**Задание на 01.02.2022**

МДК 03.02 Программно-аппаратные средства защиты информации

1. **Сделать конспект лекции**
2. **Сделать практическую работу №9 Управление доступом в операционных системах**
3. **Сделать практическую работу №10 Идентификация и аутентификация пользователей операционных систем**
4. **Отчет отправить на почту svebalch@mail.ru**

**Лекция 10**

**Бесконтактные смарт-карты и USB-ключи**

Аппаратная интеграция USB-ключей и бесконтактных смарт-карт предполагает, что в корпус брелока встраиваются антенна и микросхема, поддерживающая бесконтактный интерфейс. Это позволяет с помощью одного идентификатора организовать управление доступом и к компьютеру, и в помещения офиса. Для входа в служебное помещение сотрудник использует свой идентификатор в качестве бесконтактной карты, а при допуске к защищенным компьютерным данным - в качестве USB-ключа. Кроме того, при выходе из помещения он извлекает идентификатор из USB-разъема (чтобы потом войти обратно) и тем самым автоматически блокирует работу компьютера.

В 2004 г. на российском рынке появились два комбинированных идентификатора такого типа:

* RFiKey - разработка компании [Rainbow Technologies](http://www.rainbow.);
* eToken PRO RM - разработка компании [Aladdin Software Security R.D.](http://www.aladdin.ru) .

Идентификатор RFiKey (рис. 2) представляет собой USB-ключ iKey со встроенной микросхемой Proximity, разработанной [HID Corporation](http://www.hidcorp.com).

Рисунок 2 - Идентификатор RFiKey

Изделие RFiKey поддерживает интерфейс USB 1.1/2.0 и функционирует со считывателями HID Corporation (PR5355, PK5355, PR5365, MX5375, PP6005) и российской компании Parsec (APR-03Hx, APR-05Hx, APR-06Hx, APR-08Hx, H-Reader).

К основным характеристикам RFiKey можно отнести следующие показатели:

* частота функционирования микросхемы Proximity - 125 кГц;
* тактовая частота процессора - 12 МГц;
* реализуемые криптографические алгоритмы - MD5, RSA-1024, DES, 3DES, RC2, RC4, RC5;
* наличие аппаратного датчика случайных чисел;
* поддерживаемые стандарты - PKCS#11, MS Crypto API, PC/SC;
* файловая система с тремя уровнями доступа к данным;
* поддерживаемые операционные системы - Windows 95/98/ME/NT4 (SP3)/2000/XP/ 2003.

Идентификатор eToken RM представляет собой USB-ключ eToken Pro со встроенным чипом, поддерживающим бесконтактный интерфейс (рис. 3). Поставщика и тип микросхемы заказчик может выбирать в соответствии со своими потребностями. В настоящее время компанией предлагаются радиочипы производства HID Corporation, EM Microelectronic-Marin, Philips Electronics (технология MIFARE), Cotag International и ОАО "Ангстрем".

Рисунок 3 - Идентификатор eToken RM

Например, радиочастотный пассивный идентификатор БИМ-002 отечественной компании ["Ангстрем"](http://www.angstrem.ru) изготовлен в виде круглой метки. Он построен на базе микросхемы КБ5004ХК1, основой которой являются память EPROM емкостью 64 бит и блок программирования, используемый для записи уникального идентификационного кода.

К главным характеристикам eToken RM со встроенным идентификатором БИМ-002 можно отнести следующие показатели:

* частота функционирования БИМ-002 - 13,56 МГц;
* дальность чтения идентификационного кода - до 30 мм;
* тактовая частота процессора - 6 МГц;
* реализуемые криптографические алгоритмы - RSA-1024, DES, 3DES, SHA-1;
* наличие аппаратного датчика случайных чисел;
* поддерживаемые стандарты - PKCS#11, PKCS#15 (CRYPTOKI), MS Crypto API, PC/SC, X.509 v3, SSL v3, S/MIME, IPSec/IKE, GINA, RAS/Radius/PAP/CHAP/PAP;
* поддерживаемые операционные системы - Windows 98/ME/NT/2000/XP/2003, ASP Linux 7.2, Red Hat Linux 8.0, SuSe Linux 8.2.

На отечественном рынке ориентировочные цены комбинированных идентификаторов составляют: RFiKey 1032 - от $41, RFiKey 2032 и RFiKey 3000 - от $57, eToken RM с 32 Кб защищенной памяти и БИМ-002 - от $52.

