УДК 681.3.06:519.248.681

ОСНОВНЫЕ ТРЕБОВАНИЯ К СРЕДСТВАМ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФРАСТРУКТУРАХ ОТКРЫТЫХ КЛЮЧЕЙ

Ю.И. ГОРБЕНКО, В.А. БОБУХ

Обосновываются требования к средствам криптографической защиты информации. Представлены результаты анализа таких аппаратных средств отечественного производства.

Requirements to means of cryptographic information protection are substantiated. Results of analyzing such home-produced hardware are provided.

Анализ существующих источников показал, что наиболее широко и системно требования к средствам КЗИ вообще были определены в линейке федеральных стандартов США FIPS 140-1, FIPS 140-2 и в рабочем проекте FIPS 140-3. Ряд данных и требований относительно средств КЗИ приведено в рабочей версии ISO/IEC 19790 [6]. Из них можно сделать вывод о том, что при построении криптографических систем необходимо обосновывать и выбирать криптографические средства с соответствующим уровнем защищенности, политики их применения, криптографические преобразования и протоколы, протоколы управления и сертификацию ключей и т.п.

В первую очередь необходимо учитывать следующее[1-2, 4-5]:

– насколько важной является информационная система (ИС) или информационно-телекоммуникационная система (ИТС) для решения задач организации;

– в какой мере должны использоваться национальные и международные стандарты;

– какие требования относительно эффективности криптографических механизмов должны быть выполненными (напр., пропускная способность, время обработки, их способность противостоять действиям нарушителей и т.п.);

– какие требования должны быть выполнены относительно внутрисистемной и межсистемной способности и интероперабельности;

– требования относительно криптографических алгоритмов, криптографических протоколов и протоколов связи и т.п.;

– цель и задачи безопасности информации, цель и задачи применения криптографических средств и механизмов;

– какие услуги и по какому профилю должны предоставляться, например целостность, подлинность, конфиденциальность, доступность, наблюдательность, неопровержимость;

– на протяжении какого периода времени информация должна быть защищена;

– какие регламенты и политики должны быть применены;

– в какой мере пользователи осведомлены относительно криптографии и насколько они хорошо научены;

– в чем сущность физической и процедурной инфраструктуры из криптографической защиты информации и данных, напр., сохранение, учет и аудит, материальная и техническая поддержка и т.п.;

– относительно какой информации и данных нужно обеспечить связь с использованием криптографических преобразований и протоколов (в том числе напр., средства и процедуры физической защиты ключевых данных и информации).

Ответы на указанные проблемные вопросы могут быть использованы при формулировании подхода по разработке принципов интеграции криптографических систем и средств в существующие или новые ИС и ИТС, одним из примеров которой является специализированный центр сертификации ключей. Причем обоснованным подходом из интеграции криптографических средств и реализации методов и механизмов, есть разработка требований соответственно с целями и политиками защиты.

1. ТРЕБОВАНИЯ К СРЕДСТВАМ КЗИ ИОК

К средствам КЗИ, что применяются в центрах сертификации ключей разных уровней иерархии, в зависимости от механизмов защиты и уровней защиты, должны быть обеспечены требования международных или региональных стандартов. На наш взгляд, физическое и логическое требования по защите криптографических модулей в наиболее приемлемом виде формулируются в FIPS 140-2 [1], а также в рабочем проекте FIPS 140-3 [2]. При таком подходе криптографические алгоритмы и криптографические модули должны тестироваться перед их внедрением в существующую или новую систему. Криптографические алгоритмы и модули тестируются разработчиком и потом представляются для тестирования в соответствии с нормативными документами, например для тестирования криптографического модуля можно использовать федеральный стандарт США FIPS 140-2. Так, проведенный анализ показал, что в США для всех государственных ведомств для защиты конфиденциальной незасекреченной информации обязательным есть использования криптографических средств, которые отвечают стандарту FIPS 140-2, если эти организации считают, что такая

