**Занятие №6. Применение аппаратных средств аутентификации.**

**Метод проведения:** лекция.

**Учебные вопросы:**

1. Персональные идентификаторы.
2. Смарт-карты.
3. Электронные ключи.

**Цели занятия:**

1. Довести до обучаемых основные аппаратные средства аутентифицкации.
2. Ознакомиться со способами применения аппаратных средств аутентификации, их особенностями.

**Время и место проведения:** 2 уч. часа, аудитория (кафедра связи).

**Материальное обеспечение:** доска, мел, указка, ноутбук, проектор, презентация в формате PowerPoint.

**Литература**: Учебник. Информационная безопасность. (В.М. Зима)

Вводная часть

В вводной части проводится проверка наличия личного состава взвода. Проверяется внешний вид, готовность студентов к занятию. Доводится тематика занятий по теме, порядок ее изучения. Доводятся название занятия и его учебные вопросы, цели занятия. Доведение литературы по теме данного занятия.

**Основная часть**

Вопрос №1. Персональные идентификаторы.

Основными и наиболее часто применяемыми методами установления подлинности пользователей являются методы, основанные на использовании паролей. Под паролем при этом понимается некоторая последовательность символов, сохраняемая в секрете и предъявляемая при обращении к компьютерной системе. Ввод пароля, как правило, выполняют с клавиатуры после соответствующего запроса системы. Эффективность парольных методов может быть значительно повышена путем записи в зашифрованном виде длинных и нетривиальных криптографических ключей на информационные носители, например, USB-флеш-накопители, а также носители данных в специализированных микросхемах, называемые электронными аутентификаторами. Если с целью защиты электронного аутентификатора от несанкционированного применения использовать пароль, без знания которого воспользоваться этим аутентификатором по назначению будет невозможно, то в этом случае говорят о двухфакторной аутентификации, которая предполагает:

* предъявление компьютерной системе уникального электронного аутентификатора, например, подсоединением через USB-разъем;
* ввод пароля или PIN-кода (Personal Identification Number) с клавиатуры для возможности доступа к электронному аутентификатору.

Если для доступа к электронному аутентификатору используется аппаратный интерфейс, отличный от универсального USB-интерфейса, то компьютерная система должна включать специальные считыватели соответствующих электронных аутентификаторов, например, считыватели смарт-карт, если используются смарт-карты. Кроме того, в компьютерной систем должны быть установлены драйверы, необходимые для работы со считывателями и электронными аутентификаторами.

На практике вместо термина электронный аутентификатор чаще используется его синонимы – электронный идентификатор или электронный ключ, которые, по сути, является аутентификаторами.

В силовых ведомствах России наиболее широкое распространение получили следующие электронные идентификаторы:

* персональные идентификаторы iButton DS199x;
* смарт-карты РИК (российские интеллектуальные карты);
* электронные ключи Рутокен.

**Персональные идентификаторы iButton**

Модельный ряд персональных идентификаторов iButton, разработанный компанией Dallas Semiconductor, довольно широк и разнообразен (более 20 моделей). Но для двухфакторной аутентификации в компьютерных системах чаще всего используются идентификаторы iButton DS199x, требующие контактного считывателя, подсоединяемого к плате аппаратного модуля доверенной загрузки (АПМДЗ), например, к плате электронного замка «Соболь», вставляемой в разъем шины PCI Express компьютера. Для возможности использования как самих персональных идентификаторов iButton, так и АПМДЗ, на компьютере должен быть установлен соответствующий драйвер АПМДЗ.

В общем виде iButton представляет собой микросхему, вмонтированную в герметичный стальной корпус. Корпус отдаленно напоминает батарейку для наручных часов и имеет диаметр 17,35 мм при высоте 5,89 мм (корпус F5) или 3,1 мм (корпус F3). Он защищает и обеспечивает высокую степень защищенности идентификатора от воздействия агрессивных сред, пыли, влаги, внешних электромагнитных полей, механических ударов и т. п. Идентификатор легко крепится на носителе (карточке, брелоке).

