблоны сертификатов).

После настройки следует указать, что созданные шаблоны будут служить для выпуска сертификатов CA (New/ Certificate Template to Issue – Создать/ Выдаваемый шаблон сертификатов), исключив исходные шаблоны из списка выдаваемых.

5. Получить сертификат агента восстановления EFS, используя оснастку Сертификаты. Роль агента восстановления EFS по умолчанию доступна для администраторов, однако рекомендуется для этих целей создать отдельную учетную запись. Запрос сертификата с помощью оснастки Сертификаты позволяет изменить значения некоторых параметров шаблона, в частности осуществить выбор:

- криптопровайдера из списка доступных;
- алгоритма шифрования;
- длины ключа.

Так же существует возможность запросить сертификат с экспортируемым закрытым ключом, даже если это свойство отключено в шаблоне сертификата.

Закрытый ключ сертификата агента восстановления EFS рекомендуется экспортировать на внешний носитель, чтобы обеспечить возможность его восстановления из файла при необходимости. Файлы-контейнеры закрытого ключа рекомендуется хранить на защищенных носителях, таких как смарт-карта или USB-токен. В этом случае сертификат может быть перенесен на защищенный носитель сразу же в процессе его создания. При одновременном удалении закрытого ключа

сертификата из системы агент восстановления становится полностью независимым от своего профиля.

При использовании защищенных носителей (смарт-карты, USB-токена) предварительно должен быть настроен шаблон типа Smart Card Logon (Вход со смарт-картой) или Smart Card User (Пользователь со смарт-картой) и получен соответствующий сертификат.

6. Настроить групповую политику файловой шифрующей системы EFS в домене, указав полученный сертификат в качестве сертификата агента восстановления данных и разрешив шифрование EFS, сняв флаг Allow EFS to generate self-signed certificates when the certification authority is not available (Разрешить EFS создавать самозаверяющиеся сертификаты, если центр сертификации недоступен).

Теперь агент восстановления сможет получить доступ ко всем файлам, зашифрованным с использованием сертификатов, которые будут выданы позднее. При этом пользователи домена смогут использовать шифрование только на основе сертификатов, выданных CA.

7. При необходимости настроить службу Certification Authority Web Enrollment, добавив в настройках сайта по умолчанию web-сервера IIS, расположенного на сервере с CA, поддержку протокола HTTPS. В качестве сертификата можно использовать сертификат компьютера сервера или сертификат web-сервера, предварительно настроив соответствующий шаблон.

8. До начала использования шифрующей файловой системы EFS получить сертификаты шифрования от имени пользователей. Сертификаты могут быть получены через web-интерфейс (без поддержки экспорта закрытого ключа) либо с помощью оснастки Сертификаты. Если включена поддержка автоматической регистрации, при первом входе в систему пользователю будет предложено сформировать запрос на получение сертификата (запрос оснастки Сертификаты).

Подобная процедура позволяет использовать стандартный интерфейс ОС Windows для шифрования файлов и папок, предоставления доступа ограниченного числа пользователей к зашифрованному файлу (путем выбора их сертификатов в свойствах зашифрованного файла), а также восстанавливать файлы от лица агента восстановления EFS в случае утраты сертификата шифрования. Шифрование в сетевых папках поддерживается ограниченно. Кроме того, при отчуждении сертификата из системы (например, экспорта на защищенный внешний носитель при одновременном удалении из системы) доступ к зашифрованным данным становится невозможным даже в том случае, если был получен доступ к профилю пользователя. Поэтому даже без использования смарт-карт или usb-токенов сотрудник,

например, уезжая в отпуск, может удалить закрытый ключ из системы, сделав невозможным просмотр своих данных. После обратного импорта сертификата с закрытым ключом в систему и установки из контейнера закрытого ключа через интерфейс КриптоПро CSP доступ к зашифрованным файлам восстанавливается.

Аналогично описанной процедуре могут быть настроены шаблоны и получены сертификаты для использования в защищенном сетевом обмене по протоколу IPSec, аутентификации Kerberos и т.д. Отметим также, что указанные сертификаты могут использоваться и для подписания документов и сообщений в приложениях MS Office при установке надстройки КриптоПро Office Signature. Вместе с тем следует отметить, что сертификаты КриптоПро имеют ряд ограничений – так, не поддерживается централизованная архивация и восстановление закрытых ключей (в CA для этих целей предусмотрена роль агента восстановления ключей), шаблоны V3, а на шаблоны V2 также накладывается ряд ограничений, которые были рассмотрены выше.

