**Задание на 31.01.2022**

МДК 03.02 Программно-аппаратные средства защиты информации

1. **Сделать конспект лекции**
2. **Сделать практическую работу №7** Реализация подсистемы защиты операционной системы Windows.
3. **Сделать практическую работу №8 Обеспечение защиты** вычислительной сети.
4. **Отчет отправить на почту svebalch@mail.ru**

**Лекция 8**

**Аутентификация с использованием асимметричных алгоритмов шифрования**

В качестве примера протокола, построенного на использовании асимметричного алгоритма шифрования, можно привести следующий протокол аутентификации:



Участник *В* выбирает случайным образом *r* и вычисляет значение *х= h(r)* при условии, что значение *х* демонстрирует знание *r* без раскрытия самого значения *r*; далее он вычисляет значение *е* = *(r,B).* Под ** подразумевается алгоритм асимметричного шифрования (например, *RSA*), а под *h* ( ) — хэш-функция. Участник *В* отправляет сообщение (1) участнику *А*. Участник *А* расшифровывает *е* = *(r,B)*  и получает значения  и , а также вычисляет . После этого производится ряд сравнений, доказывающих, что *х* =  и что полученный идентификатор  действительно указывает на участника *В*. В случае успешного проведения сравнения участник *А* посылает *r*. Получив его, участник *В* проверяет, то ли это значение, которое он отправил в первом сообщении.

Еще одним примером аутентификации с использованием асимметричных алгоритмов является модифицированный протокол Нидхэма и Шредера.

Протокол имеет следующую структуру:



Под ** подразумевается алгоритм шифрования открытым ключом участника *В*.

**Электронная цифровая подпись (ЭЦП). Аутентификация, основанная на использовании цифровой подписи**

В рекомендациях стандарта Х.509 специфицирована схема аутентификации, основанная на использовании цифровой подписи, меток времени и случайных чисел.

Для описания данной схемы аутентификации введем следующие обозначения:

,,— временная метка и случайные числа соответственно;

— подпись, сгенерированная участником *А*;

— подпись, сгенерированная участником *В*;

— сертификат открытого ключа участника *А*;

— сертификат открытого ключа участника *В*.

Если участники имеют аутентичные открытые ключи, полученные друг от друга, то можно не пользоваться сертификатами; в противном случае они служат для подтверждения подлинности открытых ключей.

В качестве примеров можно привести следующие протоколы аутентификации:

1. Односторонняя аутентификация с применением меток времени:



После принятия данного сообщения участник *В* проверяет правильность метки времени , полученный идентификатор *В* и, используя открытый ключ из сертификата , корректность цифровой подписи  *(, В).*

2. Односторонняя аутентификация с использованием случайных чисел:



Участник *В*, получив сообщение от участника *А*, убеждается, что именно он является адресатом сообщения; используя открытый ключ участника *А*, взятый из сертификата , проверяет корректность подписи  *(*,*, В)* под числом , полученным в открытом виде, числом , которое было отослано в первом сообщении, и его идентификатором *В*. Подписанное случайное число  используется для предотвращения атак с выборкой открытого текста.

3. Двусторонняя аутентификация с использованием случайных чисел:



В данном протоколе обработка сообщений 1 и 2 выполняется так же, как и в предыдущем, а сообщение 3 обрабатывается аналогично сообщению 2.

**Протоколы аутентификации с нулевой передачей значений**

Широкое распространение интеллектуальных карт (смарт-карт) для разнообразных коммерческих, гражданских и военных применений (кредитные карты, карты социального страхования, карты доступа в охраняемое помещение, компьютерные пароли и ключи и т.п.) потребовало обеспечения безопасной идентификации и аутентификации таких карт и их владельцев. Во многих приложениях главная проблема заключается в том, чтобы при предъявлении интеллектуальной карты оперативно обнаружить обман и отказать обманщику в допуске, ответе или обслуживании.

для безопасной реализации процедур аутентификации разработаны протоколы аутентификации с нулевой передачей знаний. Секретный ключ владельца карты становится неотъемлемым признаком его личности. доказательство знания секретного ключа с нулевой передачей этого знания служит доказательством подлинности личности владельца карты. Аутентификацию с нулевой передачей знания можно реализовать при помощи демонстрации знания секрета, однако проверяющий должен быть лишен возможности получать дополнительную информацию о секрете доказывающего, а точнее протоколы аутентификации в виде доказательства с нулевым знанием позволяют установить истинность утверждения и при этом не передавать какой-либо дополнительной информации о самом утверждении.

