КОМПЬЮТЕР МОЖЕТ БЫТЬ ЛЮБЫМ

С компьютером сегодня связано так много сторон нашей ежедневной деятельности, что желание оснастить его так, чтобы было *все*, и все было *под рукой и удобно* – вполне понятно. По мере увеличения темпа жизни все меньше хочется тратить время на переоборудование, требующее отвертки и хотя бы минимальных специальных умений. Поэтому неудивительно, что возможность подключения через интерфейс USB существенно повышает шансы на успех любого устройства. Через этот интерфейс сегодня можно подключать не только привычные мышь, клавиатуру, и флеш-память, но и довольно экзотичные вещи типа USB-подогревателей, USB-вентиляторов с подсветкой и многого другого, не менее удивительного, без чего, наверняка, просто невозможно обойтись.

С другой стороны, по мере внедрения современных информационных технологий во всех сферах жизни человека, все большее значение приобретает возможность сочетания таких важных качеств, как *мобильность и защищенность* – в одном техническом устройстве.

Понимание этих тенденций производителями средств защиты информации заставило их направить свои усилия на разработку мобильных средств аутентификации – в форм-факторе USB-ключ. Отдавая себе отчет, что этого не достаточно для того, чтобы сделать персональную информационную среду мобильной и защищенной одновременно, мы создали **Персональное средство криптографической защиты информации (ПСКЗИ) ШИПКА™[1] (Шифрование, Идентификация, Подпись, Коды Аутентификации)**.

НЕБОЛЬШОЕ ВВЕДЕНИЕ С УКЛОНОМ В КЛАССИФИКАЦИЮ

Средства защиты информации в форм-факторе USB-ключ бывают довольно разные, но достаточно легко группируются в три класса: изделия типа HASP, USB-токены (аналоги смарт-карт) и ПСКЗИ (персональные средства криптографической защиты информации).

1. Изделия типа HASP

HASP – это аббревиатура, она расшифровывается как Hardware Against Software Piracy. То есть это система защиты программ и данных от нелегального использования и несанкционированного распространения. Механизм ее использования примерно такой – в комплект поставки ПО помимо собственно ПО на том или ином носителе входит также USB-ключ, необходимый для того, чтобы подтвердить легальность копии – без этого ключа ПО работать не будет.

Логика этого метода защиты очевидна и правильна: купил ПО – а стало быть, является его владельцем – человек, а не компьютер, соответственно возможность легального использования этого ПО должна быть связана именно с определенным владельцем, а не с определенным компьютером.

Наличие такого изделия в линейке продуктов, безусловно, очень выгодно производителю, поскольку тиражи его продаж могут быть очень велики.

2. USB-токены

USB-токены являются аналогами смарт-карт не только в функциональном, но и в буквальном – технологическом смысле. Это USB-устройство, построенное на смарт-карточном кристалле. И именно это определяет их функциональную идентичность, поскольку функциональность смарт-карты строго ограничена возможностями ее микросхемы. Этих возможностей вполне достаточно для того, чтобы реализовать различные процедуры аутентификации – в том числе, для аутентификации с использованием криптографических алгоритмов – ЭЦП или шифрования. Такие изделия могут применяться для аутентификации при локальном входе в компьютер, входе в домен Windows, для шифрования или подписи сообщений электронной почты, получения сертификатов подписи – для использования пространства PKI.

3. ПСКЗИ

ПСКЗИ – это аббревиатура, расшифровывающаяся как Персональное Средство Криптографической Защиты Информации. Характеристика ПСКЗИ, являющаяся принципиальной, – это широта и гибкость функциональности

изделия. Для того чтобы обладать такими свойствами, устройство должно иметь архитектуру, обеспечивающую не просто большой потенциал, но и возможность наращивания ресурсов, а также быть перепрограммируемым. В общем случае оба эти требования могут быть выполнены при использовании **микропроцессора**, а не смарт-карточной микросхемы.

Таким образом, USB-устройства для защиты информации делятся на группы с совершенно разной функциональностью, а значит, для того, чтобы не оказаться в ситуации сложного выбора, потенциальному пользователю достаточно просто более менее точно понимать, для каких целей он выбирает устройство.

ТРЕБОВАНИЕ ВРЕМЕНИ: ПСКЗИ ШИПКА

Поскольку криптографические преобразования – шифрование и ЭЦП – признаются единственным надежным способом защиты информации, передаваемой по каналам связи, пристальное внимание к средствам защиты информации, имеющим **криптографические функции** совершенно естественно как со стороны рынка, так и со стороны государства. А возрастающее значение мобильности в современном мире придает особую привлекательность **персональным** средствам. Однако необходимо учитывать, что использование дешевых непроверенных

и ненадежных средств влечет за собой подчас худшие последствия, чем не использование средств защиты вообще, потому что к незащищенности добавляется безосновательная успокоенность.