Интересно, что выбор стороннего CSP и отечественных алгоритмов шифрования потенциально возможен даже для парольной защиты документов Microsoft Office, поскольку процедура шифрования документа не накладывает ограничений на используемый блочный симметричный шифр или хэш-функцию [14]. Ранние версии MS Office имели слабую криптографию, реализуя такие алгоритмы, как побитовый XOR с обфускацией, RC4 с 40-битным ключом, а длина пароля была ограничена 16 символами. В большинстве случаев парольная защита документов могла быть легко взломана методом грубой силы. Начиная с версии MS Office 2010 используются алгоритмы, поставляемые на уровне ОС криптопровайдерами CSP, а схема генерации ключа значительно усилена для снижения эффективности подбора паролей (рис. 2.2). Кроме того для зашифрованных данных производится проверка целостности с использованием конструкции HMAC.

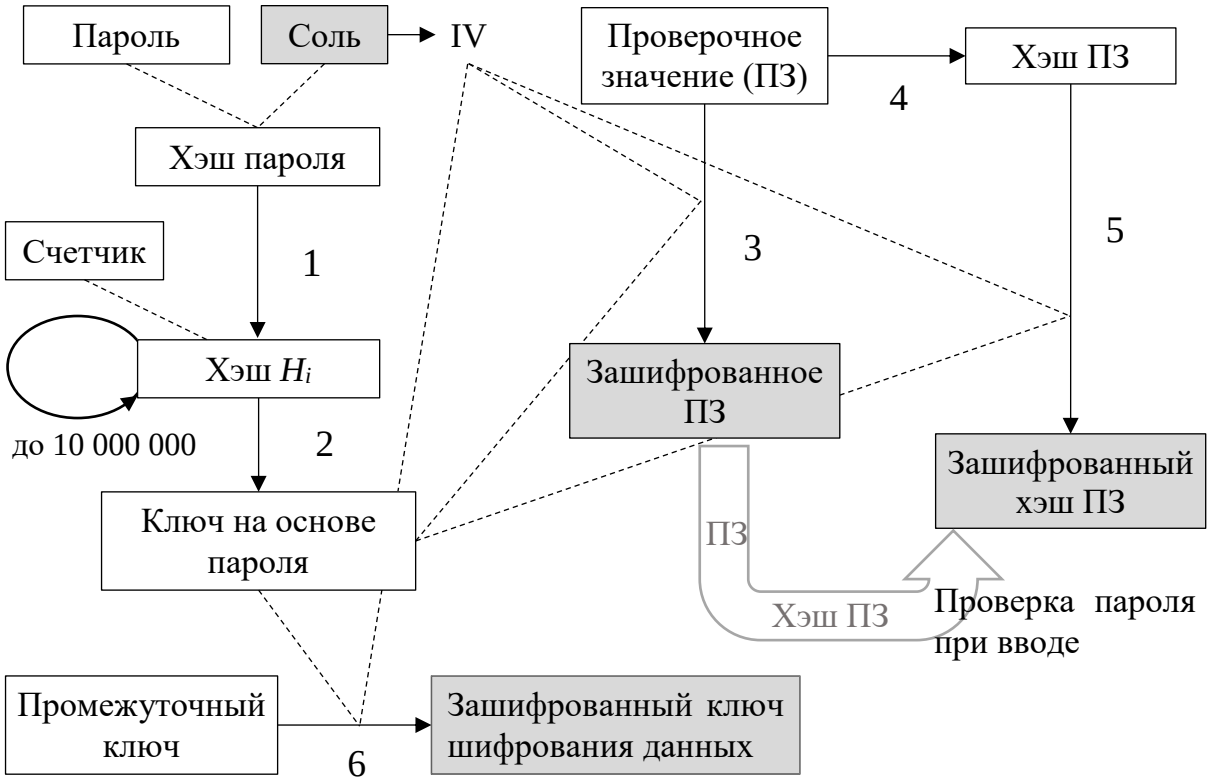

Рис. 2.2. Генерация ключевой информации в документах MS Office

Пароль пользователя дополняется случайной последовательностью (соль) и хэшируется, затем процедура хэширования итерационно повторяется (шаг 1), причем входные данные каждый раз дополняются нарастающим значением счетчика. Финальная итерация использует в качестве дополняющего значение специального вида. Ключ на основе пароля получается из финального значения хэша путем обрезки последнего, или напротив, дополнения последовательностью фиксированного вида (в зависимости от используемой хэш-функции и требуемой длины ключа) – шаг 2. Однако полученный ключ не используется для шифрования данных. Его назначение – шифрование информации, сохраняемой вместе с документом, а именно – значения, используемого для проверки правильности введенного пользователем пароля и его хэша, а также случайного ключа шифрования данных, который в документах Microsoft назван промежуточным ключом. По умолчанию для шифрования используется режим сцепления блоков CBC с вектором инициализации, получаемым на основе значения соли. Значения, сохраняемые вместе с документом, выделены на рис. 2.2 заливкой цветом.

