Правовая охрана программ и данных. Защита информации.

Авторское право на программу возникает автоматически при ее создании. Для оповещения о своих правах разработчик программы может, начиная с первого выпуска в свет программы использовать знак охраны авторского права, состоящий из трех элементов:

Знак охраны авторского права

- Латинская буква **C** внутри круга
- Имя обладателя исключительных авторских прав
- Дата первого опубликования

Международные документы

- Бернская конвенция об охране литературных и художественных произведений 1886г.

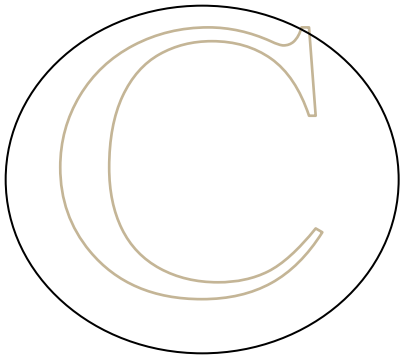
- Всемирная конвенция об авторском праве 1952г.

Документы Российской Федерации:

- Конституция Российской Федерации ст. 44
- Гражданский Кодекс Российской Федерации
- Закон об авторском праве и смежных правах 1993г.
- **Закон Российской Федерации «О правовой охране программ для ЭВМ и баз данных» 1992г.**

Знак охраны авторских прав

ПРИМЕР:



Корпорация Microsoft, 1993-1997

Личные неимущественные права авторов программ для ЭВМ и БД

- Право авторства
- Право на имя
- Право на обнародование
- Право на защиту репутации

Имущественные права авторов программ для ЭВМ и БД

- *Если программы созданы в порядке выполнения служебных обязанностей или по заданию работодателя, то они принадлежат работодателю, если в договоре между ним и автором не предусмотрено иное.*

Выписка из Уголовного кодекса Российской Федерации

Глава 28. Преступления в сфере компьютерной информации

Статья 272. Неправомерный доступ к компьютерной информации

Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, - наказывается

- штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда
- или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев,
- либо исправительными работами на срок от шести месяцев до одного года,
- либо лишением свободы на срок до двух лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, а равно использование либо распространение таких программ или машинных носителей с такими программами, -наказываются

- лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда
- или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

Те же деяния, повлекшие тяжкие последствия, -наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

Нарушение правил эксплуатации ЭВМ лицом, имеющим доступ к ЭВМ, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред,-наказывается

- лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет,
- либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов,
- либо ограничением свободы на срок до двух лет.

Электронная цифровая подпись в электронном документе признается юридически равнозначной подписи в документе на бумажном носителе.

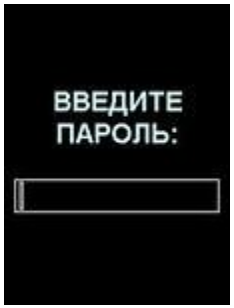
При регистрации электронно-цифровой подписи в специализированных центрах корреспондент получает два ключа: секретный и открытый. Секретный ключ хранится на дискете или смарт-карте и должен быть известен только самому корреспонденту. Открытый ключ должен быть у всех потенциальных покупателей документов и обычно рассылается по электронной почте.

Программы по их правовому статусу можно разделить на три большие группы:

- Лицензионные;
- Условно бесплатные;
- Свободно распространяемые программы.

Защита от несанкционированного доступа к информации.

Для защиты от несанкционированного доступа к данным, хранящимся на компьютере, используются пароли. Компьютер разрешает доступ к своим ресурсам только тем пользователям, которые зарегистрированы и ввели правильный пароль.

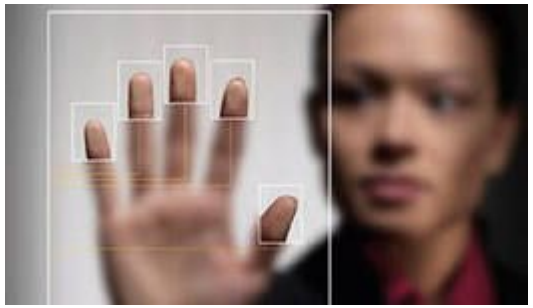


Защита с использованием пароля используется при загрузке ОС. Вход по паролю может быть установлен в программе BIOS Setup, компьютер не начнет загрузку ОС, если не введен правильный пароль.