Базовым элементом ПСКЗИ семейства ШИПКА является микропроцессор, имеющий собственную энергонезависимую память. Кроме того, ПСКЗИ ШИПКА снабжено аппаратным датчиком случайных чисел (ДСЧ) и внешней памятью (data flash).

Взаимодействие ПСКЗИ ШИПКА и персонального компьютера может быть организовано через **различные интерфейсы** (существуют реализации устройства, снабженные контроллером USB – **ШИПКА-1.5**, **ШИПКА-1.6** и **ШИПКА-1.7**, устройство **ШИПКА-CF** может обрабатывать данные, передаваемые через интерфейс compact flash, **ШИПКА-Express** и **ШИПКА-Cardbus**, соответственно, ExpressCard или PCCARD/CardBus, а **ШИПКА-Модуль** общается с ПЭВМ через I2C и UART).

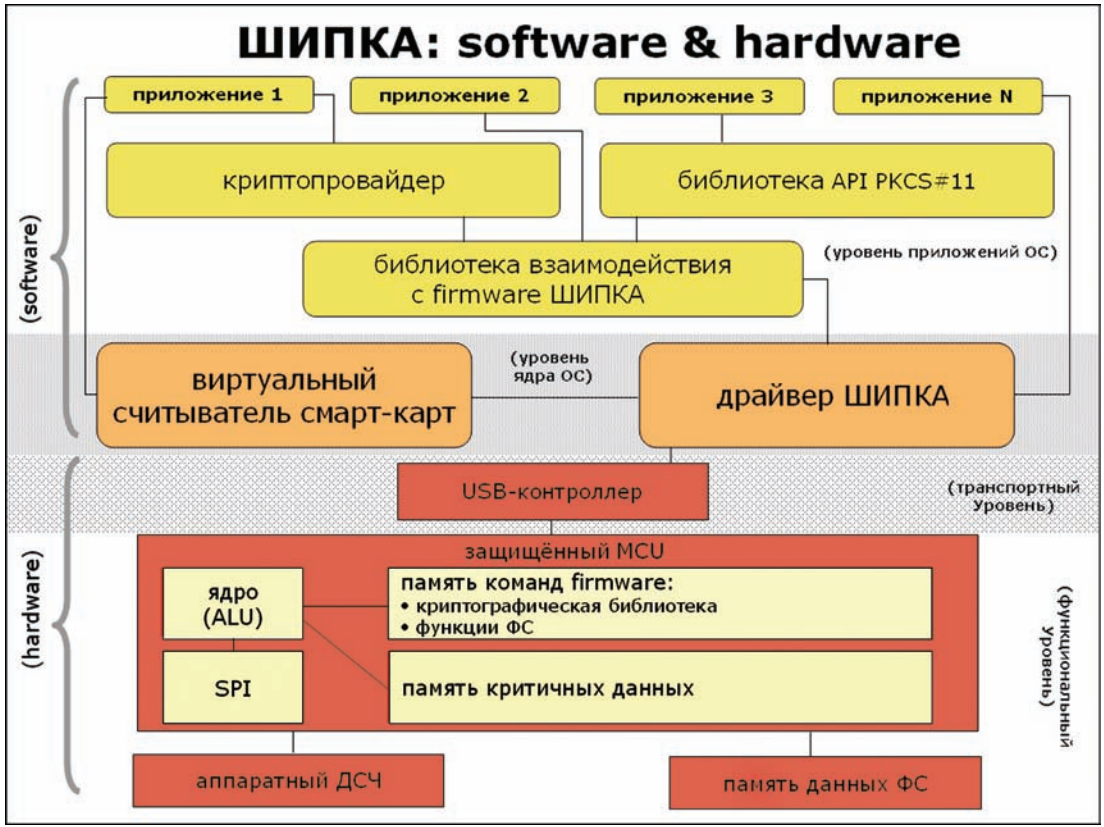
Микропроцессор может выполнять различные **операции общего назначения** (в том числе и криптографические).

В **энергонезависимой памяти** процессора можно надежно **хранить данные** (ключи защиты файловой системы, пароли доступа к ключам).

ДСЧ позволяет получать **качественные последовательности случайных чисел** (что очень важно при генерации ключей).

В **data flash** можно хранить **большие объемы данных** (файлы или ключи, защищенные на ключах защиты файловой системы).

Транспортный интерфейс позволяет **обмениваться командами и данным**и с ПЭВМ.


