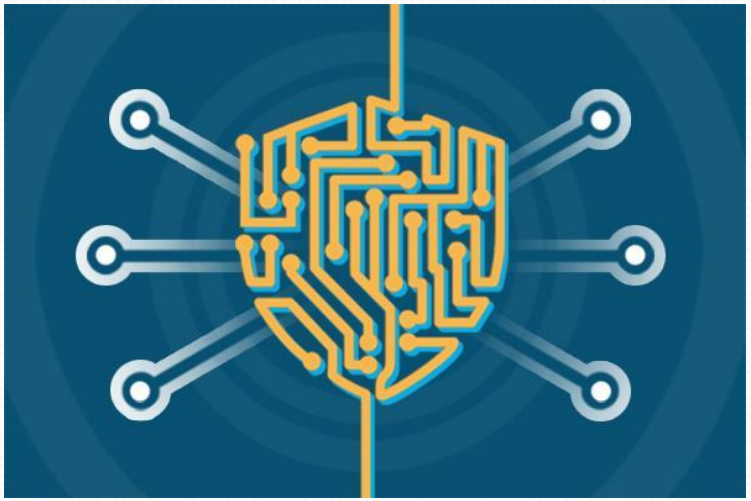
Программно-аппаратные средства для защиты информации

2018

Содержание



Несанкционированный доступ

Несанкционированный доступ - действия, нарушающи
установленный порядок доступа
правила разграничения, доступ
программам и данным, который
получают абоненты, которые не
прошли регистрацию и не имеют
права на ознакомление или рабо
с этими ресурсами.

Для предотвращения несанкционированного доступа осуществляется контроль доступа.

Защита с использованием паролей

Для защиты от несанкционированного доступа к программам и данным, хранящимся на компьютере, используются ***пароли***.

Компьютер разрешает доступ к своим ресурсам только тем пользователям, которые зарегистрированы и ввели правильный пароль.

Каждому конкретному пользователю может быть разрешен доступ только к определенным информационным ресурсам.

При этом может производиться регистрация всех попыток несанкционированного доступа.

Защита с использованием паролей

Защита с использованием пароля используется при загрузке операционной системы

Вход по паролю может быть установлен в программе BIOS Setup, компьютер не начнет загрузку операционной системы, если не введен правильный пароль. Преодолеть такую защиту нелегко.

От несанкционированного доступа может быть защищены:

- диски
- папки
- файлы локального компьютера

Для них могут быть установлены определенные права доступа:

- полный доступ
- возможность внесения изменений
- только чтение
- запись и др.

Количественная оценка стойкости парольной защиты

$$P = \frac{V \times T}{A^L}$$

- Пусть A - мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля. Например, если пароль состоит только из малых английских букв, то A=26).
- L - длина пароля.
- V- скорость перебора паролей злоумышленником.
- T - максимальный срок действия пароля.

Защита информации

Защита информации – это деятельность, направленная на предотвращение утечки информации, несанкционированных и непреднамеренных воздействий на информацию

Средства защиты информации

Средства защиты информации — это совокупность инженерно-технических, электронных, и других устройств и приспособлений, приборов используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

Средства защиты информации разделяются на:

- Технические (аппаратные) средства
- Программные средства
- Организационные средства

Технические (аппаратные) средства

Это различные по типу устройства, которые аппаратными средствами решают задачи защиты информации. Они препятствуют физическому проникновению, доступу к информации, в том числе с помощью ее маскировки. Первую часть задачи решают замки, решетки на окнах, защитная сигнализация и др. Вторую — генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить.

Программные средства

Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной информации типа временных файлов, тестового контроля системы защиты и др.

Организационные средства

Организационные средства складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых.

Биометрические системы защиты

Для защиты от несанкционированного доступа к информации используются ***биометрические системы идентификации.***

Используемые в этих системах характеристики являются неотъемлемыми качествами личности человека и поэтому не могут быть утерянными и подделанными.

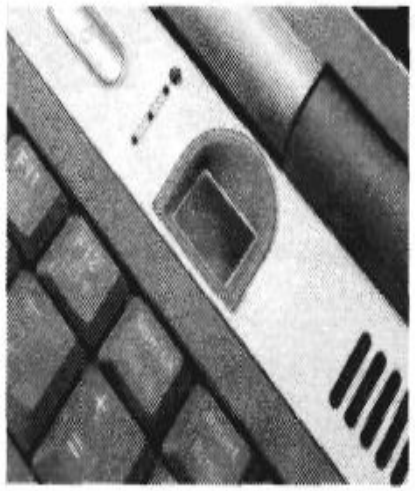
К биометрическим системам защиты информации относятся системы идентификации:

- по отпечаткам пальцев;
- по характеристикам речи;
- по радужной оболочке глаза;
- по изображению лица;
- по геометрии ладони руки.

