Учебная дисциплина «Электронные документы»

Лекция 5

Организация системы защиты информации при организации электронного документооборота

То, что информация имеет ценность, люди осознали очень давно - тогда-то и возникла задача защиты этой информации. Люди давно пытались использовать для решения этой задачи самые разнообразные методы, и одним из них была тайнопись – умение составлять сообщения таким образом, чтобы его смысл был недоступен никому, кроме посвященных в тайну. Есть свидетельства, что искусство тайнописи зародилось еще до античных времен.

Несколько десятилетий назад информация приобрела самостоятельную коммерческую ценность и стала распространяться почти как обычный товар. Возникновение индустрии обработки информации привело к железной необходимости существования индустрии средств защиты информации.

По ряду исторически сложившихся причин защита от осязаемых угроз (например, контроль доступа в помещения и физическая защита, защита от утечки информации за счет собственного электромагнитного излучения персонального компьютера) не вызывает особых проблем, а вот потенциальную опасность для информационных ресурсов значительно труднее оценить и измерить.

Федеральный Закон "Об информации, информатизации и защите информации", направленный на регулирование взаимоотношений в информационной сфере совместно с Гражданским кодексом Российской федерации дает ее определение: "Информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления". По указанному Закону защите подлежит информация ограниченного доступа, и поэтому основными целями защиты информации Закон видит:

- предотвращение утечки, хищения, искажения, подделки информации;
- предотвращение безопасности личности, общества, государства;

- предотвращение несанкционированных действий по уничтожению, искажению, блокированию информации;
- защиту конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных;
- сохранение государственной тайны, конфиденциальности документированной информации.

Федеральный Закон "Об информации, информатизации и защите информации" регламентирует отношения, возникающие при формировании и использовании информационных ресурсов Российской Федерации на основе сбора, накопления, хранения, распространения и предоставления потребителям документированной информации, а также при создании и использовании информационных технологий, при защите информации и прав субъектов, участвующих в информационных процессах и информатизации. В том числе, закон обеспечивает правовое регулирование при возникновении несанкционированного доступа к этой информации.

К основным способам несанкционированного доступа к информации относятся:

- непосредственное обращение к объектам доступа;
- создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;
- модификация средств защиты, позволяющая осуществить НСД;
- внедрение в технические средства или в автоматизированные системы технических или программных механизмов, нарушающих предполагаемую структуру и функции вычислительной техники или АС и позволяющих осуществить НСД.

К основным событиям, которые приводят к потере и/или искажению информации в программно – аппаратных комплексах, относятся:

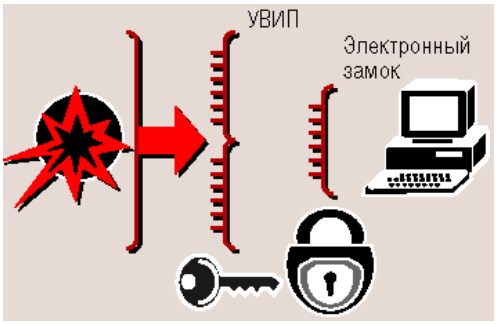
- несанкционированный доступ;
- компьютерные вирусы;

- сбои операционных систем и оборудования;
- стихийные бедствия;
- ошибки персонала

Аппаратно - программные средства защиты от несанкционированного доступа к персональному компьютеру.

На мировом рынке информационной безопасности стабильно развиваются средства ААА - аутентификация, авторизация, администрирование, предназначенные для защиты от несанкционированного доступа к информационным ресурсам автономных и сетевых компьютеров.

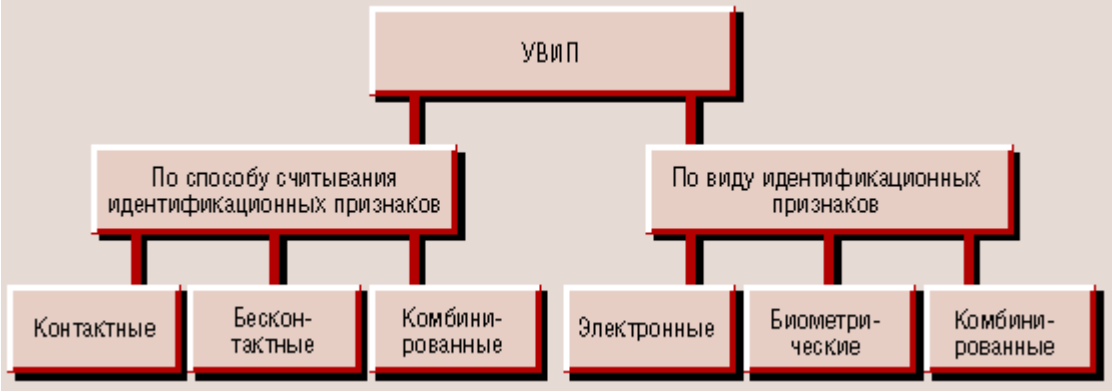
Среди средств ААА важное место занимают аппаратно-программные инструменты контроля доступа к компьютерам — электронные замки, устройства ввода идентификационных признаков (УВИП) и соответствующее ПО. Совместное применение УВИП и электронного замка дает возможность воздвигнуть две линии обороны Разумеется, речь здесь не идет о физическом взломе компьютера.