От несанкционированного доступа может быть защищен каждый диск, папка и файл локального компьютера. Для них могут быть установлены определенные права доступа (полный, только чтение, по паролю), причем права могут быть различными для различных пользователей.

В настоящее время для защиты от несанкционированного доступа к информации все чаще используют биометрические системы идентификаторы.

К биометрическим системам защиты информации относятся системы идентификации по отпечаткам пальцев, системы распознания речи, а также системы идентификации по радужной оболочке глаза.



ПО распространяется фирмами-производителями в форме дистрибутивов на CD- или DVD-дисках. Каждый дистрибутив имеет свой серийный номер, что препятствует незаконному копированию и установке программ.

На CD- или DVD-диск может быть размещен закодированный программный ключ, который теряется при копировании и без которого программа не может быть установлена.

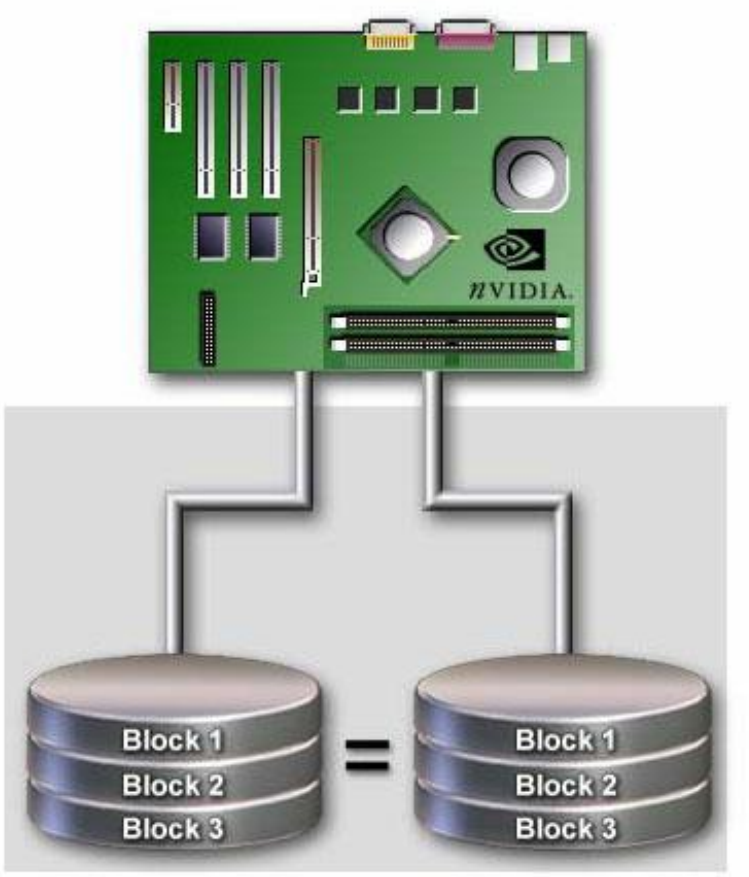
Физическая защита данных на диске

Для обеспечения большей надежности хранения данных на жестких дисках используются RAID-массивы. Несколько жестких дисков подключаются к RAID-контроллеру, который рассматривает их как единый логический носитель информации. При записи информации она дублируется и сохраняется на нескольких дисках одновременно, поэтому при выходе из строя одного из дисков данные не теряются.

Redundant Arrays of Inexpensive Disks

Для обеспечения большей скорости чтения/записи и надежности хранения данных используются ***RAID-массивы*** (избыточный массив независимых дисков)

RAID- контроллер объединяет жесткие диски в единое логическое устройство.



RAID-массивы

Реализация RAID-массива:

- ***Аппаратная*** (несколько жестких дисков управляются специальной платой)
- ***Программная*** (с помощью драйвера объединяются логические разделы диска)