**Упрощенная схема аутентификации с нулевой передачей знаний**

Схему аутентификации с нулевой передачей знаний предложили в 1986 году У. Фейге, А. Фиат и А. Шамир. Она является наиболее известным доказательством идентичности с нулевой передачей конфиденциальной информации.

Выбирают случайное значение модуля *n*, который является произведением двух больших простых чисел. Модуль *n* должен иметь длину 512—1024 бит. Это значение *n* может быть представлено группе пользователей, которым придется доказывать свою подлинность. В процессе идентификации участвуют две стороны:

• сторона *А*, доказывающая свою подлинность;

• сторона *В*, проверяющая представляемое стороной *А* доказательство.

Для того чтобы сгенерировать открытый и секретный ключи для стороны *А*, доверенный арбитр (Центр) выбирает некоторое число У, которое является квадратичным вычетом по модулю *n*. Иначе говоря, выбирается такое число У, при котором сравнение  имеет решение и существует целое число .

Выбранное значение *V* является открытым ключом для *А*. Затем наименьшее значение *S*, для которого .

Это значение *S* является секретным ключом для А.

Теперь можно приступить к выполнению протокола идентификации:

1. Сторона *А* выбирает некоторое случайное число . Затем она вычисляет и отправляет *х* стороне *В*.

2. Сторона *В* посылает *А* случайный бит *b*.

3. Если *b=0*, тогда *А* отправляет *r* стороне *В*. Если *b=1*, то *А* отправляет стороне *В* у .

4. Если *b = 0*, сторона *В* проверяет, что , чтобы убедиться, что *А* знает .

Если *b = 1*, сторона *В* проверяет, что , чтобы быть уверенной, что *А* знает .

Эти шаги образуют один цикл протокола, называемый аккредитацией. Стороны *А* и *В* повторяют весь цикл *t* раз при разных случайных значениях *r* и *b* до тех пор, пока *В* не убедится, что *А* знает значение *S*.

Если сторона *А* не знает значения *S*, она может выбрать такое значение *r*, которое позволит ей обмануть сторону *В*, если *В* отправит ей *b = 0*, либо *А* может выбрать такое *r*, которое позволит обмануть *В*, если *В* отправит ей *b*=1. Но этого невозможно сделать в обоих случаях. Вероятность того, что *А* обманет *В* в одном цикле, составляет 1/2. Вероятность обмануть *В* в *t* циклах равна (1/2)

Для того чтобы данный протокол работал, сторона *А* никогда не должна повторно использовать значение *r*. Если *А* поступила бы таким образом, а сторона *В* отправила бы стороне *А* на шаге 2 другой случайный бит *b*, то *В* имела бы оба ответа *А*. После этого *В* может вычислить значение *S*, и для *А* все закончено.

**Параллельная схема аутентификации с нулевой передачей знаний**

Параллельная схема аутентификации позволяет увеличить число аккредитаций, выполняемых за один цикл, и тем самым уменьшить длительность процесса аутентификации.

Сначала генерируется число *n* как произведение двух больших чисел. Для того чтобы сгенерировать открытый и секретный ключи для стороны *А*, сначала выбирают *К* различных чисел , где каждое  является квадратичным вычетом по модулю *n*. Т.е. выбирают такое значение , при котором сравнение  имеет решение и существует . Полученная строка  к является открытым ключом. Затем вычисляют такие наименьшие значения , что 

Эта строка  является секретным ключом стороны *А*. Протокол процесса идентификации имеет следующий вид:

1. Сторона *А* выбирает некоторое случайное число *r* при условии, что 

Затем она вычисляет  и посылает *х* стороне *В*.

2. Сторона *В* отправляет стороне *А* некоторую случайную двоичную строку из *К* бит: 

3. Сторона *А* вычисляет



Перемножаются только те значения , для которых . Например, если , то сомножитель , входит в произведение, если же , то  не входит в произведение, и т.д. Вычисленное значение у отправляется стороне *В*.

4. Сторона *В* проверяет, что



Фактически сторона *В* перемножает только те значения, для которых 

Стороны *А* и *В* повторяют этот протокол *t* раз, убедится, пока *В* не убедится, что *А* знает .