Доступ к информационным ресурсам компьютера пользователь получает после успешного выполнения процедур идентификации и аутентификации. Идентификация заключается в распознавании пользователя по присущему или присвоенному ему идентификационному признаку. Проверка принадлежности предъявленного им идентификатора (подтверждение подлинности) проводится в процессе аутентификации. В аппаратно-программных средствах контроля доступа к компьютерам идентификация и аутентификация, а также ряд других важных защитных функций, которые описываются ниже, осуществляются с помощью электронного замка и УВИП до загрузки ОС.

В состав аппаратных средств УВИП входят идентификаторы и считывающие устройства (иногда считыватели могут отсутствовать). Современные УВИП принято

классифицировать по виду идентификационных признаков и по способу их считывания:



Классификация устройств ввода идентификационных признаков

По способу считывания они подразделяются на контактные, дистанционные (бесконтактные) и комбинированные. Контактное считывание идентификационных признаков предполагает непосредственное взаимодействие идентификатора и считывателя — проведение идентификатора через считыватель или их простое соприкосновение. Бесконтактный (дистанционный) способ считывания не требует четкого позиционирования идентификатора и считывателя. Для чтения данных нужно либо на определенное расстояние поднести идентификатор к считывателю (радиочастотный метод), либо оказаться с ним в поле сканирования считывающего устройства (инфракрасный метод). Комбинированный способ подразумевает сочетание обоих методов считывания.

По виду используемых идентификационных признаков УВИП могут быть электронными, биометрическими и комбинированными.

В электронных УВИП идентификационные признаки представляются в виде кода, записанного в электронную микросхему памяти идентификатора.

В биометрических устройствах идентификационными признаками являются индивидуальные физические признаки человека (отпечатки пальцев, геометрия ладони, рисунок сетчатки глаза, голос, динамика подписи и т. д.).

В комбинированных УВИП для идентификации используется несколько идентификационных признаков одновременно.

Электронные устройства ввода идентификационных признаков iButton

Разработанное компанией Dallas Semiconductor устройство ввода идентификационных признаков на базе идентификатора iButton относится к классу электронных контактных УВИП. 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).

В структуре iButton можно выделить следующие основные части: постоянное запоминающее устройство (ПЗУ), энергонезависимое ОЗУ, сверхоперативное запоминающее устройство, часы реального времени (для марки DS1994), а также элемент питания — встроенную миниатюрную литиевую батарейку. 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 достоинствам УВИП на базе 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.

Недостатком этого устройства является зависимость его срабатывания от точности соприкосновения идентификатора и считывателя, осуществляемого вручную.

Proximity

Устройства ввода идентификационных признаков на базе идентификаторов Proximity или RFID-системы (radio-frequency identification — радиочастотная идентификация) относятся к классу электронных бесконтактных радиочастотных устройств.

Радиочастотные идентификаторы выпускаются в виде карточек, брелоков, браслетов, ключей и т. п. Каждый из них имеет собственный уникальный серийный номер. Основными их компонентами являются интегральная микросхема, осуществляющая связь со считывателем, и встроенная антенна. В состав микросхемы входят приемо-передатчик и запоминающее устройство, хранящее идентификационный код и другие данные. Внутри Proximity может находиться источник питания — литиевая батарея. Такие идентификаторы называются активными. Они обеспечивают взаимодействие со считывателем на значительном расстоянии (в несколько метров). Дистанция считывания для пассивных идентификаторов (не имеющих батареи) измеряется десятками сантиметров.

Считывающее устройство постоянно излучает радиосигнал. Когда идентификатор оказывается на определенном расстоянии от считывателя, антенна поглощает сигнал и передает его на микросхему. Получив энергию, идентификатор излучает идентификационные данные, принимаемые считывателем. Дистанция считывания в значительной степени зависит от характеристик антенного и приемо-передающего трактов считывателя. Весь процесс занимает несколько десятков микросекунд.