Идентификация по отпечаткам пальцев

Оптические сканеры считывания отпечатков пальцев устанавливаются на ноутбуки, мыши, клавиатуры, флэш-диски, а также применяются в виде отдельных внешних устройств и терминалов (например, в аэропортах и банках).

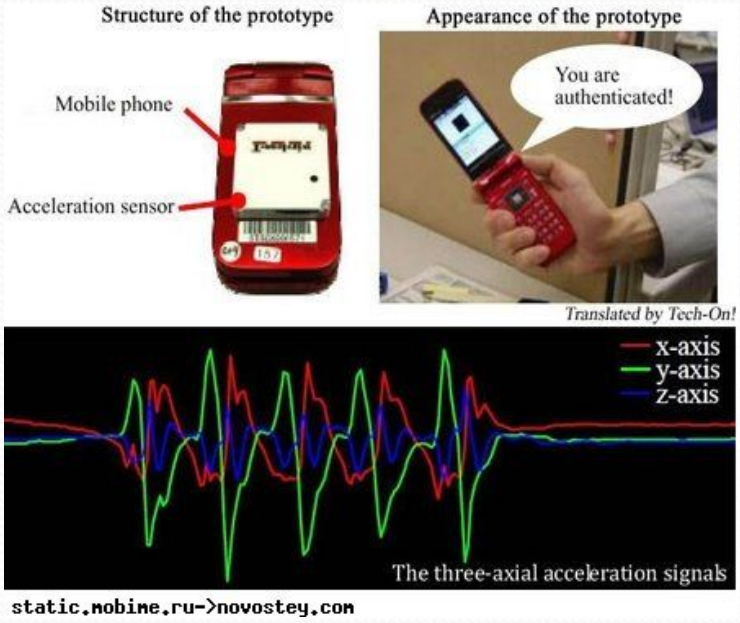
Если узор отпечатка пальца не совпадает с узором допущенного к информации пользователя, то доступ к информации невозможен.



Идентификация по характеристикам речи

Идентификация человека по голосу — один из традиционных способов распознавания, интерес к этому методу связан и с прогнозами внедрения голосовых интерфейсов в операционные системы.

Голосовая идентификация бесконтактна и существуют системы ограничения доступа к информации на основании частотного анализа речи.



Идентификация по радужной оболочке глаза

Радужная оболочка глаза является уникальной для каждого человека биометрической характеристикой.

Изображение глаза выделяется из изображения лица и на него накладывается специальная маска штрих-кодов. Результатом является матрица, индивидуальная для каждого человека.

Для идентификации по радужной оболочке глаза применяются специальные сканеры, подключенные к компьютеру.

Идентификация по изображению лица

Для идентификации личности часто используются технологии распознавания по лицу. Распознавание человека происходит на расстоянии.

Идентификационные признаки учитывают форму лица, его цвет, а также цвет волос. К важным признакам можно отнести также координаты точек лица в местах, соответствующих смене контраста (брови, глаза, нос, уши, рот и овал).

В настоящее время начинается выдача новых загранпаспортов, в микросхеме которых хранится цифровая фотография владельца.

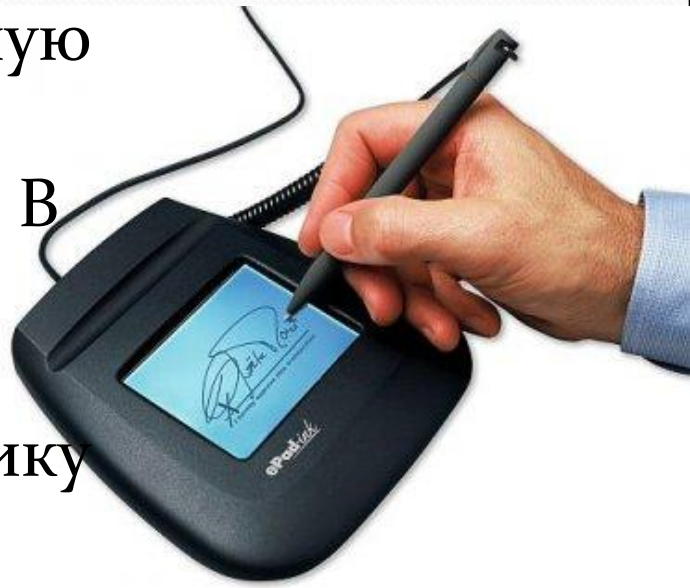
Идентификация по ладони руки

В биометрике в целях идентификации используется простая геометрия руки — размеры и форма, а также некоторые информационные знаки на тыльной стороне руки (образы на сгибах между фалангами пальцев, узоры расположения кровеносных сосудов).