Вероятность того, что *А* может обмануть *В*, равна (1/2) .

**Лекция 9**

**СИСТЕМЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ**

Предотвратить ущерб, связанный с утратой хранящейся в компьютерах конфиденциальной информации, - одна из важнейших задач для любой компании. Известно, что персонал предприятия нередко оказывается главным виновником этих потерь. По результатам исследования [Computer Security Institute](http://www.), на непреднамеренные ошибки сотрудников приходится 55% такого ущерба, на действия нечестных и обиженных коллег - соответственно 10% и 9%. Оставшуюся часть потерь связывают с проблемами физической защиты (стихийные бедствия, электропитание) - 20%, вирусами - 4% и внешними атаками - 2%.

Основным способом защиты информации от злоумышленников считается внедрение так называемых средств ААА, или 3А (authentication, authorization, administration - аутентификация, авторизация, администрирование). Среди средств ААА значимое место занимают аппаратно-программные системы идентификации и аутентификации (СИА) и устройства ввода идентификационных признаков (термин соответствует ГОСТ Р 51241-98), предназначенные для защиты от несанкционированного доступа (НСД) к компьютерам.

При использовании СИА сотрудник получает доступ к компьютеру или в корпоративную сеть только после успешного прохождения процедуры идентификации и аутентификации. Идентификация заключается в распознавании пользователя по присущему или присвоенному ему идентификационному признаку. Проверка принадлежности пользователю предъявленного им идентификационного признака осуществляется в процессе аутентификации.

В состав аппаратно-программных СИА входят идентификаторы, устройства ввода-вывода (считыватели, контактные устройства, адаптеры, платы доверенной загрузки, разъемы системной платы и др.) и соответствующее ПО. Идентификаторы предназначены для хранения уникальных идентификационных признаков. Кроме того, они могут хранить и обрабатывать разнообразные конфиденциальные данные. Устройства ввода-вывода и ПО пересылают данные между идентификатором и защищаемым компьютером.

На мировом рынке информационной безопасности сегмент ААА стабильно растет. Эта тенденция подчеркивается в аналитических обзорах и прогнозах [Infonetics Research](http://www.infonetics.com), [IDC](http://www.idc.com), [Gartner](http://www4.gartner.com) и других консалтинговых компаний.

В нашей статье основное внимание будет уделено комбинированным системам идентификации и аутентификации. Такой выбор обусловлен тем, что в настоящее время системы этого класса обеспечивают наиболее эффективную защиту компьютеров от НСД.

**Классификация систем идентификации и аутентификации**

Современные СИА по виду используемых идентификационных признаков разделяются на электронные, биометрические и комбинированные (см. рис. 1).

Рисунок 1 - Классификация СИА по виду идентификационных признаков

В электронных системах идентификационные признаки представляются в виде цифрового кода, хранящегося в памяти идентификатора. Такие СИА разрабатываются на базе следующих идентификаторов:

* контактных смарт-карт;
* бесконтактных смарт-карт;
* USB-ключей (другое название - USB-токенов);
* идентификаторов iButton.

В биометрических системах идентификационными признаками являются индивидуальные особенности человека, называемые биометрическими характеристиками. В основе идентификации и аутентификации этого типа лежит процедура считывания предъявляемого биометрического признака пользователя и его сравнение с предварительно полученным шаблоном. В зависимости от вида используемых характеристик биометрические системы делятся на статические и динамические.

Статическая биометрия (также называемая физиологической) основывается на данных, получаемых из измерений анатомических особенностей человека (отпечатки пальцев, форма кисти руки, узор радужной оболочки глаза, схема кровеносных сосудов лица, рисунок сетчатки глаза, черты лица, фрагменты генетического кода и др.).

Динамическая биометрия (также называемая поведенческой) основывается на анализе совершаемых человеком действий (параметры голоса, динамика и форма подписи).

Несмотря на многочисленность биометрических характеристик, разработчики СИА основное внимание уделяют технологиям распознавания по отпечаткам пальцев, чертам лица, геометрии руки и радужной оболочки глаза. Так, например, согласно отчету [International Biometric Group](http://www.biometricgroup.com), на мировом рынке биометрической защиты в 2004 г. доля систем распознавания по отпечаткам пальцев составила 48%, по чертам лица - 12%, геометрии руки - 11%, радужке глаза - 9%, параметрам голоса - 6%, подписи - 2%. Оставшаяся доля (12%) относится к промежуточному ПО.