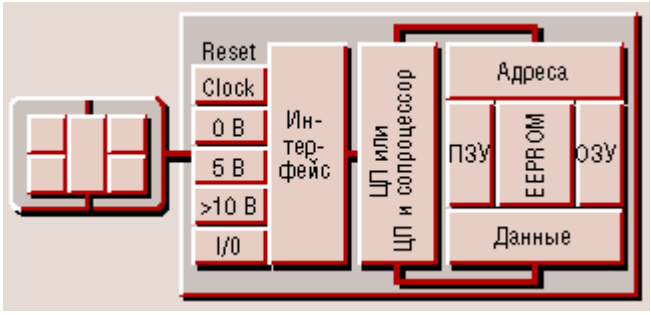
Устройство чтения может размещаться внутри корпуса компьютера. Взаимная ориентация идентификатора и считывателя не имеет значения, а ключи и другие металлические предметы, находящиеся в контакте с картой, не мешают передаче информации.

Основными достоинствами УВИП на базе идентификаторов Proximity являются:

- бесконтактная технология считывания;
- долговечность пассивных идентификаторов;
- точность, надежность и удобство считывания идентификационных признаков.

Устройства ввода на базе смарт-карт

Устройства ввода идентификационных признаков на базе смарт-карт относятся к классу электронных устройств. Они могут быть контактными и бесконтактными (дистанционными).



Основой внутренней организации смарт-карты является так называемая SPOM-архитектура (Self Programming One-chip Memory), предусматривающая наличие центрального процессора (CPU), ОЗУ, ПЗУ и электрически перепрограммируемой постоянной памяти EEPROM. Как правило, в карте также присутствует специализированный сопроцессор.

Процессор обеспечивает разграничение доступа к хранящейся в памяти информации, обработку данных и реализацию криптографических алгоритмов (совместно с сопроцессором). В ПЗУ хранится исполняемый код процессора, оперативная память используется в качестве рабочей, постоянная память необходима для хранения изменяемых данных владельца карты.

Каждая смарт-карта обладает собственным уникальным серийным номером. Он задается на заводе-изготовителе, его нельзя изменить на протяжении всего срока эксплуатации карты. Идентификация по серийному номеру, шифрование данных и аутентификация областей памяти с помощью секретных ключей обеспечивают надежную защиту смарт-карт от взлома.

По отношению к компьютеру устройства чтения смарт-карт могут быть внешними и внутренними. Считыватель работает под управлением специальной программы — драйвера устройства чтения. На базе ISO 7816 разработан стандартный интерфейс для работы со смарт-картами. Включенные в него спецификации PC/SC облегчают интеграцию смарт-карт-технологий в программно-аппаратные комплексы на базе платформы персонального компьютера и создание средств разработки приложений для смарт-карт.

Несомненными достоинствами УВИП на базе смарт-карт считаются удобство хранения идентификатора и считывания идентификационных признаков. К

недостаткам можно отнести ограниченный срок эксплуатации из-за неустойчивости смарт-карты к механическим повреждениям.

Устройства ввода на базе USB-ключей

Устройства ввода идентификационных признаков на базе USB-ключей относятся к классу электронных контактных устройств (см. рис. 2.4),. В составе УВИП данного типа отсутствуют дорогостоящие аппаратные считыватели. Идентификатор, называемый USB-ключом, подключается к USB-порту компьютера непосредственно или с помощью соединительного кабеля.

Конструктивно USB-ключи выпускаются в виде брелоков, которые легко размещаются на связке с обычными ключами. Брелоки выпускаются в цветных корпусах и снабжаются световыми индикаторами работы. Каждый идентификатор имеет собственный уникальный серийный номер. Основными компонентами USB-ключей являются встроенные процессор и память. Процессор выполняет функции криптографического преобразования информации и USB-контроллера. Память предназначается для безопасного хранения ключей шифрования, цифровых сертификатов и любой другой важной информации. Поддержка спецификаций PC/SC позволяет без труда переходить от смарт-карт к USB-ключам и встраивать их как в существующие приложения, так и в новые.

Электронные замки

На электронные замки возлагается выполнение следующих защитных функций:

- идентификация и аутентификация пользователей с помощью УВИП;
- блокировка загрузки операционной системы с внешних съемных носителей;
- контроль целостности программной среды компьютера;
- регистрация действий пользователей и программ.