криптографическая защита необходима. Причем стандарт FIPS 140-2 необходимо применять в компьютерных и телекоммуникационных системах при проектировании, создании, тестировании и применении систем безопасности на базе использования криптографических преобразований. Кроме того, национальный институт стандартизации США (NIST) и Организация по Коммуникационной Безопасности (CSE) правительства Канады основали специальную программу CMVP. Цель этой программы – обеспечить государственные организации метрическими свидетельствами безопасности для использования при поставках оборудования, которое содержит криптографические модули. Результаты независимого тестирования обеспечиваются аккредитованными лабораториями. Аттестационное тестирование криптографических модулей выполняется с использованием производных требований тестирования (DTR) для FIPS 140-2. В DTR перечислены все требования к поставщику и организации, которая осуществляет тестирование криптографических модулей. Согласно приведенным нормативным документам криптографический модуль представляет собой набор аппаратных средств, программного обеспечения или микропрограммных (программно-аппаратных) средств, или некоторой их комбинации, которые реализуют криптографическую логику или криптографические преобразования. Примерами криптографических модулей могут быть: такие автономные устройства, как аппаратуры шифрования; включая платы шифрования, которые встраиваются в компьютерные системы; прикладные программы, которые выполняются на микропроцессорах; программы и средства цифровой подписи и т.п. Если криптографические преобразования реализованы в виде программного обеспечения, то процессор, который использует программное обеспечение, также является частью криптографического модуля.

В целом анализ состояния разработки и внедрение FIPS 140-3 показал, что в связи со сложностью, процесс разработки федерального стандарта FIPS 140-3 продлевается, в нем принимает участие широкий круг специалистов, заказчиков и заинтересованных организаций и лиц. В табл. 1 приведены требования к модулям криптографической защиты на национальном уровне, которые разработаны с учетом рабочей версии FIPS140-3[2].

Таблица 1

Требования к модулям КЗИ специализированных центров

	Уровень Защиты 1	Уровень Защиты 2	Уровень Защиты 3	Уровень Защиты 4	Уровень Защиты 5
1. Описание Криптографического Модуля	Описание модуля, границ, Утвержденных алгоритмов и Утвержденных режимов действия. Описание аппаратных средств и программного обеспечения модуля. Документация модуля				
	Политика Защиты определяет Утвержденный режим действия	Указание Утвержденного режима действия модуля			
2. Порты и Интерфейсы Криптографического Модуля	Нужные и Опциональные Интерфейсы. Определение всех интерфейсов и всех входных и выходных путей данных	Ввод и вывод критических параметров защиты физически или логически отделенных с использованием доверенного канала от других портов и интерфейсов			
3. Роли, Услуги и Аутентификация	Определение ролей и услуг модуля	Аутентификация, основанная на роли или идентификации	Аутентификация, основанная на идентификации оператора	Двухфакторная Аутентификация	
4. Защита Программного Обеспечения	Исполнительный код, Утвержденный метод проверки целостности, MSI, ограничение по чтению и модификации, обнуление при разгрузке, проверка формата	Тестирование целостности, основанное на цифровой подписи	MSI команда для инициализации тестирования целостности программного обеспечения. Обнуление хеш-значения	Шифрование и расшифровка CSP параметров и кода тестирования целостности	Шифрование и расшифровка PSP параметров и кода тестирования целостности
5. Операционная среда	OS одного пользователя или разграничительный контроль доступа	Механизмы контроля. Разграничительный контроль доступа	Криптографическое программное обеспечение, SSP и защита данных аудита. Доверенный канал. Расширенный аудит	Требования расширенного аудита	