В комбинированных системах для идентификации используется одновременно несколько идентификационных признаков. Такая интеграция позволяет воздвигнуть перед злоумышленником дополнительные преграды, которые он не сможет преодолеть, а если и сможет, то со значительными трудностями. Разработка комбинированных систем осуществляется по двум направлениям:

* интеграция идентификаторов в рамках системы одного класса;
* интеграция систем разного класса.

В первом случае для защиты компьютеров от НСД используются системы, базирующиеся на бесконтактных смарт-картах и USB-ключах, а также на гибридных (контактных и бесконтактных) смарт-картах. Во втором случае разработчики умело "скрещивают" биометрические и электронные СИА (далее такой конгломерат будем называть биоэлектронной системой идентификации и аутентификации).

**Особенности электронных систем идентификации и аутентификации**

С электронными СИА и анализом их ключевых характеристик, позволяющим сделать выбор в пользу того или иного продукта, можно познакомиться в обзоре "Защита компьютеров: электронные системы идентификации и аутентификации" (см. PC Week/RE, № 12/2004, с. 18). Отметим основные особенности электронных СИА, знание которых помогает понять структуру и принцип работы комбинированных систем.

В состав комбинированных СИА могут входить электронные контактные и бесконтактные смарт-карты и USB-ключи. Основным элементом этих устройств являются одна или более встроенных интегральных микросхем (чипов), которые могут представлять собой микросхемы памяти, микросхемы с жесткой логикой и микропроцессоры (процессоры). В настоящее время наибольшей функциональностью и степенью защищенности обладают идентификаторы с процессором.

Основу чипа микропроцессорной контактной смарт-карты составляют центральный процессор, специализированный криптографический процессор (опционально), оперативная память (RAM), постоянная память (ROM), энергонезависимая программируемая постоянная память (PROM), датчик случайных чисел, таймеры, последовательный коммуникационный порт.

Оперативная память используется для временного хранения данных, например, результатов вычислений, произведенных процессором. Ее емкость составляет несколько килобайтов.

В постоянной памяти хранятся команды, исполняемые процессором, и другие неизменяемые данные. Информация в ROM записывается при производстве карты. Емкость памяти может составлять десятки килобайтов.

В контактных смарт-картах используется два типа памяти PROM: однократно программируемая память EPROM и чаще встречающаяся многократно программируемая память EEPROM. Память PROM служит для хранения пользовательских данных, которые могут считываться, записываться и модифицироваться, и конфиденциальных данных (например, криптографических ключей), недоступных для прикладных программ. Емкость PROM составляет десятки и сотни килобайтов.

Центральный процессор смарт-карты (обычно это RISC-процессор) обеспечивает реализацию разнообразных процедур обработки данных, контроль доступа к памяти и управление ходом выполнения вычислительного процесса.

На специализированный процессор возлагается реализация различных процедур, необходимых для повышения защищенности СИА:

* генерация криптографических ключей;
* реализация криптографических алгоритмов (ГОСТ 28147-89, DES, 3DES, RSA, SHA-1 и др.);
* выполнение операций с электронной цифровой подписью (генерация и проверка);
* выполнение операций с PIN-кодом и др.

Бесконтактные смарт-карты разделяются на идентификаторы Proximity и смарт-карты, базирующиеся на международных стандартах ISO/IEC 15693 и ISO/IEC 14443. В основе функционирования большинства СИА на базе бесконтактных смарт-карт лежит технология радиочастотной идентификации. Конструктивно радиочастотные идентификаторы (см. табл. 1) изготавливаются в виде пластиковых карточек, брелоков, жетонов, дисков, меток и т. п.

Таблица 1 - Радиочастотные идентификаторы

Основные компоненты бесконтактных смарт-карт - чип и антенна. Внутри идентификаторов также может находиться литиевая батарея. Идентификаторы с батареей называются активными, без батареи - пассивными. Каждый идентификатор имеет уникальный 32/64-разрядный серийный номер.