Сканеры идентификации по ладони руки установлены в некоторых аэропортах, банках и на атомных электростанциях .

Цифровая (электронная) подпись

eSign - программа для идентификации подписи, использующая специальную цифровую ручку и электронный блокнот для регистрации подписи. В процессе регистрации eSign запоминает не только само изображение подписи, но и динамику движения пера. eSign анализирует целый ряд параметров, включающих и общие признаки почерка конкретного лица.



от вредоносных программ

Вредоносная программа — злонамеренная программа, то есть программа, созданная со злым умыслом или злыми намерениями.

Для защиты от вредоносных программ используют антивирусы. Причиной проникновения вирусов на защищенные антивирусом компьютеры могут быть:

- антивирус был отключен пользователем;
- антивирусные базы были слишком старые;
- были установлены слабые настройки защиты;
- вирус использовал технологию заражения, против которой у антивируса не было средств защиты;
- вирус попал на компьютер раньше, чем был установлен антивирус, и смог обезвредить антивирусное средство;
- это был новый вирус, для которого еще не были выпущены антивирусные базы

Антивирусные программы

Современные антивирусные программы обеспечивают **комплексную защиту программ** и данных на компьютере от всех типов вредоносных программ и методов их проникновения на компьютер:

- Интернет,
- локальная сеть,
- электронная почта,
- съемные носители информации.

Принцип работы антивирусных программ основан на проверке файлов, загрузочных секторов дисков и оперативной памяти и поиске в них известных и новых вредоносных программ.

Антивирусные программы

Антивирусный монитор запускается автоматически при старте операционной системы. Основная задача его состоит в обеспечении максимальной защиты от вредоносных программ при минимальном замедлении работы компьютера.

Антивирусный сканер запускается по заранее выбранному расписанию или в произвольный момент пользователем. Антивирусный сканер производит поиск вредоносных программ в оперативной памяти, а также на жестких и сетевых дисках компьютера.

Резервное копирование и восстановление данных

Резервное копирование — процесс создания копии данных на носителе, предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения.

Восстановление данных — процедура извлечения информации с запоминающего устройства в случае, когда она не может быть прочитана обычным способом.

Хакерские утилиты и защита от них

Сетевые атаки на удаленные серверы реализуются с помощью специальных программ, которые посылают на них многочисленные запросы. Это приводит к зависанию сервера, если ресурсы атакуемого сервера недостаточны для обработки всех поступающих запросов.

Некоторые хакерские утилиты реализуют фатальные сетевые атаки. Такие утилиты используют уязвимости в операционных системах и приложениях и отправляют специально оформленные запросы на атакуемые компьютеры в сети. В результате сетевой запрос специального вида вызывает критическую ошибку в атакуемом приложении, и система прекращает работу.

Утилиты взлома удалённых компьютеров

Утилиты взлома удаленных компьютеров предназначены для проникновения в удаленные компьютеры с целью дальнейшего управления ими или для внедрения во взломанную систему других вредоносных программ.

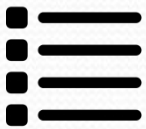
Профилактическая защита от таких хакерских утилит состоит в своевременной загрузке из Интернета обновлений системы безопасности операционной системы и приложений.

Защита от хакерских атак сетевых червей и троянских программ

Защита компьютерных сетей или отдельных компьютеров от несанкционированного доступа может осуществляться с помощью межсетевого экрана.

Межсетевой экран позволяет:

- блокировать хакерские DoS-атаки, не пропуская на защищаемый компьютер сетевые пакеты с определенных серверов
- не допускать проникновение на защищаемый компьютер сетевых червей
- препятствовать троянским программам отправлять конфиденциальную информацию о пользователе и компьютере.



Виды и методы защиты информации

Вид защиты	Метод защиты
От сбоев оборудования	• Архивирование файлов (со сжатием или без); • резервирование файлов
От случайной потери или искажения информации, хранящейся в компьютере	• Запрос на подтверждение выполнения команд, изменяющих файлы; • установка специальных атрибутов документов и программ; • возможность отмены неверного действия или восстановления ошибочно удалённого файла; • разграничение доступа пользователей к ресурсам файловой системы