Конструктивно электронные замки выполняются в виде плат расширения, устанавливаемых в разъемы системных шин PCI или ISA. На платах электронных замков размещаются микросхемы энергонезависимой памяти, перепрограммируемая логическая матрица, встроенный датчик случайных чисел, реле аппаратной блокировки устройств. При каждом включении компьютера автоматически проверяется работоспособность датчика случайных чисел.

Свои основные функции электронные замки реализуют до загрузки операционной системы компьютера. Для этого в составе каждого изделия имеется собственная память EEPROM, дополняющая базовую систему ввода-вывода BIOS компьютера. При включении компьютера выполняется копирование содержимого EEPROM замка в так называемую теневую область оперативной памяти компьютера, с которой и ведется дальнейшая работа.

Программным и/или аппаратным способом возможен запрет загрузки ОС с внешних носителей (магнитных, оптических и магнитно-оптических дисков) путем блокировки доступа к устройствам чтения при запуске компьютера. После успешной загрузки ОС доступ восстанавливается с помощью специальной программы, входящей в состав электронного замка. Контроль целостности программной среды компьютера заключается в проверке изменения файлов и секторов жесткого диска. Для этого вычисляются некоторые текущие контрольные значения проверяемых объектов и сравниваются с заранее рассчитанными эталонными.

Электронные замки устанавливаются в компьютеры, функционирующие под управлением операционных систем MS- DOS, Windows, UNIX FreeBSD.

Электронные замки доверенной загрузки

Термином “доверенная загрузка” разработчики замка определяют случай, когда операционная система загружается только после идентификации и аутентификации пользователя, а также после проверки целостности технических и программных средств компьютера. Российские контроллеры “Аккорд-5”

и “Аккорд 4.5” обеспечивают режим доверенной загрузки для операционных систем MS-DOS, Windows, OS/2, UNIX FreeBSD.

Резидентное ПО замков (средства администрирования, идентификации и аутентификации, поддержки контроля целостности, журнал регистрации) размещается в энергонезависимой памяти контроллеров. Электронные замки комплектуются неконтролируемыми аппаратными датчиками случайных чисел. Аутентификация осуществляется по паролю, вводимому пользователем с клавиатуры

Помимо традиционного контроля целостности программной среды электронные замки обеспечивают проверку целостности технических средств защищаемого компьютера, что немаловажно при отсутствии контроля над физической целостностью корпуса компьютера.

Биометрические методы идентификации и аутентификации

Основные достоинства биометрических методов идентификации и аутентификации:

- высокая степень достоверности идентификации по биометрических признакам из-за их уникальности;
- неотделимость биометрических признаков от дееспособной личности;
- трудность фальсификации биометрических признаков.

В качестве биометрических признаков, которые могут быть использованы для идентификации потенциального пользователя, могут служить:

- узор радужной оболочки и сетчатки глаз;
- отпечатки пальцев;
- геометрическая форма руки;
- форма и размеры лица;
- особенности голоса.

При регистрации пользователь должен продемонстрировать один или несколько раз свои характерные биометрические признаки. Эти признаки (известные как подлинные) регистрируются системой как контрольный "образ"

законного пользователя. Этот образ пользователя хранится в электронной форме и используется для проверки идентификации личности, соответствующего законному пользователю.

Узор радужной оболочки и сетчатки глаз

Системы идентификации по узору радужной оболочки и сетчатки глаз могут быть разделены на два класса: использующие рисунок радужной оболочки глаза и использующие рисунок кровеносных сосудов сетчатки глаза. Поскольку вероятность повторения данных параметров равна 10^{-78}, эти системы являются наиболее надежными среди всех биометрических систем.

Отпечатки пальцев

Системы идентификации по отпечаткам пальцев являются самыми распространенными. Одна из основных причин широкого распространения таких систем заключается в наличии больших банков данных по отпечаткам пальцев.

Геометрическая форма руки

Системы идентификации по геометрической форме руки используют сканеры формы руки, обычно устанавливаемые на стенах. Следует отметить, что подавляющее большинство пользователей предпочитают системы именно этого типа, а не описанные выше.

Форма и размеры лица, особенности голоса

Системы идентификации по лицу и голосу являются наиболее доступными из-за их дешевизны, поскольку большинство современных компьютеров имеют видео- и аудиосредства. Системы данного класса широко применяются при удаленной идентификации в телекоммуникационных сетях.

Следует отметить, что применение биометрических параметров при идентификации субъектов доступа автоматизированных систем пока не получило надлежащего нормативно-правового обеспечения, в частности в виде стандартов. Поэтому применение систем биометрической идентификации допускается только в системах, обрабатывающих и хранящих персональные данные, составляющие коммерческую и служебную тайну.