УДК 004.383

ПЕРСПЕКТИВЫ РАЗВИТИЯ НОСИТЕЛЕЙ КЛЮЧЕВОЙ ИНФОРМАЦИИ ДЛЯ СИСТЕМ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В УКРАИНЕ

А.В. Карпов
ООО «АВТОР»
e-mail: Andrey.Karpov@author.kiev.ua

Носители ключевой информации (НКИ) представляют собой программные или аппаратно-программные средства, предназначенные для хранения ключевых данных пользователей, с помощью которых осуществляется формирование и проверка электронной цифровой подписи (ЭЦП), шифрование данных, а также аутентификация.

На сегодняшний день проблема защиты личной ключевой информации является актуальной, так как ее компрометация может привести к фальсификации, краже информации, а также к несанкционированному доступу к приложениям пользователя.

Наибольшего распространения в системе ЭЦП Украины получили следующие типы носителей ключевой информации: файловые носители, смарт-карты и электронные ключи.

Файловые носители являются программными носителями. Ключевые данные пользователей хранятся в виде файлов операционной системы на жестком диске, дискетах или флэш-памяти. Такие носители являются очень дешевыми (фактически – по себестоимости запоминающего устройства), однако и очень ненадежными: защита файловых носителей требует очень точных и сложных организационных процедур, которые должны соблюдать пользователи, следовательно, на систему защиты сильно влияет человеческий фактор. Выполнение криптографических операций с ключевыми данными производится в незащищенной среде – оперативной памяти операционной системы, организовать защиту которой от несанкционированного доступа достаточно сложно.

Смарт-карты – специализированные многофункциональные устройства. В задачах защиты информации используются для хранения и выполнения криптографических преобразований над ключевыми данными. Основой смарт-карт является смарт-чип, который имеет собственную операционную систему обеспечивающую контроль над работой аппаратной части и выполнение криптографических преобразования в защищенной среде. Следует, однако, различать системы информационной безопасности, использующие активные НКИ (смарт-карты самостоятельно выполняют криптографические преобразования) и пассивные НКИ (смарт-карты используются только в качестве хранилища ключей, а криптографические преобразования выполняются программно). Понятно, что для задач обеспечения информационной безопасности эффективно использовать именно активные НКИ.

Работа со смарт-картами происходит через карт-ридеры, которые является стандартизированным устройством (т.е. несовместимости реализаций не возникает). Протоколы работы со смарт-картами описаны стандартами ISO и поддерживаются всеми существующими операционными системами.

По интерфейсам доступа смарт-карты делятся на контактные и бесконтактные. Контактные карты для работы требуют постоянного физического контакта чипа со считывающим устройством – карт-ридером. Бесконтактные карточки могут взаимодействовать с карт-ридерами на расстоянии до 10 см. Контактные смарт-карты

дешевле и более приспособлены к выполнению длительных криптографических операций, однако бесконтактные значительно проще в использовании, в частности, в задачах аутентификации. Для сочетания преимуществ обоих типов были созданы гибридные смарт-карты, объединяющие два чипа с различными интерфейсами доступа и дуальные смарт-карты, несущие один чип, но предоставляющие оба интерфейса доступа к нему.

Электронные ключи – носители ключевой информации, работающие через интерфейс USB. Фактически электронный ключ является карт-ридером с вставленной смарт-картой, выполненной в компактной форме «флешки», поэтому он предоставляет все преимущества контактной активной смарт-карты, является удобным в использовании, но дороже, чем смарт-карты. Именно ценовая разница устанавливает предел эффективности. Электронные ключи следует использовать вместо смарт-карт в тех системах, в которых сложно оснастить каждый терминал соответствующим карт-ридером – например, в виртуальных частных сетях, где терминалом может быть любой компьютер, подключенный к сети Интернет.

На сегодняшний день большинство НКИ работают в пассивном режиме и в полной мере не защищают от потери секретной информации, так как закрытые ключи извлекаются из НКИ во время работы. Решением данной проблемы является использование активных НКИ с неизвлекаемым закрытым ключом. Примером НКИ данного типа являются смарт-карты CryptoCard-337 и электронные ключи SecureToken-337 производства компании «АВТОР», обеспечивающие выполнение криптографических преобразований в активном режиме и реализующие дополнительные функции информационной безопасности благодаря использованию аппаратных средств смарт-чипа.

Данные НКИ выполнены на базе смарт-чипов компании NXP Semiconductors P5CC037 и обладают идентичными возможностями.

Смарт-чип имеет несколько уровней защиты от несанкционированного доступа к сохраненной в нем информации: аппаратный, технологический и программный.