Разница между стоимостью комбинированных и обычных USB-ключей приблизительно соответствует цене смарт-карты Proximity. Отсюда следует, что интеграция бесконтактных смарт-карт и USB-ключей почти не ведет к росту затрат на аппаратную часть при переходе на комбинированную систему идентификации и аутентификации. Выигрыш же очевиден: один идентификатор вместо двух.

**Гибридные смарт-карты**

Гибридные смарт-карты содержат не связанные между собой разнородные чипы (рис. 4). Один чип поддерживает контактный интерфейс, другие (Proximity, ISO 14443/15693) - бесконтактный. Как и в случае интеграции USB-ключей и бесконтактных смарт-карт, СИА на базе гибридных смарт-карт решают двоякую задачу: защиту от НСД к компьютерам и в помещения компании, где они содержатся. Кроме этого на смарт-карте помещается фотография сотрудника, что позволяет идентифицировать его визуально.

Рисунок 4 - Структура гибридной смарт-карты

Стремление к интеграции радиочастотной бесконтактной и контактной смарт-карт-технологий находит отражение в разработках многих компаний: HID Corporation, [Axalto](http://www.axalto.com), [GemPlus](http://www.gemplus.com), [Indala](http://www.indala.com), Aladdin Knowledge Systems и др.

Например, корпорация HID, ведущий разработчик СИА на базе бесконтактных идентификаторов, выпустила идентификаторы-карты, объединяющие в себе различные технологии считывания идентификационных признаков. Результатом этих разработок явилось создание гибридных смарт-карт:

* Smart ISOProx II - интеграция Proximity-чипа и чипа с контактным интерфейсом (опционально);
* iCLASS - интеграция чипа ISO/IEC 15693 и чипа с контактным интерфейсом (опционально);
* iCLASS Prox - интеграция Proximity-чипа, чипа ISO/IEC 15693 и чипа с контактным интерфейсом (опционально).

На отечественном рынке цены на эти изделия составляют: iCLASS - от $5,1; Smart ISOProx II - от $5,7; iCLASS Prox - от $8,9.

В России компанией Aladdin Software Security R.D. разработана технология производства гибридных смарт-карт eToken Pro/SC RM. В них микросхемы с контактным интерфейсом eToken Pro встраиваются в бесконтактные смарт-карты. Фирма предлагает смарт-карты различных производителей: ОАО "Ангстрем" (БИМ-002), HID Corporation (ISOProx II), Cotag International (Bewator Cotag 958), Philips Electronics (технология MIFARE) и других. Выбор варианта комбинирования определяет заказчик.

Анализ финансовых затрат при переходе на применение гибридных смарт-карт, как и в случае комбинирования бесконтактных смарт-карт и USB-ключей, снова подтверждает торжество принципа "два в одном". Если же на идентификатор поместить фотографию сотрудника, то этот принцип трансформируется в "три в одном".

**Биоэлектронные системы**

Для защиты компьютеров от НСД биометрические системы обычно объединяются с двумя классами электронных СИА - на базе контактных смарт-карт и на базе USB-ключей.

Интеграция с электронными системами на базе бесконтактных смарт-карт главным образом используется в системах управления физическим доступом в помещения.

Как уже было замечено, технологии идентификации по отпечаткам пальцев сегодня лидируют на рынке биометрических средств защиты. Столь почетное место дактилоскопии вызвано следующими обстоятельствами:

* это самый старый и наиболее изученный метод распознавания;
* его биометрический признак устойчив: поверхность кожного покрова на пальце не меняется со временем;
* высокие значения показателей точности распознавания (по заявлениям разработчиков дактилоскопических средств защиты, вероятность ложного отказа в доступе составляет 10-2, а вероятность ложного доступа -10-9);
* простота и удобство процедуры сканирования;
* эргономичность и малый размер сканирующего устройства;
* самая низкая цена среди биометрических систем идентификации.

В связи с этим сканеры отпечатков пальцев стали наиболее используемой составной частью комбинированных СИА, применяемых для защиты компьютеров от НСД. На втором месте по распространенности на рынке компьютерной безопасности находятся СИА на базе контактных смарт-карт.

Примером такого рода интеграции служат изделия Precise 100 MC (рис. 5) и AET60 BioCARDKey (рис. 6) компаний [Precise Biometrics AB](http://www.precisebiometrics.com) и [Advanced Card Systems](http://www.acs.com.hk) соответственно. Чтобы получить доступ к информационным ресурсам компьютера с помощью этих средств, пользователю необходимо вставить в считыватель смарт-карту и приложить палец к сканеру. Шаблоны отпечатков пальцев хранятся в зашифрованном виде в защищенной памяти смарт-карты. При совпадении изображения отпечатка с шаблоном разрешается доступ к компьютеру. Пользователь очень доволен: не надо запоминать пароль или PIN-код, процедура входа в систему значительно упрощается.