ШИПКА: software & hardware
приложение 1
приложение 2
приложение 3
приложение N
криптопровайдер
библиотека API PKCS#11
библиотека взаимодействия
с firmware ШИПКА
(уровень приложений ОС)
(software)
виртуальный
считыватель смарт-карт
(уровень
ядра ОС)
драйвер ШИПКА
USB-контроллер
(транспортный
Уровень)
защищённый MCU
ядро
(ALU)
память команд firmware:
• криптографическая библиотека
• функции ФС
SPI
память критичных данных
(hardware)
(функциональный
уровень)
аппаратный ДСЧ
память данных ФС

Задачи, которые можно решать с помощью ПСКЗИ ШИПКА разных версий, можно разделить на три большие группы:

1. создание защищенной и одновременно мобильной персональной информационной среды и защита информационного взаимодействия граждан и организаций,

2. создание корпоративных систем защищенного электронного документооборота разного уровня сложности, внедрения и использования ЭЦП и работа с Удостоверяющими центрами и пространством PKI,

3. разработка специализированных приборов и устройств, включающих криптографическую подсистему.

1. ПЕРВАЯ ГРУППА ЗАДАЧ

К задачам первой группы относятся, в частности, следующие:

- шифрование и/или подпись файлов;
- автоматическое заполнение веб-форм и хранение необходимых для этого данных, в том числе паролей;
- аппаратная идентификация и аутентификация пользователя на ПК и ноутбуках, а также в терминальных решениях типа «тонкий клиент»;
- защищенное хранилище ключей шифрования и подписи и аппаратный датчик случайных чисел;
- авторизация при входе в домены;
- шифрование и подпись сообщений электронной почты с использованием различных стандартов;
- защита информационных технологий с помощью защитных кодов аутентификации.

2. ВТОРАЯ ГРУППА ЗАДАЧ

Архитектура ПСКЗИ ШИПКА такова, что доступ к информации имеет только владелец, но правила доступа к устройству задает администратор в соответствии с корпоративными документами, что позволяет правильно использовать *персональное* средство защиты информации в *корпоративной* среде.

Помимо организации с помощью ШИПКИ доступа к тем или иным приложениям и прочей функциональности стандартных смарт-карт, ПСКЗИ ШИПКА может применяться для **обеспечения подтверждения авторства и целостности электронных сообщений и документов в ЛВС или при использовании технологий терминального доступа**, потому что

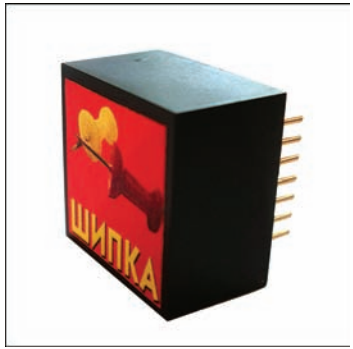
- **ключевая информация**, ассоциированная с пользователем, и **программное обеспечение**, выполняющее криптографические преобразования, **сосредоточены в одном устройстве**, доступны на исполнение **только авторизованному пользователю** и **технологически защищены** от чтения и модификации;
- **собственные ресурсы устройства** (возможность получения аппаратной случайной последовательности, возможность хранения собственного секретного и открытого ключа, возможность хранения отрытого ключа терминального сервера, а также возможность вычисления и проверки ЭЦП) **достаточны для организации защиты виртуальных каналов**.

При этом, что очень важно, внутреннее ПО ПСКЗИ ШИПКА **не нуждается в адаптации для терминального либо локального использования**.

Поддержка **стандартных интерфейсов** (**криптопровайдера и PKCS#11**), позволяет **комфортно работать с ПО различных производителей без дополнительной настройки процедур взаимодействия** с внутренним ПО ПСКЗИ ШИПКА.

Это важно, поскольку корпоративная система информационного взаимодействия не может строиться по шаблону – она должна решать задачи, стоящие перед данной организацией, а они могут быть связаны с использованием самых разных приложений.

3. ТРЕТЬЯ ГРУППА ЗАДАЧ



По мере движения к информационному обществу в самых разных сферах жизни применяется все большее число электронных устройств бытового и промышленного назначения, в которые в определенных обстоятельствах может быть нужно **встроить поддержку криптографических функций**.

Очень часто эти устройства или какие-либо их узлы в той или иной степени представляют собой микрокомпьютер, однако в таких решениях обычно не применяются интерфейсы для расширения типа PCI, PCI-Express и т. п., а используются шины типа I2C, SPI и т. п.

В этом случае каждое устройство должно проектироваться с учетом соответствующих **требований** для таких устройств и (скорее всего) с расчетом на проведение соответствующих процедур **сертификации.**

Учитывая огромное количество возможных архитектурных и схемотехнических решений, для которых возможно потребуется разработка и сертификация криптографической подсистемы, хорошо понятно, что **отдельное решение для каждого случая – не может быть реализовано в разумные сроки**, хотя бы из-за конечной пропускной способности сертифицирующих органов.