Продолжение табл. 1

<table>
<tr><td>6. Физическая Защита</td><td>Промышленные компоненты</td><td>Доказательство вмешательства. Непрозрачное покрытие или корпус</td><td>Схема реагирования на вмешательство и обнуление на съемных крышках и дверце. Защита вентиляции от зондирования. Крепкое покрытие или корпус</td><td>EFP или EFT для температуры и напряжения. Схема выявления вмешательства и обнуление для многокристальных модулей</td><td>EFP для температуры и напряжения. Непрозрачное для невизуальной радиационной экспертизы. Защита от отключения схемы выявления вмешательства и обнуление</td></tr>
<tr><td>7. Неинвазивные Атаки Физической Защиты</td><td colspan="2">Никаких дополнительных требований</td><td>Защита CSP параметров от атак временного анализа</td><td>Защита CSP параметров от SPA и DPA атак</td><td>Защита CSP параметров от EME атак</td></tr>
<tr><td rowspan="2">8. SSP Управление</td><td colspan="5">Требования для генераторов случайных бит, генерации SSP, установление SSP, введение и вывода SSP, хранение SSP и обнуление CSP</td></tr>
<tr><td colspan="2">Неэлектронно транспортируемые SSP могут вводиться и выводиться в открытой форме</td><td>Неэлектронно транспортируемые SSP, введенные или выведенные в зашифрованной форме или с использованием процедур раздела знания</td><td colspan="2">Обнуление PSP</td></tr>
<tr><td>9. Самотестирование</td><td colspan="5">Передэксплуатационное самотестирование: тестирование целостности программного обеспечения, тестирование криптографического алгоритма, и передэксплуатационное тестирование обхода. Условное самотестирование: тестирование парной согласованности, тестирование нагрузки программного обеспечения, тестирование ручного ввода ключей, беспрерывное RBG тестирование, тестирование источника RBG энтропии и тестирование условного обхода</td></tr>
<tr><td rowspan="7">10. Гарантия Жизненного Цикла (CMS) (Проектирование) (FSM) (Разработка) - (Тестирование Поставщика) (Доставка и Оператор) (Управляющая Документация)</td><td colspan="3">CMS для модуля, компонентов и документации. Каждый уникально идентифицированный и отслеженный на протяжении всего жизненного цикла</td><td colspan="2">Автоматизированная CMS</td></tr>
<tr><td>Соответствие между модулем и Политикой Защиты</td><td>Функциональная Спецификация</td><td>Детальное проектирование</td><td>Неформальное доказательство соответствия между перед- и постусловиями и функциональной спецификацией</td><td>Формальное моделирование и неформальное доказательство соответствия между формальной моделью и функциональной спецификацией</td></tr>
<tr><td colspan="5">Модель Конечного состояния</td></tr>
<tr><td>Аннотированный начальный код, схематика или HDL язык</td><td colspan="4">Высокоуровневый язык программного обеспечения. Высокоуровневый язык аппаратного описания</td></tr>
<tr><td>Функциональное Тестирование</td><td colspan="4">Низкоуровневое Тестирование.</td></tr>
<tr><td>Процедуры Запуска</td><td>Процедуры Поставки</td><td colspan="3">Аутентификация оператора с использованием обеспеченной поставщиком информации аутентификации</td></tr>
<tr><td colspan="5">Руководство администратора и не администратора</td></tr>
<tr><td>11. Противодействие Другим Атакам</td><td colspan="5">Никаких механизмов противодействия не указано в Политике Защиты</td></tr>
</table>

Необходимо отметить, что требования применения в ЦСК аппаратных модулей КЗИ есть взаимно признанными и закрепленными в соответствующих Политиках сертификации. Так Политика Сертификации (СР) мостового центра США[3] определяет семь политик сертификации. Политики представляют пять разных уровней гарантии (Рудиментарный, Базовый, Средний, Средний Аппаратный и Высокий) для сертификатов открытого ключа. Понятие уровня гарантии относится к стойкости связи между открытым ключом и лицом, субъектное имя которого упоминается в сертификате, к механизмам, которые используются для руководства использованием личного ключа и защиты, которая обеспечивается самим PKI. Суть в том, что высокий уровень гарантий обеспечивается, во-первых, за все за счет выполнения требований к средствам КЗИ, что применяются в соответствующих ЦСК.

2. ТРЕБОВАНИЯ К ОТДЕЛЬНЫМ ТЕХНИЧЕСКИМ СРЕДСТВАМ ИОК

Состав и характеристики отдельных технических средств, которые входят в состав комплекса, и требования и характеристики программного обеспечения соответствующих средств, приведены в табл. 2.

В состав всех технических средств должны входить источники бесперебойного питания (ИБП).

В состав сервера ЦСК должен входить аппаратный модуль подписи (АМП), которая предназначен для:

– управления личным ключом ЦСК (генерации, хранения, ввода, использования, резервного копирования, восстановления и уничтожения);

– формирования ЭЦП с использованием личного ключа ЦСК.

В состав средств РС генерации ключей пользователей должен входить аппаратный генератор случайных чисел (АГСЧ), который предназначен для генерации последовательностей случайных чисел при генерации ключевых данных программными комплексами.

В состав сервера сертификации-регистрации должен входить устройство записи на оптические диски, который предназначен для записи на диски резервных копий данных и создание долгосрочных архивов.

3. СПЕЦИАЛЬНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА ДЛЯ ИОК

3.1. Аппаратный генератор случайных чисел «Гряда-3»

Аппаратный генератор случайных чисел «Гряда-3 (или другой генератор подобного типа) предназначен для аппаратной генерации последовательностей случайных чисел на основе физических датчиков шума во время генерации ключевых данных и параметров, которые должны формироваться случайно. Аппаратный модуль используется в программном комплексе генерации ключей пользователей.

Внешний вид генератора «Гряда-3» приведено на рис. 1.

Рис. 1. «Гряда-3»

3.2. Аппаратный модуль подписи «Гряда-41П»

Аппаратный модуль подписи «Гряда-41Г» или другой модуль КЗИ такого же класса предназначен для аппаратной реализации формирования ЭЦП и обеспечивает использование и защиту личного ключа ЦСК. Личный ключ ЦСК генерируется, сохраняется и используется только в середине модуля в защищенном виде.