Рисунок 5 - Изделие Precise 100 MC

Рисунок 6 - Изделие AET60 BioCARDKey

Изделия Precise 100 MC и AET60 BioCARDKey - это USB-устройства, работающие в среде Windows. Считыватели смарт-карт поддерживают все типы микропроцессорных карточек, удовлетворяющих стандарту ISO 7816-3 (протоколы T=0, T=1). Дактилоскопические считыватели представляют собой сканеры емкостного типа со скоростями сканирования 4 и 14 отпечатков пальцев в секунду у Precise 100 MC и AET60 BioCARDKey соответственно.

Чтобы уменьшить число периферийных устройств, можно интегрировать дактилоскопический сканер и считыватель смарт-карт в USB-клавиатуру защищаемого компьютера. Примерами таких устройств служат изделия KBPC-CID (рис. 7) альянса Fujitsu Siemens Computers , Precise 100 SC Keyboard (рис. 8) и Precise 100 MC Keyboard компании Precise Biometrics AB.

Рисунок 7 - Изделие KBPC-CID

Рисунок 8 - Изделие Precise 100 SC Keyboard

Для доступа к информационным ресурсам компьютера, как и в предыдущем варианте, пользователю необходимо поместить смарт-карту в считыватель и к сканеру приложить палец. Представляется интересным и перспективным решение разработчиков комбинированных систем защиты объединить USB-ключ с дактилоскопической системой идентификации (далее такое устройство будем именовать USB-биоключом). Примером этого решения могут служить USB-биоключи FingerQuick (рис. 9) японской корпорации NTT Electronics и ClearedKey (рис. 10) американской компании [Priva Technologies](http://www.cleared.com).

Рисунок 9 - USB-биоключ FingerQuick

Рисунок 10 - USB-биоключ ClearedKey

В ближайшем будущем USB-биоключи могут получить широкое распространение благодаря своим достоинствам:

* высокий уровень защищенности (наличие дактилоскопического сканера, хранение секретных данных, в частности шаблонов отпечатков пальцев, в защищенной энергонезависимой памяти идентификатора, шифрование обмена данными с компьютером);
* аппаратная реализация криптографических преобразований;
* отсутствие аппаратного считывателя;
* уникальность признака, малые размеры и удобство хранения идентификаторов.

Главным недостатком USB-биоключей является их высокая цена. Например, приблизительная стоимость FingerQuick составляет $190.

На первый взгляд комбинированные системы идентификации и аутентификации представляют собой какие-то дорогостоящие, экзотические продукты. Но мировой опыт разработок систем компьютерной безопасности показывает, что все используемые в настоящий момент средства защиты тоже когда-то были такими вот экзотическими изделиями. А сейчас они - норма безопасной жизни. Отсюда с высокой вероятностью можно утверждать, что подобная судьба ожидает и комбинированные системы.

**Лекция 11**

**Ключи. Организация хранения ключей (с примерами реализации). Распределение ключей. Использование комбинированной криптосистемы. Метод распределения ключей Диффи-Хеллмана. Протокол вычисления ключа парной связи ЕСКЕР.**

Любая криптографическая система основана на использовании криптографичес­ких ключей. Под ключевой информацией понимают совокупность всех действую­щих в информационной сети или системе ключей. Если не обеспечено достаточно надежное управление ключевой информацией, то, завладев ею, злоумышленник получает неограниченный доступ ко всей информации в сети или системе. Управ­ление ключами включает реализацию таких функций, как генерация, хранение и распределение ключей. Распределение ключей - самый ответственный процесс в управлении ключами.

**1. Ключи. Организация хранения ключей**

При работе с открытыми КС необходимо обеспечить защиту аутентифицирующей информации, хранимой в КС. В открытых КС часто отсутствуют внешние максимально защищенные от НСД устройства, хранящие аутентифицирующую информацию, и данную информацию, используемую для аутентификации, приходится хранить в реальном объекте файловой системы (БД аутентификации).

Эту информацию необходимо защищать от 2 основных видов угроз:

 - угроза непосредственного доступа злоумышленника к БД аутентификации с целью ее копирования, модификации, удаления;

 - угроза несанкционированного изучения БД аутентификации.