Обмен информацией идентификатором и компьютером происходит в соответствии с протоколом 1-Wire с помощью разнообразных считывающих устройств, подсоединяемых к специализированным платам для шины PCI Express или USB-порту.Для записи и считывания данных из идентификатора нужно, чтобы корпус iButton соприкоснулся со считывающим устройством. Время контакта – не более 5 мс, гарантированное количество контактов составляет несколько миллионов.

В структуре iButton можно выделить следующие основные части: постоянное запоминающее устройство (ПЗУ, 64 байта), энергонезависимое (nonvolatile – NV) ОЗУ (от 1 до 64 Кбит), сверхоперативное запоминающее устройство (scratchpad memory – SM, 256-512 бит), часы реального времени (для DS1994), а также элемент питания – встроенную миниатюрную литиевую батарейку. Изделие DS1990 содержит только ROM. В ПЗУ идентификаторов хранится 64-разрядный код – он состоит из 8-разрядного кода типа идентификатора, 48-разрядного уникального серийного номера и 8-разрядной контрольной суммы. К этому коду как раз и выполняется привязка персонального идентификатора iButton к учетной записи пользователя в системах защиты. Второй фактор аутентификации – ввод и проверка пароля при использовании iButton после предъявления пользователем идентификатора iButton и считывания АПМДЗ кода идентификатора должен быть реализован в АПМДЗ или программном средстве защиты от НСД, например, в Secret Net.



Рисунок – Персональные идентификаторы iButton DS199x и считыватель iButton для платы электронного замка «Соболь»

К **достоинствам** электронных ключей iButton относятся:

* надежность
* долговечность (время хранения информации в памяти идентификатора составляет не менее 10 лет);
* высокая степень механической и электромагнитной защищенности;
* малые размеры;
* относительно невысокая стоимость.

**Недостатками** этого устройства являются:

* небольшая внутренняя память;
* отсутствие поддержки каких-либо криптографических протоколов для более стойкой аутентификации;
* возможность дублирования на программаторах;
* зависимость его срабатывания от точности ручного соприкосновения идентификатора и считывателя, осуществляемого вручную.

Таким образом, персональные идентификаторы iButton являются устаревшими, но все еще широко используемыми электронными ключами.

Вопрос №2. Смарт-карты.

В качестве смарт-карт будут рассмотрены смарт-карты РИК.

Российская интеллектуальная карта РИК – микропроцессорная карта, разработанная государственным унитарным предприятием «Научно-технический центр «Атлас» совместно с другими российскими производителями, выполнена на основе отечественного микроконтроллера КБ5004ВЕ1 с операционной системой ОС UniCos.

Структура карты и операционная система обеспечивают возможность реализации широкого спектра различных приложений на базе РИК:

* двухфакторная аутентификация пользователей компьютерных систем;
* поддержка криптографических преобразований;
* хранение ключей шифрования;
* электронные удостоверения различного рода;
* носитель ключевой информации для систем защищенного электронного документооборота и других приложений.



Рисунок – Внешний вид смарт-карты РИК

Основные технические характеристики РИК на базе микроконтроллера КБ5004ВЕ1:

* 8-разрядный микроконтроллер с RISC-архитектурой;
* 256 байт оперативной памяти (ОЗУ);
* 2 килобайта электрически стираемого перепрограммируемого постоянного запоминающего устройства (ЭСППЗУ);
* не менее 10 лет хранения записанной информации;
* не менее 100 000 циклов стирания/записи;
* канал последовательного доступа, совместимый со стандартом ISO 7816-3.

КБ5004ВЕ1 имеет высокую степень защиты от несанкционированного доступа к информации, хранящейся на карточке. Это достигается с помощью следующего комплекса мер:

* кристалл не имеет точек подключения, кроме предусмотренных стандартом ISO 7816-3;
* использование средств самотестирования для отбраковки при производстве и при каждом включении кристалла;
* специальные меры по предотвращению снятия информации и анализа работы кристалла;
* меры противодействия вводу микроконтроллера в нештатный режим работы путем внешних воздействий.