Для проверки правильности пароля, введенного пользователем для доступа к защищенному документу, используется генерируемое

случайным образом проверочное значение. Оно шифруется и сохраняется вместе с документом (шаг 3). Затем вычисляется хэш проверочного значения (шаг 4), который также шифруется (шаг 5) и сохраняется. Теперь после ввода пароля пользователем может быть вычислен ключ, расшифровано значение проверочного значения, вычислен его хэш, последний должен быть зашифрован и сравнен с сохраненным зашифрованным значением хэша. Совпадение значений подтверждает правильность пароля.

По умолчанию приложения MS Office используют симметричный блочный шифр AES с 128-битовым ключом и хэш-функция SHA-1. Поскольку SHA-1 генерирует хэш-код размером 160 бит, а алгоритм AES производит шифрование блоками по 128 бит, на шаге 5 приходится производить шифрование двух блоков, второй из которых является неполным и дополняется до полной длины нулевыми битами. Тогда при попытке определения ключа с помощью операции, обратной шагу 5, нарушитель получит критерий проверки правильности подбора ключа – наличие заданного количества нулей на конце расшифрованного значения [10]. Даже с учетом практической невозможности полного перебора ключей размером 128 бит, данный факт внушает определенные опасения. Поэтому можно сформулировать следующие требования к алгоритмам, используемым для парольной защиты документов MS Office:

- размер выхода хэш-функции должен быть не короче длины ключа симметричного шифра;
- размер выхода хэш-функции должен быть кратен размеру блока симметричного шифра.

Применительно к алгоритмам, используемым в MS Office по умолчанию, достаточно заменить алгоритм хэширования SHA-1 на хэш-функцию SHA-256 или SHA-512, тем более что SHA-1 в настоящее время признан небезопасным [12]. Следует отметить, что российские криптоалгоритмы полностью удовлетворяют сформулированным требованиям.

Настройка криптографии MS Office осуществляется с помощью групповой или локальной политики и загружаемых с сайта производителя шаблонов безопасности. После копирования файлов шаблонов в стандартное расположение на компьютере параметры безопасности автоматически считываются редактором групповой политики. Для MS Office возможен выбор криптопровайдера с указанием используемого симметричного шифра и длины ключа (политика Тип шифрования для защищенных паролем файлов Office Open XML). Указанная политика распространяется на шифрование защищенных

паролем документов MS Excel, PowerPoint и Word при условии использования пользовательской COM-надстройки для шифрования. COM-надстройки – механизм, позволяющий разработчику расширить функциональные возможности приложений Office для решения пользовательских задач. COM-надстройка представляет собой элемент ActiveX DLL и может быть использована после установки, регистрации в реестре Windows и активации в окне приложения. Однако подобные надстройки ведущими отечественными разработчиками СКЗИ не предоставляются.

Кроме того, для приложений MS Access, Excel, OneNote, PowerPoint, Project и Word определены собственные политики, связанные с парольной защитой. Эти политики позволяют задавать такие параметры, как:

- используемый симметричный блочный шифр (Задать алгоритм шифрования CNG);
- режим работы блочного шифра (Настройка режима цепочки шифрования CNG);
- длину ключа блочного шифра (Задать длину ключа шифрования CNG);
- используемую хэш-функцию (Задать алгоритм хэширования CNG),

а также значения некоторых параметров процедуры генерации ключа (размер соли, число итераций вычисления хэша пароля).

Перечисленные политики конкретных приложений предполагают указание имен алгоритмов без выбора криптопровайдера, что создает определенные сложности в плане использования отечественной криптографии.

Политики цифровой подписи документов MS Office не предполагают выбор криптографических алгоритмов, поскольку последние определяются имеющимися сертификатами пользователя. Для обеспечения возможности использования сертификатов с российскими криптоалгоритмами для подписывания документов MS Office компания КритоПро предлагает установить соответствующую надстройку (КриптоПро Office Signature).

Следует отметить, что само по себе использование сертифицированного поставщика криптографических функций или эталонных реализаций криптографических стандартов [8] при самостоятельной реализации приложения не гарантирует требуемого уровня защищенности. Это связано необходимостью решения ряда проблемных вопросов, и прежде всего, обеспечения корректности использования ключей, безопасности управления ключевой

информацией и взаимодействия со средой функционирования СКЗИ. Так, например, приведенная выше схема парольной защиты компании Microsoft существенно отличается от рекомендаций как американского NIST [15], так и отечественного технического комитета по стандартизации «Криптографическая защита информации» (ТК 26) [6, 9], схема генерации ключа в которых предусматривает использование не простого хэширования, а конструкции HMAC.