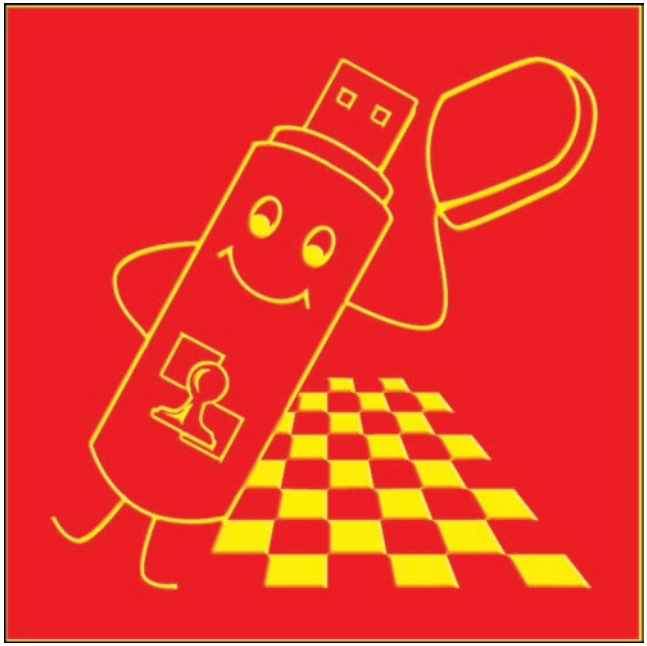
Именно для разработчиков таких устройств, которые должны иметь криптографическую подсистему, предназначена **ШИПКА-Модуль**: разработчик специализированного устройства может использовать готовую аппаратную криптографическую подсистему, а не разрабатывать собственную.

Достоинством ПСКЗИ ШИПКА, важным для решения всех трех групп задач, является ее **перепрограммируемость**. В основе устройства – универсальный перепрограммируемый микропроцессор, а это значит, **что**

- функциональность устройства может быть изменена под те или иные требования, что делает **интеграцию устройства в различные системы более удобной**;

• набор реализованных в криптографической библиотеке **алгоритмов** может включать в себя **те, алгоритмы, которые предпочтительнее для тех или иных задач и не содержать никаких других**, а может предоставлять пользователю возможность выбора, если это предусмотрено политикой безопасности;

• дополнительные функции, реализованные в ПО ПСКЗИ ШИПКА, если они появились позже, чем устройство было приобретено, могут быть получены пользователем **в виде обновления** – это существенно **продлевает срок эффективной службы устройства и делает его применение более экономичным**, чем использование более дешевых средств, не предполагающих возможность обновления и расширения возможностей.



В этом состоит очень важное отличие ПСКЗИ ШИПКА от USB-токенов – аналогов смарт-карт: разрабатывая новые возможности для своего продукта, мы не склоняем пользователей выбросить старое изделие и купить новое.

МЫ ПРЕДЛАГАЕМ ПОЛУЧАТЬ ОБНОВЛЕНИЯ НА СВОЙ ЭКЗЕМПЛЯР.

ОПИСАНИЕ СЕМЕЙСТВА ШИПКА (С УКЛОНОМ В КЛАССИФИКАЦИЮ)

Итак, ПСКЗИ ШИПКА представляет собой специализированное мобильное устройство, позволяющее надежно выполнять криптографические преобразования и хранить ключи.

Семейство включает в себя серию USB-устройств (осознавая, что на рынке СКЗИ сегодня достаточно широк выбор лишь дешевых средств – аналогов смарт-карт, мы разработали модификации со значительно различающимися показателями):

ШИПКА-1.5, **ШИПКА-1.6** и **ШИПКА-1.7**, а также устройства в конструктиве **CF Type II**, **PC CARD Type II**, **ExpressCard 34** и устройство **ШИПКА-Модуль**.

Криптографическая функциональность всех этих устройств одинакова – это шифрование, ЭЦП, хэш-функция, генерация ключей, долговременное хранение ключей и сертификатов.

Реализация криптографических операций во всех случаях аппаратная (по отношению к ПК).

Для **хранения ключевой информации** во всех устройствах есть энергонезависимая защищенная память объемом 4 Кбайт, расположенная непосредственно в процессоре.

Все устройства снабжены **дополнительной энергонезависимой памятью типа DataFlash с файловой системой, подобной ISO/IEC 7816**; имеют в своем составе **аппаратные ДСЧ.**

Все модификации ПСКЗИ ШИПКА работают под **ОС семейства Win32**, имея для этого **программные интерфейсы** – Криптопровайдер Microsoft CryptoAPI, библиотека API PKCS#11.

Во всех устройствах семейства ШИПКА реализованы **все российские криптографические алгоритмы**:

шифрование: ГОСТ 28147-89;
вычисление хэш-функции: ГОСТ Р 34.11-94;
вычисление и проверка ЭЦП: ГОСТ Р 34.10-94; ГОСТ Р 34.10-2001;
вычисление ЗКА.