Управление доступом к информации на Российской Интеллектуальной Карте осуществляется средствами операционной системы UniCOS, установленной на карте. Данные средства позволяют организовать разграничение полномочий на доступ к различным ресурсам карты и добиться высокого уровня защищенности информации на РИК от несанкционированного доступа.

Для каждого типа файлов на карте РИК определен набор видов доступа. Для каждого вида доступа можно назначить права доступа, т.е. совокупность требований, которые должны быть удовлетворены, чтобы субъект (пользователь, терминал или скрипт) осуществил данный вид доступа к объекту (файлу). В данной терминологии права доступа назначаются объекту, а субъект приобретает права доступа (если, например, требуется предъявление какого-либо ключа) или удовлетворяет правам доступа (если речь идет, например, о необходимости шифровать данные при передаче).

Значительная часть команд ОС может быть как подана снаружи, так и выдана исполняемым скриптом. ОС назначает разные права в этих двух случаях, поэтому в таблице прав доступа в описании файлов некоторые виды доступа указываются дважды: как «внешний» и «внутренний».

Некоторые виды доступа разрешены всегда, другие конфигурируются при создании файла. Во многих случаях можно назначать разные права доступа для одинаковых внешних и внутренних команд. Файл любого типа может иметь до 8 различных конфигурируемых прав доступа, смысл которых зависит от типа файла. Права доступа задаются при создании файла и впоследствии не могут меняться. Приложения могут вводить новые нестандартные права доступа к файлам и устанавливать для них права доступа.

Права доступа характеризуются атрибутами доступа. Существуют 4 атрибута доступа, которые могут быть использованы независимо друг от друга:

* требование предъявления PIN;
* требование предъявления ключа аутентификации;
* требование шифрования передаваемых данных на определенном ключе;
* требование снабжения передаваемых данных имитовставкой, сформированной на определенном ключе (сертификация данных).

Для осуществления прав доступа на каждом уровне иерархии можно использовать до 15 ключей, которые располагаются на текущем или расположенном выше уровне.

В заголовке каждого файла РИК находится таблица прав доступа фиксированного размера, содержащая номера шаблонов доступа. Поскольку в реальных приложениях большинство видов доступа имеют одинаковые права доступа, соответствующие всего нескольким шаблонам, то в целях экономии пространства, в заголовках файлов хранятся не сами атрибуты доступа, а ссылки на шаблоны доступа, которые расположены в заголовке файла директории.

Таблица шаблонов доступа размещается в текущей директории или в одной из директорий более высокого уровня в заголовке файла директории. Шаблоны в таблице шаблонов доступа располагаются в произвольном порядке. Поиск осуществляется по номеру шаблона. Если шаблон доступа не найден, то поиск продолжается в таблице шаблонов доступа, расположенной в директории более высокого уровня. Если шаблон доступа не был найден, то доступ запрещается.

Поиск ключей, обозначенных в таблице шаблонов доступа, производится в директории, где располагается таблица шаблонов доступа и выше. Если файл не найден, доступ запрещается.

Алгоритм контроля прав доступа к файлу выглядит следующим образом:

* определяется ячейка таблицы прав доступа, содержащая права доступа для данного типа доступа;
* из таблицы прав доступа в заголовке файла читается номер шаблона доступа;
* производится поиск шаблона доступа в таблице шаблонов доступа текущей директории, а затем, если шаблон не был найден, - в таблицах директорий более высокого уровня вплоть до корневого файла РИК;
* поскольку не для всех видов доступа допустимы любые атрибуты доступа, на шаблон доступа накладывается маска, сбрасывающая значения указателей наличия запрещенных видов доступа;
* для всех используемых атрибутов доступа из шаблона доступа считывается номер соответствующего ключа;
* далее номера ключей используются для осуществления контроля доступа и защищенной передачи сообщений.