Защита от первого вида угрозы реализуется, как правило, на уровне ядра ОС путем ограничения доступа к той БД аутентификации всех субъектов, за исключением привилегированных. Либо защита от данного вида угроз реализуется путем определения дискреционной политики безопасности. Однако, как правило, способы защиты от угроз первого вида не работают корректно и их можно обойти, используя существующие уязвимости.

Поэтому при защите БДА большее внимание уделяется защите от несанкционированного исследования их содержимого.

Методы:

1). Шифрование

Такой подход к закрытию содержимого БД аутентификации не является стойким, так как:

1. Шифрование должно быть на ключах, которые необходимо хранить. Хранение в операционной системе недопустимо.
2. При аутентификации пользователя необходимо расшифровать пароль, тем самым нарушить его секретность. Такой способ также уязвим к атакам, например, к атакам, заключенным в пошаговом исследовании процесса аутентификации с помощью известных отладчиков.

2). Хэширование

Для защиты от исследования БДА используется две типовых схемы хранения ключевой информации:

Схема 1

Пусть пользователь с N i имеет идентификатор $ID\_{i}$и ключ идентификации $K\_{i}$, тогда первая типовая схема предполагает наличие в БД аутентификации двух основных полей:

|  |  |  |
| --- | --- | --- |
| № | Информация для идентификации | Информация для аутентификации |
| 1 | ID1 | E1 |
| 2 | ID2 | E2 |
| … |  |  |
| n | IDn | En |

$Ei = F\left(IDi, Ki\right), F$ – функция хэширования. Функция $F$ должна удовлетворять следующим свойствам:

1). Необратимостью: восстановить$ Ki$ возможно было бы только полным перебором

2). Вероятность совпадения хэшей 2 произвольно взятых сообщений должна быть чрезмерно мала, если длина сообщения меньше длины хэша, то вероятность должна быть равна нулю.

3) Рассеивание – при малейшем изменении сообщения его хэш должен существенным образом изменяться.

При использовании такой схемы хранения ключевой информации, ОС в явном виде не знает те ключи, пароли, которые используются пользователем для входа в систему.

Алгоритм аутентификации пользователя будет выглядеть следующем образом:

 Пользователь вводит идентификатор при входе в систему. Подсистема аутентификации ищет наличие данного идентификатора в БД аутентификации. Если данный идентификатор не найден, то идентификация отклоняется. Если же введенный идентификатор равен некому $IDi$, то подсистема аутентификации извлекает $Ei$, соответствующий ему. Далее пользователь вводит пароль k. Подсистема аутентификации вычисляет $y = F(IDi, ki)$. Если $y=Ei$ , то аутентификация принимается.

Недостатком данной схемы является то, что достаточно часто закрытые образы паролей формируются как $Ei = F(ki)$. Тогда пользователи, имеющие одинаковые пароли, будут иметь одни и те же хэши. Злоумышленник, обнаружив подобную ситуацию, может сделать вывод, что пользователи используют одинаковые пароли.

Для устранения этого вводится вторая схема аутентификации.

Схема 2

Вторая типовая схема предполагает хранение вместе с идентификатором $ID\_{i}$случайной информации $S\_{i}$, формирующейся при создании учетной записи.$ S\_{i}$ называется символом привязки.

$$Ei = F(S\_{i},ki)$$

|  |  |  |
| --- | --- | --- |
| **№** | **Информация для идентификации** | **Информация для аутентификации** |
| 1 | ID1 , S1 | E1 |
| 2 | ID2, S2 | E2 |
| … |  |  |
| n | IDn, Sn | En |

В этом случае хэши будут различны. Данная схема используется в системах класса Unix.

**Утверждение о подмене эталона**

Если злоумышленник имеет доступ на запись в БД аутентификации, то он может пройти аутентификацию как любой пользователь КС, отраженный в ней, в том числе и как администратор. Следовательно, доступ на запись в БД аутентификации должны иметь только привилегированные субъекты.

**Защита баз данных аутентификации операционных систем класса Windows NT.**

В данных ОС БД аутентификации хранится в каталоге: winnt\system32\config

БДА носит название SAM, а файл System, в котором хранится ключ шифрования БД аутентификации.

В данной БД аутентификации хранится 2 вида хэшей:

 - LANMAN, используемый для удаленной сетевой аутентификации с ранних версий Windows;

 - NTLM, используется для локальной аутентификации.