Идентификаторы Proximity функционируют на частоте 125 кГц. В состав чипа входит микросхема памяти (или микросхема с жесткой логикой) со вспомогательными блоками: модулем программирования, модулятором, блоком управления и др. Емкость памяти составляет от 8 до 256 байт. В Proximity в основном используется однократно программируемая постоянная память EPROM, но встречается и перезаписываемая EEPROM. В памяти содержатся уникальный номер идентификатора, код устройства и служебная информация (биты четности, биты начала и конца передачи кода и т. д.).

Обычно идентификаторы Proximity являются пассивными и не содержат химического источника питания - литиевой батареи. В этом случае питание микросхемы происходит посредством электромагнитного поля, излучаемого считывателем. Чтение данных считыватель осуществляет со скоростью 4 кбит/с на расстоянии до 1 м.

Системы идентификации и аутентификации на базе Proximity криптографически не защищены (за исключением заказных систем).

Бесконтактные смарт-карты функционируют на частоте 13,56 МГц и разделяются на два класса, которые базируются на международных стандартах ISO/IEC 15693 и ISO/IEC 14443.

Стандарт ISO/IEC 14443 включает в себя версии А и В, различающиеся способами модуляции передаваемого радиосигнала. Стандарт поддерживает обмен (чтение-запись) данными со скоростью 106 кбит/с (возможно увеличение скорости до 212, 424 или 848 кбит/с), дистанция чтения - до 10 см.

Для реализации функций шифрования и аутентификации в идентификаторах стандарта ISO/IEC 14443 могут применяться чипы трех видов: микросхема с жесткой логикой MIFARE, процессор или криптографический процессор. Технология MIFARE является разработкой компании Philips Electronics и представляет собой расширение ISO/IEC 14443 (версии А).

Стандарт ISO/IEC 15693 увеличивает дистанцию применения бесконтактного идентификатора до 1 м. На этом расстоянии обмен данными осуществляется со скоростью 26,6 Кбит/с.

USB-ключи (см. табл. 2) предназначаются для работы с USB-портом компьютера. Они конструктивно изготавливаются в виде брелоков, которые выпускаются в цветных корпусах, имеют световые индикаторы работы и легко размещаются на связке с ключами. Каждый идентификатор имеет прошиваемый при изготовлении уникальный 32/64-разрядный серийный номер.

Таблица 2 - Характеристики USB-ключей

На российском рынке наибольшей популярностью пользуются следующие USB-ключи:

* серии iKey 10xx, iKey 20xx, iKey 3000 - разработка компании [Rainbow Technologies](http://www.rainbow.com), вошедшей в состав корпорации [<>;](http://www.safenet-inc.comSafeNet)
* [eToken R2, eToken Pro фирмы](http://www.safenet-inc.comSafeNet) [Aladdin Knowledge Systems](http://www.aks.com);
* ePass1000, ePass2000 фирмы [Feitian Technologies](http://www.ftsafe.com);
* [ruToken](http://www.rutoken.ru) - совместная разработка компании "Актив" и фирмы ["АНКАД"](http://www.ancud.ru) .

USB-ключи являются преемниками контактных смарт-карт. Поэтому структуры USB-ключей и смарт-карт, как и объемы аналогичных запоминающих устройств, практически идентичны. В состав USB-ключей могут входить:

* процессор - управление и обработка данных;
* криптографический процессор - реализация алгоритмов ГОСТ 28147-89, DES, 3DES, RSA, DSA, MD5, SHA-1 и других криптографических преобразований;
* USB-контроллер - обеспечение интерфейса с USB-портом компьютера;
* RAM - хранение изменяемых данных;
* EEPROM - хранение ключей шифрования, паролей, сертификатов и других важных данных;
* ROM - хранение команд и констант.

**Комбинированные системы**

Внедрение комбинированных СИА (см. табл. 3) в систему информационной безопасности компании увеличивает количество идентификационных признаков, позволяя таким образом более эффективно защитить компьютеры и корпоративную сеть от НСД. Кроме того, некоторые типы систем способны управлять физическим доступом в здания и помещения и контролировать его.

Таблица 3 - Основные функции комбинированных СИА

Сегодня на рынке компьютерной безопасности присутствуют комбинированные системы идентификации и аутентификации следующих типов:

* системы на базе бесконтактных смарт-карт и USB-ключей;
* системы на базе гибридных смарт-карт;
* биоэлектронные системы.