В некоторых командах (например, диверсификация ключа), атрибут доступа маскируется, но, тем не менее, соответствующий номер ключа используется при выполнении команды.

Полученные номера ключей используются для извлечения соответствующих ключей (шифрования, электронной подписи) из файлов ключей, находящихся на РИК. Файл ключа предназначен для хранения ключей или паролей и представляет собой особую разновидность файла записей постоянной длины. Ключи могут иметь длину от нескольких байт (в случае использования открытого текста в качестве ключа) до 256 бит (в случае использования алгоритма шифрования ГОСТ 28147-89).

Параметры файла ключей включают в себя:

* количество сделанных записей;
* размер записи;
* тип алгоритма: открытый текст, ГОСТ 28147-89, DES, Triple DES;
* максимальное и оставшееся количество попыток предъявления;
* флажки;
* номер сессии, в которой происходила диверсификация ключа или генерация сессионного ключа;
* признак генерации сессионного ключа;
* буфер для хранения производного ключа.

Если для некоторого вида доступа в качестве атрибутов установлены требование PIN или требование предъявления ключа аутентификации, то доступ разрешается только в случае предъявления соответствующих ключей. В каждый момент времени определена битовая маска предъявленных ключей, которая модифицируется при предъявлении ключа или переходе в другую директорию.

Приобретенные права доступа распространяются на текущую директорию, файлы текущей директории и все вложенные поддиректории. Приобретенные права доступа теряются при переходе в директорию, не вложенную в текущую.

Таким образом, в отличие от идентификатора iButton, смарт-карта РИК помимо возможности реализации двухфакторной аутентификации пользователей компьютерных систем обеспечивает поддержку криптографических преобразований, защищенное хранение ключей шифрования, а также дополнительных реквизитов, и, к тому же, исключает возможность дублирования смарт-карты на программаторе. К недостатку можно отнести необходимость наличия специализированного считывателя, подсоединяемого через интерфейс USB.

Вопрос №3. Электронные ключи.

В качестве электронных ключей будут рассмотрены ключи Рутокен, разработанные отечественной компанией «Актив». Именно они получили наиболее широкое распространение в защищенных автоматизированных системах (АС) для двухфакторной аутентификации, поддержки криптографических преобразований и электронной подписи.

Так как надежная аутентификация основана на криптографии, то важной особенностью электронных ключей Рутокен является изначальная ориентация на решение задач защиты для базовых этапов жизненного цикла криптографических ключей:

* генерация – нужно обеспечить защиту от прогнозирования, а также конфиденциальность и целостность;
* хранение – нужно обеспечить конфиденциальность и целостность;
* использование – нужно обеспечить защиту от перехвата, повторного использования, подмены;

При использовании электронных ключей Рутокен для аутентификации, шифрования и электронной подписи обеспечивается повышение уровня защищенности криптографических ключей за счет их генерации, хранения, использования и уничтожения во внешнем ключе Рутокен, способном аппаратно выполнять криптографические преобразования.

Рутокен является USB аналогом смарт-карты, подсоединяется к компьютеру непосредственно через интерфейс USB, не требуя для компьютера наличия специализированного считывателя. Имеется также разновидность ключа Рутокен с реализацией интерфейса Bluetooth.

Модельный ряд Рутокен включает следующие виды электронных ключей, различающихся поддержкой функций аутентификации, шифрования и электронной подписи:

1) Рутокен S (встроенная память ЭСППЗУ от 32 до 128 Кбайт). USB-устройство предназначено для безопасной двухфакторной аутентификации пользователей (предъявление самого USB-токена и уникального PIN-кода), защищенного хранения ключей шифрования и ключей электронной подписи, цифровых сертификатов и иной информации, а также аппаратной поддержки шифрования по алгоритму ГОСТ 28147-89 - шифрование внешних данных в любом режиме: простая замена, гаммирование, гаммирование с обратной связью; выработка 32-битной имитовставки, генерация 256-битных случайных чисел, защищенное хранение ключей шифрования ГОСТ без возможности их выгрузки.