Таблица 2

Состав и характеристики отдельных технических средств

Техническое средство	Тип и характеристика	Специальные технические (аппаратные) средства	Системное программное обеспечение	Специальное программное обеспечение
РС сертификации-регистрации	ПЭВМ	Съёмный криптографический модуль	ОС	Программные компоненты работы с криптографическим модулем. Программный комплекс РС сертификации-регистрации
Сервер сертификации-регистрации	ЭВМ серверного типа	Устройство записи на оптические диски. Аппаратный модуль подписи	ОС серверного типа. СУБД	Программные компоненты работы с АМП. Программный комплекс сервера сертификации-регистрации
РС генерации ключей пользователей	ПЕОМ	Аппаратный генератор случайных чисел	ОС	Программные компоненты работы с АГВЧ. Программный комплекс РС генерации ключей пользователей

Внешний вид модуль приведен на рис. 2.

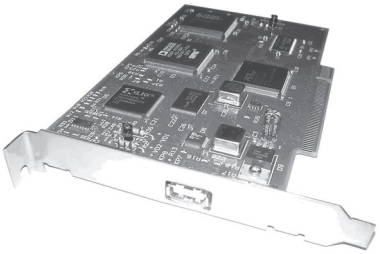

Рис. 2. «Гряда-41Г»

Модуль должен выполнять как минимум такие функции:

– управление личным ключом ЕЦП, что включает:

– прием и хранения общих параметров для алгоритма ЭЦП;

– генерацию личного ключа ЭЦП с использованием алгоритма генерации случайных битовых последовательностей и встроенного аппаратного ГСЧ;

– хранение личного ключа ЭЦП в зашифрованном виде;

– запись личного ключа ЭЦП на внешний носителя ключевой информации (НКИ) в защищенном виде (резервное копирование личного ключа ЭЦП);

– считывание личного ключа ЕЦП с внешнего НКІ и запись в АМП (восстановление личного ключа ЕЦП);

– уничтожение личного ключа ЕЦП в АМП и на внешнему НКІ;

– формирование ЭЦП от данных, которые загружаются из ПЭВМ, с использованием личного ключа ЭЦП;

– аутентификацию пользователей для работы в разных режимах соответственно функциональным ролям пользователей с использованием симметричной схемы аутентификации;

– управление параметрами аутентификации пользователей, которое включает:

– добавление и изменение данных автентификации пользователей АМП;

– удаление данных автентификации пользователей АМП.

3.3. Криптографический модуль «Гряда-61»

Криптографический модуль предназначен для аппаратной реализации криптографических преобразований в составе программного комплекса сертификации-регистрации.

Внешний вид модуль приведен на рис. 3.

Рис. 3. «Гряда – 61»

Модуль «Гряда-61» как минимум выполняет следующие функции:

– аутентификацию оператора ЭВМ при доступе к модулю;

– генерацию личных и открытых ключей для алгоритма ЭЦП и протокола распределения ключей;

– генерацию ключей для алгоритма шифрования и генерацию случайных последовательностей на основе аппаратного генератора;

– хранение личных ключей во внутренней памяти и защиту их от НСД;

– вычисление хеш-функции, формирование и проверку ЭЦП;

– распределение ключевых данных на основе асимметричного протокола распределения и шифрование данных;

– контроль целостности и работоспособности встроенного программного обеспечения и др.

4. ПРОГРАММНО-ТЕХНИЧЕСКИЙ КОМПЛЕКС ПОЛЬЗОВАТЕЛЯ

4.1. Программный комплекс специального пользователя ЦСК

Программный комплекс пользователя ЦСК должен реализовывать функции генерации и управление ключами пользователей, а также механизмы ЭЦП и шифрование данных.

Программный комплекс пользователя ЦСК должен выполнять такие функции:

– генерацию личного и открытого ключей пользователя;

– формирование и передачу запроса на формирование сертификата пользователя к ЦСК;

– получение, проверку, хранение и использование сформированного сертификата;

– формирование и передачу запросов на блокирование, отмена и возобновление сертификата пользователя к ЦСК;

– введение и использование личных ключей пользователя;

– обеспечение использования пользователем сертификатов и списков отозванных сертификатов;

– формирование и проверка ЭЦП, а также шифрование данных пользователя в системах электронной почты, электронного документооборота и т.п.

4.2. Электронный ключ «Кристалл-1»

В составе программного обеспечения пользователей ЦСК может использоваться аппаратный электронный ключ.