Дисковый
RAID массив
Maxtronic SA-4551S

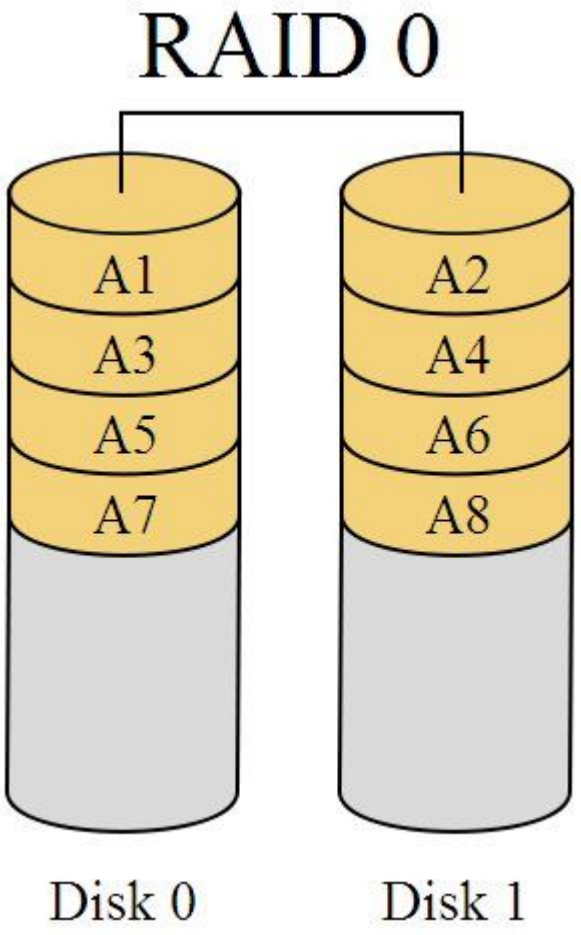
Существует несколько разновидностей (уровней RAID-массива)

Уровень 0

Разделение потока данных между несколькими дисками.

+ увеличение скорости ввода/вывода пропорционально числу дисков.

- при отказе одного из дисков будут утрачены все данные.

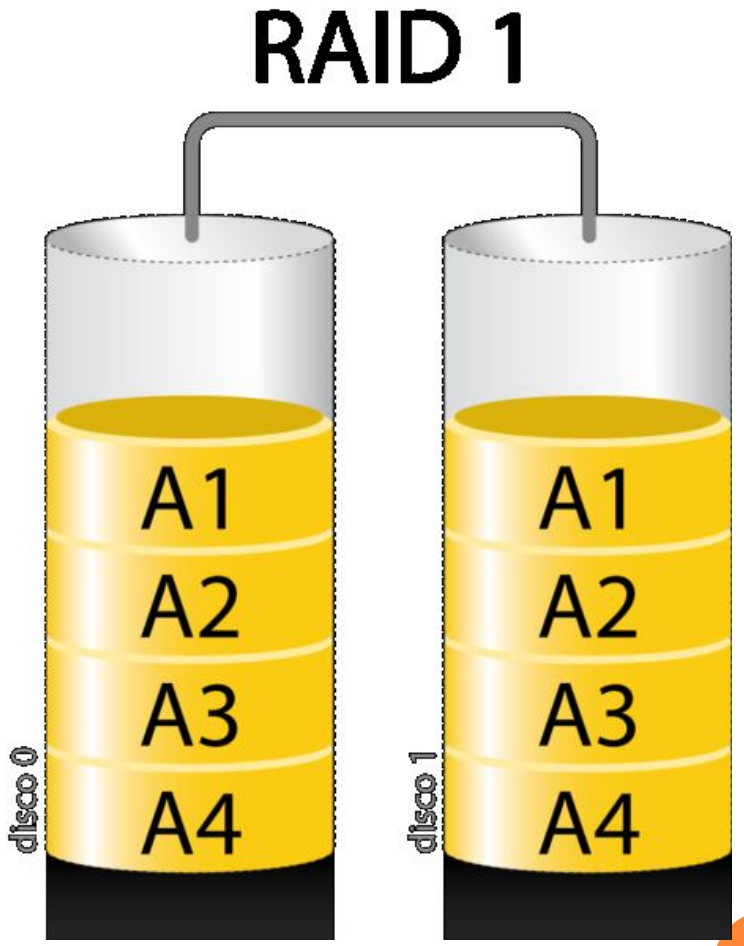


Уровень 1

Организация "зеркальных" дисков (информация дублируется на зеркальном диске)