2) Рутокен ЭП (встроенная память ЭСППЗУ 64 Кбайт). USB-устройство предназначено для безопасной двухфакторной аутентификации пользователей (предъявление самого USB-токена и уникального PIN-кода), защищенного хранения ключей шифрования и ключей электронной подписи, цифровых сертификатов и иной информации, а также реализация алгоритмов формирования и проверки электронной подписи, шифрования:

* Поддержка алгоритмов ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012: генерация ключевых пар с проверкой качества, формирование и проверка электронной подписи, срок действия закрытых ключей до 3-х лет.
* Поддержка алгоритмов ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012: Вычисление значения хеш-функции данных, в том числе с возможностью последующего формирования ЭП.
* Поддержка алгоритма ГОСТ 28147-89: генерация и импорт ключей шифрования, шифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью, вычисление и проверка криптографической контрольной суммы данных (имитовставки ГОСТ).
* Выработка сессионных ключей (ключей парной связи): по схеме VKO GOST R 34.10-2001 (RFC 4357) и VKO GOST R 34.10-2012 (RFC 7836, Протокол ТК 26 №13 от 24.04.2014 г.), расшифрование по схеме EC El-Gamal.
* Поддержка алгоритма RSA: поддержка ключей размером до 2048 бит, генерация ключевых пар с настраиваемой проверкой качества, формирование электронной подписи.
* Генерация последовательности случайных чисел требуемой длины.

3) Рутокен ЭП Bluetooth (встроенная память ЭСППЗУ 64 Кбайт). Данное Bluetooth устройство аналогично по функциям USB-устройству Рутокен ЭП, но в качестве интерфейса взаимодействия с компьютером используется беспроводной интерфейс Bluetooth. Решение совмещает в себе всю функциональность USB-токена Рутокен ЭП с возможностью использования при работе с мобильными устройствами (смартфонами и планшетами).

4) Рутокен Lite (встроенная память ЭСППЗУ 64 Кбайт). USB-устройство предназначено для безопасной двухфакторной аутентификации пользователей (предъявление самого USB-токена и уникального PIN-кода), защищенного хранения ключей шифрования и ключей электронной подписи, а также цифровых сертификатов и иной информации.

5) Рутокен Web. Устройство предназначено для безопасной двухфакторной аутентификации пользователей на основе технологии электронной подписи (предъявление самого USB-токена и уникального PIN-кода) при доступе к Web- ресурсам с помощью Web-браузера, а также криптографической поддержки следующих функций в процессе аутентификации:

* Аппаратная генерация ключевых пар с проверкой качества по алгоритму ГОСТ Р 34.10-2001.
* Аппаратное хеширование по стандарту ГОСТ Р 34.11-94.
* Аппаратное формирование электронной подписи по алгоритму ГОСТ Р 34.10-2001.

Рутокен Web состоит из трех компонентов:

* USB-токен - электронный ключ, имеющий возможность осуществлять электронную подпись. Работает как HID-устройство, не требует установки драйверов.
* Плагин для браузера - осуществляет связь между USB-токеном и браузером. Не требует административных прав для установки. Использует только встроенные в браузер API и не требует установки дополнительных компонентов, фреймворков и платформ, таких как Java, Microsoft Silverlight и другие. Работает со всеми известными браузерами на платформах Microsoft Windows, Apple macOS/OSX, GNU/Linux.
* Серверная часть - реализация проверки электронной подписи на сервере. Механизмы реализованы для разных платформ и средств разработки, а именно: PHP, ASP.NET, WordPress, Joomla и Битрикс.

Рутокен выпускается в двух форм-факторах:

* в виде обычного USB флеш-носителя – Рутокен (размеры 58х16х8мм; масса 6,3г);
* в миниатюрном исполнении – Рутокен micro (размеры 17,8х15,4х5,8мм; масса 1,6г).