Конструктивно электронный ключ типа «Кристалл-1» выполнено в виде брелка с интерфейсом USB для подключения к ЭВМ.

Внешний вид электронного ключа в пластмассовом корпусе приведено на рис. 4.

Электронный ключ предназначен для аппаратной реализации всех криптографических преобразований, которые выполняются пользователем. Аппаратная реализация обеспечивает защищенность

процесса выполнения криптографических преобразований и делает невозможным доступ к личным ключам со стороны программной среды ЭВМ.

Рис. 4. «Кристалл – 1»

Устройство должно выполнять следующие функции:

– аутентификацию оператора ЭВМ при доступе к ключу;

– генерацию личных и открытых ключей для алгоритма ЭЦП и протокола распределения ключей;

– генерацию ключей для алгоритма шифрования и генерацию случайных последовательностей на основе аппаратного генератора;

– хранение личных ключей во внутренней памяти и защиту их от НСД;

– вычисление хеш-функции;

– формирование и проверка ЭЦП;

– шифрование данных;

– распределение ключевых данных на основе асимметрического протокола распределения;

– хранение произвольных данных во внутренней памяти и защита их от НСД;

– контроль целостности и трудоспособности встроенного программного обеспечения и др.

5. ТРЕБОВАНИЯ К СПЕЦИАЛЬНЫМ ХАРАКТЕРИСТИКАМ ПРОГРАММНЫХ И АППАРАТНЫХ СРЕДСТВ ЦСК

В программных и аппаратных средствах ЦСК в качестве носителей ключевой информации при соответствующем обосновании могут использоваться такие носители информации:

– гибкие диски 3,5”, электронные диски с внутренним ПЗУ;

– компакт-диски (CD-R, CD-RW, DVD-R или DVD-RW);

– электронные ключи ИИТ Кристалл;

– электронные ключи Aladdin eToken R2, PRO;

– электронные ключи Актив ruToken.

– электронные ключи Технотрейд uaToken.

– электронные ключи Автор Secure EToken и др.

В программных и аппаратных средствах ЦСК должны быть реализованы такие криптографические алгоритмы и протоколы:

– алгоритм шифрования согласно ГОСТ 28147-89 (режим простой замены, режим сдерживания и режим изготовления имитовставки) или другой алгоритм, который разрешен к использованию;

– алгоритм ЭЦП согласно ДСТУ 4145-2002;

– хеш-функция согласно ГОСТ 34.311-95;

– протокол распределения ключевых данных Диффи – Хелмана в группе точек эллиптической кривой или другой согласованный протокол;

– могут также использоваться другие криптоалгоритмы ЭЦП и хеширования или протоколы, если они разрешены к использованию в установленном порядке.

Методика распределения ключевых данных на основе протокола Диффи-Хелмана в группе точек эллиптической кривой должна быть согласована с ГСССЗИ Украины (Госспецсвязи) и должна быть согласованной с ДСТУ ISO/ IEC 15946 – 3:2006.

Форматы ключевых данных и другой специальной информации должны отвечать требованиям международных стандартов, рекомендаций и действующих национальных нормативных документов.

Параметры криптографических алгоритмов и протоколов (параметры эллиптических кривых и долгосрочные ключевые элементы (ДКЭ)) должны быть сменными.

Литература.

[1] Federal Information Processing Standards Publication (FIPS PUB) 140-2. Security requirements for cryptographic modules. NIST, 1999.

[2] National Institute of Standards and Technology, FIPS 140-3(DRAFT), Security for cryptographis modules. : http://www.nist.gov/cmvp.

[3] X.509 Certificate Policy for the FederalBridgeCertificatio nAuthority (FBCA). V. 1.06.2000.

[4] NISTspecialPublication800-56A. Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography. March, 2006.

[5] NIST special Publication 800-57 Draft. Recommendation for Key Management-Part 2: Best Pracnices for Key Manageme Jrganizationsnt. April, 2005.

[6] ISO/IEC FCD 19790: Information technology- Security requirements for cryptographicmodules. Proect:1.27.40.

Поступила в редколлегию 9.09.2008

Горбенко Юрий Иванович, кандидат технических наук, технический директор ЗАО «ИИТ», научный сотрудник НИЦ «Z» каф. БИТ ХНУРЭ. Область научных интересов: защита информации в информационно-телекоммуникационных системах.

Бобух Всеволод Анатольевич, начальник отдела аппаратных средств защиты информации ЗАО «ИИТ», младший научный сотрудник каф. БИТ, кандидат технических наук. Область научных интересов: аппаратные средства систем защиты информации.