В них также реализована возможность **поддержки зарубежных криптографических алгоритмов**.
Набор зарубежных алгоритмов для всех устройств одинаков:

Шифрование: RC2, DES, DESX, TripleDES, AES;
Хеширование: MD5, SHA-1;
ЭЦП: RSA (ШИПКА-1.5 – 512-бит, остальные – 2048-бит), DSA (ШИПКА-1.5 – 1024-бит, остальные – 2048-бит).

Все устройства являются полностью **перепрограммируемыми** – firmware может обновляться непосредственно пользователем. Это дает возможность расширения его функциональности и создания индивидуальных решений для тех или иных задач заказчика, в случаях, когда эксклюзивное решение предпочтительнее стандартного.

ПСКЗИ ШИПКА МОЖЕТ ИСПОЛЬЗОВАТЬСЯ КАК ХРАНИЛИЩЕ КЛЮЧЕЙ, СГЕНЕРИРОВАННЫХ ПК «АТЛИКС КЛИЕНТ» (КРИПТОПРО) ДЛЯ УЦ СИСТЕМЫ «СТАНДАРТ УЦ».

«Стандарт УЦ» – это типовой доверенный программный комплекс, выполняющий целевые функции удостоверяющего центра (См. Федеральный закон «Об электронной цифровой подписи»). Он предназначен для выполнения задач по созданию, проверке и управлению сертификатами открытых ключей и соответствует классу защиты на уровне достаточном для использования в сетях общего пользования.

Сертитификат открытых ключей, или «цифровой сертификат» – это подписанная электронной цифровой подписью Удостоверяющего центра пара «персональные данные пользователя+его открытый ключ».

Подпись УЦ гарантирует:

• Соотнесенность сведений, содержащихся в сертификате, с пользователем;

• Целостность этих сведений (попытка вмешательства в структуру или данные сертификата нарушают его целостность, соответственно, если подтверждена целостность, то изменений каких-либо данных в сертификате, в том числе и подмены открытого ключа – не было).

Цифровые сертификаты широко используются в **системе управления открытыми ключами** (Public-Key Infrastructure, PKI), так как позволяют пользователям обмениваться открытыми ключами уже непосредственно друг с другом, фактически без участия третьей стороны. Применение цифровых сертификатов в системе PKI позволяет упростить процесс работы с ключевой информацией. При обмене зашифрованными данными сессионный ключ просто зашифровывается на открытом ключе получателя сообщения и подписывается на секретном ключе отправителя.

Взаимодействие пользователя с УЦ обеспечивается с помощью программного комплекса **«Атликс клиент»**, который, в частности, генерирует ключевую пару (секретный и открытый ключ) и записывает ее на **ключевой носитель**.

В качестве такого носителя может использоваться ПСКЗИ ШИПКА.

В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ (ПО) ПСКЗИ ШИПКА ПРЕДУСМОТРЕНА ВОЗМОЖНОСТЬ РАБОТЫ С САМОПОДПИСАННЫМИ СЕРТИФИКАТАМИ

Система работы с сертификатами, подписанными удостоверяющим центром, удобна для корпоративных пользователей, потому что центр сертификации несет ответственность за аутентичность своих конечных пользователей, обеспечивая при обмене деловой информацией уверенность как в источнике, так и в получателе.

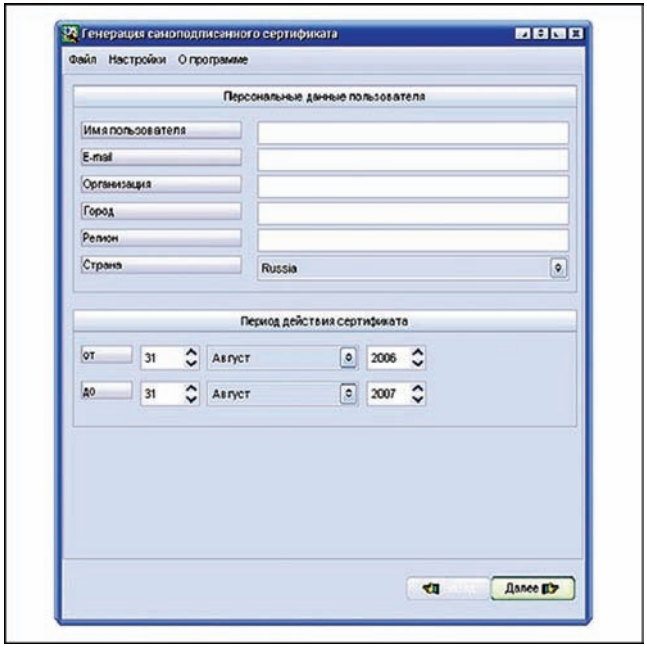
Однако для пользователей, которые хотят вести защищенный обмен данными друг с другом в личных целях, генерация и использование сертификатов, выписанных УЦ, может вызвать ряд неудобств.