Рисунок – Внешний вид электронных ключей Рутокен

Кроме того, в модельном ряде каждого вида Рутокен присутствует дополнительный вариант Рутокен RF с интегрированной RFID-меткой (поддержка стандартов HID, EM-Marine, MF-Mifare) для дополнительного использования в качестве RFID-идентификаторов вместо соответствующих карт для бесконтактных считывателей в системах контроля физического доступа пользователей в охраняемые помещения.

**Общие характеристики** электронного идентификатора Рутокен:

* Имеет встроенный микропроцессор.
* 32-битовый уникальный серийный номер.
* Энергонезависимая память – электрически стираемое перепрограммируемое постоянное запоминающее устройство (ЭСППЗУ);
* Встроенная файловая система по стандарту ISO/IEC 7816.
* Прозрачное шифрование содержимого памяти по ГОСТ 28147 на основе данных, уникальных для каждого экземпляра Рутокен.
* Аппаратное шифрование внешних данных по ГОСТ 28147 в любом режиме: простая замена, гаммирование, гаммирование с обр.связью.
* Защищенное хранение ключей шифрования в объектах данных без возможности их экспорта из токена.
* Поддержка стандартов электронной подписи - ГОСТ Р 34.10, ГОСТ Р 34.11 с длиной ключа 256 и 512 бит. Защищенное хранение ключей асимметричного шифрования и цифровых сертификатов.
* Выработка 32-битовой имитовставки.
* Генерация 256-битовых случайных чисел.
* 2-факторная аутентификация (по факту наличия Рутокен и по факту предъявления PIN-кода).

Рассмотрим ряд особенностей Рутокен:

1. Микропроцессорная технология:

* Вычислительной основой линейки Рутокен служат 32-разрядные высокопроизводительные микропроцессоры архитектуры ARM. Благодаря значительной вычислительной мощности процессора ресурсоемкие вычисления, такие как генерация ключевых пар, вычисление и проверка электронной подписи выполняются достаточно быстро, несмотря на отсутствие специальных ускорителей криптографических операций
* На скорость вычислений также оказывает влияние тот факт, что все микропрограммы устройств Рутокен реализованы на компилируемом языке, который в отличие от, например, Java, дает гораздо больше возможностей по оптимизации. В аппаратных решениях Рутокен используются современные защищенные микроконтроллеры с большим объемом энергонезависимой памяти для хранения пользовательских данных.

1. Интерфейс USB в Рутокен:

* USB CCID. Спецификация USB CCID (Chip Card Interface Devices) широко используется для считывателей смарт-карт, подключаемых через интерфейс USB. Большое количество приложений использует драйверы USB CCID, входящие в состав операционных систем, что решает проблемы совместимости и поддержки пользователей. Реализации этого драйвера имеются практически во всех широко используемых ОС. Основные модели Рутокен работают на основе этой спецификации.
* USB HID (Human Interface Device) не типичен для токенов и считывателей смарт-карт, но поскольку драйвер USB HID присутствует практически во всех современных операционных системах, он был использован для идентификаторов Рутокен Web. Применение этого интерфейса позволяет сделать Рутокен Web работоспособным почти на любых платформах. Пользователю не нужно беспокоиться об установке каких-либо дополнительных драйверов, что снижает риски возникновения технических проблем и сильно удешевляет техническую поддержку.