Аппаратный уровень защиты от несанкционированного доступа поддерживается ресурсом смарт-чипа P5CC037. Для этого в нем реализуются специальные датчики, устройства и элементы:

- детекторы пониженного и повышенного напряжения питания, тактовой частоты и температуры;
- стирание области RAM при сбросе или срабатывании датчиков;
- защита от высокочастотных помех;
- генераторы случайных чисел и тактов ожидания;
- скремблирование внутренних шин, шифрования RAM и EEPROM;
- аппаратная защита чтения областей ROM, EEPROM;
- уникальный идентификационный номер кристалла;
- защита от накопления статистических данных по энергопотреблению и времени выполнения команд;
- самотестирование структуры чипа;
- защита от подключений зондами.

На разных стадиях производства смарт-чипов применяются технологические приемы, которые затрудняют воссоздание структуры чипа и получение тайной информации. Создаются многослойные структуры кристаллов, ответственные части схемы (блоки шифрования памяти, сопроцессоры) размещаются внутри, создаются

дополнительные слои металлизации. Данные мероприятия защищают чип от оптического и электронного сканирования, обеспечивают его разрушение при послойном спиливании.

Программный уровень защиты реализуется средствами операционной системы (ОС) «УкрКОС 3.0». Гарантированный уровень безопасности ОС «УкрКОС 3.0» обеспечивается благодаря разделению ядра системы и разных приложений, которые в свою очередь работают независимо друг от друга, имея персональные механизмы защиты. Все операции выполняются в защищенной памяти смарт-чипа. В ОС «УкрКОС 3.0» не существует команды, которая позволяет извлекать тайный ключ из памяти смарт-чипа, что подтверждает активный режим работы НКИ и обеспечивает высокий уровень информационной безопасности.

На сегодняшний день в коммерческих структурах зачастую используются международные криптографические алгоритмы для обеспечения информационной безопасности, в государственных – национальные, а в банковских – и те и другие. В связи с этим возникла необходимость одновременной реализации как национальных криптоалгоритмов, так и международных на одном НКИ. Перспективные носители ключевой информации, для обеспечения данной потребности, должны выполнять:

- генерацию ключевых данных и формирование ЭЦП в соответствии с ДСТУ 4145-2002 с длиной ключа – 163-509 бит;
- шифрование/расшифрование данных в соответствии с ДСТУ ГОСТ 28147:2009;
- вычисление хеш-функции в соответствии с ГОСТ 34.311-95;
- генерацию случайной битовой последовательности;
- генерацию личных ключевых данных и формирование ЭЦП в соответствии с PKCS#1 RSA Cryptography Standard, с длиной ключа 512-2048 бит;
- шифрование/расшифрование сообщений в соответствии с PKCS#1 RSA Cryptography Standard, с длиной ключа 512-2048 бит;
- хранение до 10 личных ключей.

В таблице 1 приведены скоростные характеристики формирования ЭЦП современными носителями ключевой информации в соответствии с национальными и международными стандартами.

Таблица 1

Название стандарта	Длина ключа, бит	Время формирования ЭЦП, мс
ДСТУ 4145-2002	191	30
	257	50
	509	185
PKCS#1 RSA Cryptography Standard	1024	300
	1536	1000
	2048	2000

Одними из перспективных решений развития НКИ является использование Smart-MicroSD и средств защищенной визуализации подписываемых данных.

Smart-MicroSD - это специальная флешь-память в формате microSD со встроенным дополнительным смарт-чипом для выполнения криптографических операций. Smart-MicroSD имеет такие же свойства, как смарт-карты и электронные ключи предоставляя

возможность осуществления криптографических операций с мобильных устройств (смартфонов, планшетов и т.д.).

Средства защищенной визуализации подписываемых данных представляют собой считыватель смарт-карт, позволяющий визуально контролировать содержание передаваемых на подпись в смарт-карту данных, путем вывода их на дисплей. Данные средства не позволяют подписать документ до тех пор, пока не будет нажата кнопка подтверждения операции подписи. Данные устройства чаще всего применяются в банковской сфере, так как могут вывести основные реквизиты финансовой операции на экран, а отобразить содержимое большого электронного документа в понятном для пользователя формате – проблематично.

На сегодняшний день активные НКИ в различных форм-факторах начинают широко применятся в системах клиент-банк, Интернет-банкинга, внешнего и внутреннего электронного документооборота, аутентификации, а также электронного правительства в качестве электронного удостоверения личности.

Исходя из вышесказанного, приведем основные перспективные тенденции развития носителей ключевой информации для систем ЭЦП в Украине:

- обеспечение активного режима выполнения криптографических преобразований;
- одновременная реализация как национальных, так и международных криптографических алгоритмов;
- применение Smart-MicroSD для обеспечения выполнения криптографических операций с мобильных устройств;
- применение средств защищенной визуализации подписываемых данных при выполнении финансовых операций.