Множество вопросов связано и с реализацией генерации случайных значений. Например, периодически появляются сообщения о слабости шифрования документов MS Office, связанные с использованием одинаковых ключей (в частности, подобная уязвимость была обнаружена как для старых [1], так и для относительно новых [13] версий MS Excel). Встроенные генераторы «случайных» чисел, доступные в большинстве высокоуровневых языков программирования, как правило, не являются криптографически сильными. В случае же использования специальных криптографических библиотек источником проблем может быть отсутствие или не полнота документации, а также невозможность управления отдельными параметрами. Ориентиром в этом направлении являются рекомендации по стандартизации группы «Информационная технология. Криптографическая защита информации» и методические документы ТК 26, в частности проект рекомендаций по стандартизации [7].

Следует также иметь в виду, что согласно федеральному закону «О лицензировании отдельных видов деятельности» от 04.05.2011 № 99-ФЗ, разработка, производство, распространение (и др.) СКЗИ и информационных систем, защищенных с помощью СКЗИ, подлежит обязательному лицензированию.

Литература:

1. В системе шифрования Office обнаружена ошибка / Роберт Лемос (Robert Lemos), CNET News.com, 21.01.2005 электронный ресурс]. URL: http://www.astera.ru/news/?id=20957 (дата обращения: 11.11.2017).
2. ГОСТ Р34.10–2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – М.: Стандартинформ, 2012. – 29 с.
3. ГОСТ Р 34.11–2012 Информационная технология. Криптографическая защита информации. Функция хэширования – М.: Стандартинформ, 2012. – 34 с.

4. ГОСТ Р 34.12–2015 Информационная технология. Криптографическая защита информации. Блочные шифры. – М.: Стандартинформ, 2015. – 21 с.
5. ГОСТ Р 34.13–2015 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. – М.: Стандартинформ, 2015. – 38 с.
6. Парольная защита с использованием алгоритмов ГОСТ. Методические рекомендации технического комитета по стандартизации «Криптографическая защита информации» (ТК 26), 27.11.2012 [электронный ресурс]. URL: https://www.tc26.ru/methods/containers_v1/ Addition_to_PKCS5_v1_0.pdf (дата обращения: 11.11.2017).
7. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации [электронный ресурс]. URL: http://www.tc26.ru/standard/gost/ (дата обращения: 11.11.2017).
8. Программная реализация криптографического преобразования базовых блочных шифров, определенных стандартом «Информационная технология. Криптографическая защита информации. Блочные шифры» и режимов их работы [электронный ресурс]. URL: http://www.tc26.ru/standard/gost/PR_GOSTR_bch_v9.zip (дата обращения: 11.11.2017).
9. Рекомендации по стандартизации Р 50.1.111–2016. Информационная технология. Криптографическая защита информации. Парольная защита ключевой информации. – М.: Стандартинформ, 2016. – 15 с.
10. Старые недоработки в MS Office на новый лад/ Pavel Semjanov, 03.12.2009 // Все о паролях и практической криптографии [электронный ресурс]. URL: http://www.password-crackers.ru/blog/?p=87 (дата обращения: 11.11.2017).
11. Чернокнижный Г.М. Вычислительные сети. Контроль безопасности в компьютерных сетях: учебное пособие – СПб.: Изд-во СПбГЭУ, 2016. – 97 с.
12. Эксперты осуществили первую успешную атаку поиска коллизий хеш-функций SHA-1, 25.02.2017 [электронный ресурс]. URL: https://www.aktiv-company.ru/press-center/publication/2017-02-25.html (дата обращения: 11.11.2017).
13. Mitsunari Shigeo, Yoshinari Takesako Backdoors with the MS Office file encryption master key and a proposal for a reliable file format, 28.10.2015 [электронный ресурс]. URL: https://www.slideshare.net/codeblue_jp/ backdoors-with-the-ms-office-

file-encryption-master-key-and-a-proposal-for-a-reliable-file-format-by-mitsunari-shigeo-yoshinari-takesako (дата обращения: 11.11.2017).
14. [MS-OFFCRYPTO]: Office Document Cryptography Structure [электронный ресурс]. URL: https://msdn.microsoft.com/ru-ru/library/cc313071.aspx (дата обращения: 11.11.2017).
NIST Special Publication 800-132 Recommendation for Password-Based Key Derivation. Part 1: Storage Applications, December 2010 [электронный ресурс]. URL: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf (дата обращения: 11.11.2017).