1. Файловая система Рутокен:

* Как и любая другая, файловая система Рутокен является частью ОС, предназначенной для хранения данных и обеспечения доступа к ним, а также разграничения прав. Файловая система регламентируется тем же стандартом ISO/IEC 7816-4
* Особенность файловой системы токена состоит в том, что различные виды данных хранятся в различных типах объектов, содержащих кроме всего прочего атрибуты безопасности (Security Attributes). Окружение безопасности (Security Environment) используется для удобной настройки параметров криптографических операций
* Для хранения ключевой информации: ключей шифрования, сертификатов и т.п. используются файлы Рутокен Special File (RSF-файлы). Разные виды ключевой информации хранятся в предопределенных папках с автоматическим выбором нужной папки при создании и использовании RSF- файлов

1. Аутентификация пользователей Рутокен:

* Поддержка 3-х категорий владельцев: Администратор, Пользователь, Гость
* Поддержка 2-х Глобальных PIN-кодов: Администратора и Пользователя
* Поддержка Локальных PIN-кодов для защиты конкретных объектов (например, контейнеров сертификатов) в памяти устройства
* Настраиваемый минимальный размер PIN-кода (для любого PIN-кода настраивается независимо).
* Поддержка комбинированной аутентификации: по схеме «Администратор или Пользователь» и аутентификация по Глобальным PIN-кодам в сочетании с аутентификацией по Локальным PIN-кодам
* Индикация факта смены Глобальных PIN-кодов по умолчанию на оригинальные

1. Криптографические операции в Рутокен:

* Поддержка алгоритмов ГОСТ Р 34.10-2012 и ГОСТ Р 34.10-2001: генерация ключевых пар, формирование и проверка электронной подписи.
* Поддержка алгоритмов ГОСТ Р 34.11-2012 и ГОСТ Р 34.11-94: вычисление значения хеш-функции данных, в том числе с возможностью последующего формирования электронной подписи.
* Поддержка алгоритма ГОСТ 28147-89: генерация и импорт ключей шифрования, шифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью, вычисление и проверка криптографической контрольной суммы данных (имитовставки ГОСТ).
* Выработка сессионных ключей (ключей парной связи) по схемам VKO GOST R 34.10-2001 (RFC4357) и VKO GOST R 34.10-2012.
* Генерация последовательности случайных чисел требуемой длины.
* Поддержка алгоритма RSA, с ключами до 2048 бит.

1. Система команд Рутокен:

* Карточная ОС имеет мало общего с операционной системой в обычном понимании, поскольку, например, не имеет средств для интерактивного взаимодействия с пользователем. Взаимодействие со смарт-картами и токенами возможно через специальную систему команд.
* Команды формируются пользовательскими приложениями или терминалами. В ответ на команды токен производит различные операции и формирует ответы. Команды и ответы составляют протокол, который называется APDU (Application Protocol Data Unit). Стандарт APDU определен в ISO/IEC 7816-4.



Рисунок – Архитектура PCSC (Public Key Cryptography Standarts)

1. Программные интерфейсы для Рутокен (middleware). В большинстве случаев конечный пользователь не сталкивается с ПО промежуточного уровня (middleware), но без него невозможна работа устройств Рутокен со всевозможными приложениями, оперирующими со смарт-картами и токенами через следующие программные интерфейсы:

* библиотеки, реализующие интерфейс с Рутокен по стандарту PKCS#11 - Public Key Cryptography Standarts (Рисунок 48), #11 - Cryptographic Token Interface (Cryptoki).
* Рутокен CSP и Рутокен MiniDriver, дающие возможность задействовать Microsoft Crypto API (MS CAPI) и стандартные функции Windows для работы со смарт-картами.
* Рутокен Плагин – кроссплатформенный и мультибраузерный плагин, который позволяет работать с аппаратной реализацией российских криптоалгоритмов в устройствах Рутокен из контекста браузера.

В устройствах Рутокен программный интерфейс для поддержки архитектуры PKCS#11 обеспечивается сервис-провайдером Рутокен, состоящим из двух компонент:

* Сервис-провайдера смарт-карты (ICC Service Provider, ICCSP);
* Криптографического сервис-провайдера (Cryptographic Service Provider, CSP).

**Заключение**

В ходе проведения лекции обучающиеся ознакомились с основными аппаратными средствами аутентификации. Были изучены понятия смарт-карты, персональных идентификаторов, электронных ключей, их особенности, способы применения.

Старший преподаватель кафедры связи

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_С.Шестаков