Во-первых, услуги удостоверяющего центра являются **платными**.

Во-вторых, необходимо **доверие** к самому УЦ, как к независимой и беспристрастной части системы PKI.

В-третьих, в случае сбоя программного обеспечения УЦ или его некорректной работы **обмен данными между пользователями может быть нарушен**.

В этом случае гораздо удобнее использовать ***самоподписанные* сертификаты**. При этом производится ***самовыдача* сертификата**, то есть **сертификат формируется самим пользователем и подписывается на своем собственном секретном ключе**, что позволяет решить все вышеперечисленные проблемы: создание сертификата не требует финансовых затрат и исключает участие удостоверяющего центра в дальнейшей работе пользователей.



Но из-за отсутствия третьей стороны необходимо обеспечить особые условия хранения и передачи такого сертификата.

Генерация самоподписанного сертификата с помощью программного обеспечения ПСКЗИ ШИПКА позволяет **не только ключевую пару, но и сам сертификат сохранить непосредственно на устройстве**.

При этом пользователи смогут обменяться своими сертификатами, даже не передавая их по сети, а восстановив контекст сертификата с устройства на машине другого пользователя.

Специальное программное обеспечение ПСКЗИ ШИПКА позволяет создавать самоподписанные сертификаты **как через интерфейс криптопровайдера, так и через интерфейс Cryptoki, определенный стандартом PKCS #11**.

При этом секретный ключ ключевой пары **генерируется непосредственно в ПСКЗИ ШИПКА**, где и **хранится в защищенной памяти** устройства.

Генерация сертификатов возможна с использованием следующих алгоритмов подписи:

- **PKCS #1 v1.5 RSA** с функцией хеширования MD5;
- **PKCS #1 v1.5 RSA** с функцией хеширования SHA-1;
- **ГОСТ Р 34.10-94** с функцией хеширования ГОСТ Р 34.11-94;
- **ГОСТ Р 34.10-2001** с функцией хеширования ГОСТ Р 34.11-94.

В ПО ПСКЗИ ШИПКА РЕАЛИЗОВАНА ПОДДЕРЖКА RFC 4357 ЧЕРЕЗ ИНТЕРФЕЙС CSP И ЧЕРЕЗ PKCS#11

Те разработчики, которые понимают, что **возможность интеграции СКЗИ** в настоящее время совершенно необходима как пользователям, так и производителям, придерживаются **стандартов работы** с криптографическими алгоритмами.

В январе 2006 года IETF (Internet Engineering Task Force) был принят стандарт RFC 4357 “Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms”, разработанный специалистами компании Крипто-Про.

Этот стандарт описывает параметры, необходимые для работы с российскими криптографическими алгоритмами ГОСТ 28147-89, ГОСТ Р 34.10-94, ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001.

В ПО ПСКЗИ ШИПКА работа с криптографическими алгоритмами как через интерфейс CSP, так и через PKCS#11 реализована **с поддержкой стандарта rfc 4357**.

Эти интерфейсы по-разному используются разработчиками при создании новых приложений – как из-за сложившихся областей применения (приложения, разработанные Microsoft используют CSP (в частности, шифрование сообщений в почтовой программе Outlook и Outlook-express происходит через CSP, а в почтовой программе The BAT! – с помощью PGP через PKCS#11)), так и из-за различающейся

функциональности. Поэтому **возможность стандартизованной работы с помощью обоих API существенно расширяет сферу применения ПСКЗИ ШИПКА**.

СУЩЕСТВЕННЫЕ РАЗЛИЧИЯ МЕЖДУ УСТРОЙСТВАМИ СЕМЕЙСТВА ШИПКА ЛЕЖАТ В ОБЛАСТИ ПРОИЗВОДИТЕЛЬНОСТИ ВЫЧИСЛЕНИЙ ПО РОССИЙСКИМ КРИПТОГРАФИЧЕСКИМ АЛГОРИТМАМ

ШИПКА-1.5

Самое недорогое средство с базовыми показателями производительности. Однако даже эти показатели существенно выше показателей многих аналогичных изделий других производителей, представленных сегодня на рынке. Не углубляясь в детали, приведем один из них – во многом определяющий. ШИПКА-1.5 работает в режиме USB Full-Speed, в отличие от изделий наших коллег, работающих в режиме Low-Speed. Это значит, что скорость обмена данными между ПК и ШИПКОЙ – **в 25 раз выше**, чем у этих изделий.

Для пользователя это обозначает, что какой бы ни была скорость криптографических преобразований у процессора устройства, скорость работы

устройства как целого (а именно она имеет значение для пользователя) – будет в любом случае **не выше скорости обмена данными с ПК**.