**Алгоритм вычисления хэша LANMAN**



Например, если пароль будет состоять из заглавных букв английского алфавита (26), прописных букв английского алфавита (26), цифр (10), специальных символов (13), то

$$A=26+26+10+13=75$$

$$S=75^{10}$$

Тогда время подбора $T=\frac{75^{10}}{10^{7}}$ сек

Используя хэш LANMAN, получим, что

$$A=49$$

$$S=49^{7}$$

Время подбора пароля $T=\frac{49^{7}}{10^{7}}≈5^{7}$

Минусы:

 - все символы пароля преобразуются в заглавные, что уменьшает энтропию паролей, сокращает пространство их перебора;

 - пароль разбивается на две части, которые образуются независимо друг от друга;

При выборе паролей больше 14 символов хэши LANMAN из БД исчезают, следовательно, необходимо выбирать пароли из 15-16 символов.

**Хэш NTLM**



Хэш NTLM имеет длину 16 байт. Каждому из паролей длины меньшей или равной 16 символов соответствует единственный хэш NTLM, по которому ОС будет определять корректность его ввода пользователем. Однако если выбрать пароли больше 17 символов, то для них найдутся другие с длинной меньше или равной 16 символам, которые будут иметь тот же самый хэш. В этом случае ОС будет пускать пользователя на пароле меньшей длины. Есть вероятность, что длина таких паролей будет очень мала. Поэтому в целях безопасности использование паролей длиной больше или равной 17 символов необходимо запретить. Для ОС, построенных на технологии NT, следует выбирать пароли 15-16 символов.

**2. Распределение ключей**

При использовании симметричной криптосистемы две вступающие в инфор­мационный обмен стороны должны сначала согласовать секретный сессионный ключ, то есть ключ для шифрования всех сообщений, передаваемых в процессе обмена. Этот ключ должен быть неизвестен всем остальным, и его необходимо периодически обновлять одновременно у отправителя и получателя. Процесс со­гласования сессионного ключа называют также обменом или распределением ключей.

Асимметричная криптосистема предполагает использование двух ключей -открытого и закрытого (секретного). Открытый ключ можно разглашать, а за­крытый надо хранить в тайне. При обмене сообщениями необходимо пересылать только открытый ключ, обеспечив его подлинность.

К распределению ключей предъявляются следующие требования:

* оперативность и точность распределения;
* конфиденциальность и целостность распределяемых ключей.

Для распределения ключей между пользователями компьютерной сети исполь­зуются следующие основные способы [95]:

1. Использование одного или нескольких центров распределения ключей.

2. Прямой обмен ключами между пользователями сети.

Проблемой первого подхода является то, что центру распределения ключей известно, кому и какие ключи распределены, и это позволяет читать все сообще­ния, передаваемые по сети. Возможные злоупотребления могут существенно на­рушить безопасность сети. При втором подходе проблема состоит в том, чтобы надежно удостовериться в подлинности субъектов сети.

Задача распределения ключей сводится к построению такого протокола распре­деления ключей, который обеспечивает:

* взаимное подтверждение подлинности участников сеанса;
* подтверждение достоверности сеанса;
* использование минимального числа сообщений при обмене ключами.

Характерным примером реализации первого подхода является система аутен­тификации и распределения ключей Kerberos.

Остановимся подробнее на втором подходе - прямом обмене ключами между пользователями сети.

При использовании для защищенного информационного обмена криптосисте­мы с симметричным секретным ключом два пользователя, желающие обменяться криптографически защищенной информацией, должны обладать общим секрет­ным ключом. Эти пользователи должны обменяться общим ключом по каналу связи безопасным образом. Если пользователи меняют ключ достаточно часто, то доставка ключа превращается в серьезную проблему.

Для решения этой проблемы можно применить два основных способа:

1. Использование асимметричной криптосистемы с открытым ключом для за­щиты секретного ключа симметричной криптосистемы.

2. Использование системы открытого распределения ключей Диффи-Хеллмана.

Реализация первого способа осуществляется в рамках комбинированной крип­тосистемы с симметричными и асимметричными ключами. При таком подходе симметричная криптосистема применяется для шифрования и передачи исходно­го открытого текста, а асимметричная криптосистема с открытым ключом - для шифрования, передачи и последующего расшифрования только секретного клю­ча симметричной криптосистемы.

Второй способ безопасного распространения секретных ключей основан на применении алгоритма открытого распределения ключей Диффи-Хеллмана. Этот алгоритм позволяет пользователям обмениваться ключами по незащищен­ным каналам связи.