ПСКЗИ ШИПКА-1.6

Архитектура новой версии ПСКЗИ ШИПКА – ШИПКА-1.6 включает аппаратный сопроцессор, что позволяет не тратить ресурсы микропроцессора на криптографические вычисления, но тем не менее осуществлять их **в доверенной среде**.

Логика аппаратного сопроцессора позволяет выполнять криптографические операции **аппаратно**, но в то же время **существенно быстрее**, чем микропроцессором устройства, поскольку сопроцессор сконфигурирован специально для выполнения криптографических преобразований, и, стало быть, выполняет их намного эффективнее.

ЭЦП по ГОСТ Р 34.10-2001:

- выработка ключа – **30** мс;
- вычисление ЭЦП – **40** мс;
- проверка ЭЦП – **70** мс;

Скорость вычисления хеш-функций и шифрования ограничена пропускной способностью канала – примерно 100 кб/с в одну сторону.

Соответственно, скорость вычисления **хэш-функции** – **100** кб/с, скорость **шифрования** – примерно **60** кб/с.

Эффективность работы устройства напрямую зависит от того, какова библиотека аппаратно реализованных алгоритмов – от ее полноты и адаптивности.

На сегодняшний день существуют конфигурации сопроцессора со следующими наборами алгоритмов:

- ЭЦП + шифрование **ГОСТ** + хэш **ГОСТ**;
- ЭЦП + шифрование **DES/TripleDES** + хэш **SHA-1**;
- ЭЦП + шифрование **RC2** + хэш MD5;
- ЭЦП + шифрование **AES** + хэш **SHA-1**;

Архитектура ШИПКА-1.6 дает возможность динамически перепрограммировать сопроцессор на нужный набор аппаратных функций. Это значит, что фактически все эти алгоритмы доступны одновременно.

Различаются версии ШИПКА-1.6 и ШИПКА-1.6+, имеющие одноплечевой и двуплечевой датчик случайных чисел соответственно (то есть на одном или на двух диодах).

ПСКЗИ ШИПКА-1.7

Для решения задач, требующих от ПСКЗИ **высокой производительности**, мы разработали ШИПКА-1.7 – устройство принципиально другого уровня по отношению как к модификации ШИПКА-1.5, так и к ШИПКА-1.6, в первую очередь потому, что работает в режиме **USB High-Speed**.

Использование USB-контроллера High-Speed позволило повысить производительность устройства до следующих показателей:

- вычисление **хеш-функции** происходит со скоростью около **3** Мбайт/с,
- **шифрование** – со скоростью около **1.5** Мбайт/с.

Речь идет именно о порядке величин, поскольку скорость обмена данными по USB-интерфейсу в режиме High-Speed на разных ПК может существенно различаться.

Показатели по **ЭЦП** (по **ГОСТ Р 34.10-2001**) у ШИПКА-1.7 такие же, как у модификации ШИПКА-1.6:

- выработка ключа – **30** мс,
- вычисление ЭЦП – **40** мс,
- проверка ЭЦП – **70** мс.

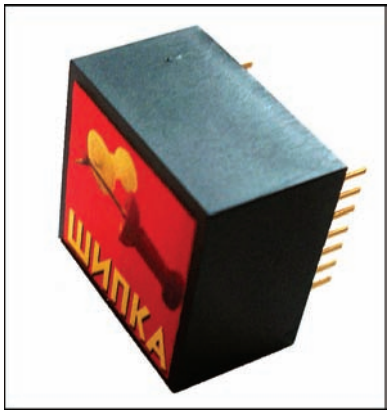
Возможность обмена данными по USB-интерфейсу в режиме High-Speed позволяет реализовать в устройстве **дополнительные возможности**, которые при применении даже режима Full-Speed эффективно использовать было бы невозможно. Например, это добавление в устройство **защищенного диска памяти большого объема**.

Работа с шифрованным диском была бы бессмысленна в устройстве с USB-интерфейсом другого режима, поскольку шифрование всех данных, записываемых на диск, и расшифрование данных, читаемых с диска, занимало бы слишком много времени.

Возможности ШИПКА-1.7 позволяют **эффективно работать с защищенным диском**. **Поэтому ШИПКА-1.7 по заказу дополнительно может быть оснащена шифрованным диском большой емкости (16 Мбайт – 1 Гбайт).**

ШИПКА-Модуль

Устройство является вариантом изделия Шипка-1.6, имеющим интерфейсы типа **I2C** (**100** кБит, **400** кБит) и **UART** (до **115200** бод).



Конструктивно выполнено в виде модуля **25**x**25**x**15** мм, имеющего 14 штыревых выводов.

Модуль предназначен для монтажа на печатную плату.

Имеет повышенную **влагостойкость** и **вибропрочность**. Возможны исполнения как для коммерческого (**0..+70**), так и для индустриального (**40..+85**) температурных диапазонов.

Для питания требуется напряжение **+5V** для питания ядра и напряжение **+1.5..5V** для питания интерфейсных схем.

Скорость шифрования и вычисления хэш-функции определяется только скоростью интерфейса. Это значит, что реальная скорость вычисления **хэш-функции** (с учетом накладных расходов) – приблизительно **300** кБит/с, скорость **шифрования**, соответственно, **150** кБит/с.

ЭЦП по **ГОСТ Р 34.10-2001**:

- выработка ключа – **30** мс;
- вычисление ЭЦП – **40** мс;
- проверка ЭЦП – **70** мс.

Разборка устройства механически затруднена (модуль залит **жестким компаундом**), однако даже если ее осуществить – криптографические **критичные данные извлечь будет невозможно** из-за архитектурных особенностей примененной элементной базы.

ПСКЗИ РАСШИРЕННОЙ ФУНКЦИОНАЛЬНОСТИ

Если от ПСКЗИ требуется *повышенная производительность* при реализации алгоритмов шифрования (например, нужно шифровать содержимое диска или сетевой трафик ноутбука, но при этом нет технической возможности для установки стационарного СКЗИ в ноутбук или стационарное размещение СКЗИ недопустимо по соображениям безопасности), то использование USB-устройства **нецелесообразно**: даже при реализации в ПСКЗИ интерфейса типа USB 2.0 High Speed приемлемого уровня интегрального снижения производительности получить невозможно.

Надо признать, что USB-интерфейс в принципе не приспособлен для обработки массовых многозадачных запросов, особенно в случае **двунаправленного обмена данными**.

Специально для решения такого класса задач предназначены **ШИПКА-Express**, **ШИПКА-Cardbus** и **ШИПКА-CF**.

Первые два изделия ориентированы на использование в **ноутбуках**, имеющих слоты для установки ExpressCard или PCCARD/CardBus.

За счет использования интерфейсов PCI-Express и PCI 32-бит 33 МГц ШИПКА-Express и ШИПКА-Cardbus **аналогичны по производительности стационарным СКЗИ линии Аккорд-5.5**.

Эти ПСКЗИ могут использоваться не только в ноутбуках, но и в **стационарных компьютерах**, оборудованных соответствующими адаптерами для установки стандартных карт или имеющих слот для работы с ExpressCard на фронтальной панели (таких компьютеров в настоящее время становится все больше).

ПСКЗИ ШИПКА-CF выполнено в стандартном формате карты памяти Compact Flash Type 2, что делает возможным применение в составе любого оборудования (в том числе и **КПК**), имеющего слот для таких карт памяти.

Производительность и возможности ШИПКА-CF в целом аналогичны характеристикам ПСКЗИ ШИПКА-1.7.

С любого из этих трех изделий можно **загружать операционную систему** (если такую возможность предоставляет BIOS основного компьютера), в каждом из них реализован объем энергонезависимой памяти, достаточный для загружаемого ПО.

Это значит, что ШИПКА-Express, ШИПКА-Cardbus и ШИПКА-CF могут использоваться и в качестве элемента СЗИ от НСД.

ЧТО ИМЕННО ДОЛЖНО БЫТЬ ПЕРСОНАЛЬНЫМ?

Слова очень сильно влияют на людей. Когда-то ПК – ***персональный компьютер*** – действительно был прорывом в смысле удобства организации собственной рабочей зоны и персональной информационной среды, функцию интерфейса к которой он выполняет.

С изменением требований времени к ритму жизни, мы стали гораздо **легче на подъем** – во всех смыслах.

Мы стали проще относиться к переездам, перелетам, сменам офисов и жилья.

Мы понимаем, что машину можно взять в аренду в том городе, куда мы прилетели на самолете, а не везти с собой свою.

Но вот компьютер, поскольку он называется ***персональный*** – мы все еще считаем уникальным и незаменимым устройством.

Еще бы – там, внутри – вся наша жизнь. **Персональная информационная среда**.

ПОРА ОТКАЗАТЬСЯ ОТ ШАБЛОНА!

Ведь теперь есть инструмент, позволяющий сделать персональную информационную среду мобильной и защищенной одновременно.

Для защищенного информационного взаимодействия **больше не нужно носить с собой свой компьютер**.

Достаточно персонального средства криптографической защиты информации ШИПКА.

А компьютер может быть **любым**.

***ПЕРСОНАЛЬНЫМ* КОМПЬЮТЕР ДЕЛАЕТЕ ВЫ САМИ – С ПОМОЩЬЮ ПЕРСОНАЛЬНОГО СКЗИ!**

Примечание

[1] Правообладателем товарного знака «ШИПКА», согласно свидетельству Государственного Реестра товарных знаков и знаков обслуживания № 240660, является ОКБ САПР.