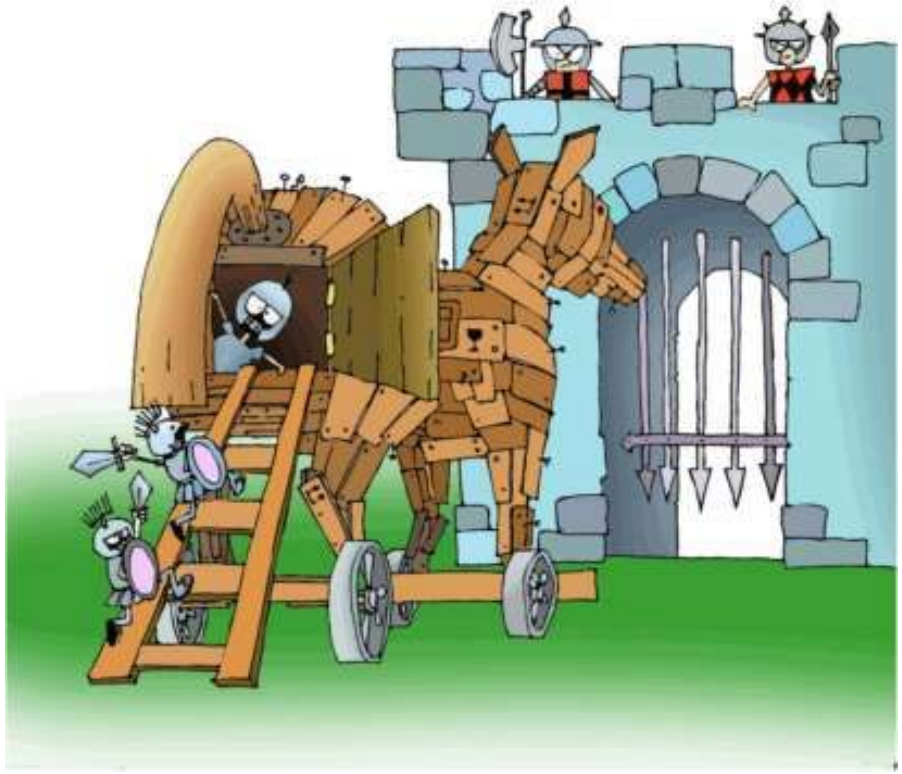
+ при выходе из строя основного диска его заменяет "зеркальный".

- Скорость обмена информации не увеличивается
- Фактическое сокращение дискового пространства



ТРОЯНСКИЕ ПРОГРАММЫ

Троянская программа, троянец (от англ. trojan) – вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удаленному пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.



Троянские программы обычно проникают на компьютер как сетевые черви, а различаются между собой по тем действиям, которые они производят на зараженном компьютере.

ТРОЯНСКИЕ УТИЛИТЫ УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ

Утилиты скрытого управления позволяют принимать или отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т. д.

При запуске троянец устанавливает себя в системе и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях троянской программы в системе.

В 2003 году широкое распространение получила троянская программа Backdoor.Win32.BO, которая осуществляет следующие действия:

- высылает имена компьютера, пользователя и информацию о системе: тип процессора, размер памяти, версию системы, информацию об установленных устройствах;
- посылает/принимает, уничтожает, копирует, переименовывает, исполняет любой файл;
- отключает пользователя от сети;
- читает или модифицирует системный реестр.

ТРОЯНСКИЕ ПРОГРАММЫ - ШПИОНЫ

Троянские программы ворующие информацию, при запуске ищут файлы, хранящие конфиденциальную информацию о пользователе (банковские реквизиты, пароли доступа к Интернету и др.) и отсылают ее по указанному в коде троянца электронному адресу или адресам.

Троянцы данного типа также сообщают информацию о зараженном компьютере (размер памяти и дискового пространства, версию операционной системы, IP-адрес и т. п.).

Некоторые троянцы воруют регистрационную информацию к программному обеспечению.

ТРОЯНСКИЕ ПРОГРАММЫ - ШПИОНЫ

Данные троянцы осуществляют электронный шпионаж за пользователем зараженного компьютера: вводимая с клавиатуры информация, снимки экрана, список активных приложений и действия пользователя с ними сохраняются в каком-либо файле на диске и периодически отправляются злоумышленнику.

Троянские программы этого типа часто используются для кражи информации пользователей различных систем онлайновых платежей и банковских систем.

Троянские программы часто изменяют записи системного реестра операционной системы, поэтому для их удаления необходимо в том числе восстановление системного реестра.

ТРОЯНСКИЕ ПРОГРАММЫ – ИНСТАЛЛЯТОРЫ ВРЕДОНОСНЫХ ПРОГРАММ

Троянские программы этого класса скрытно инсталлируют другие вредоносные программ и используются для «подсовывания» на компьютер-жертву вирусов или других троянских программ.

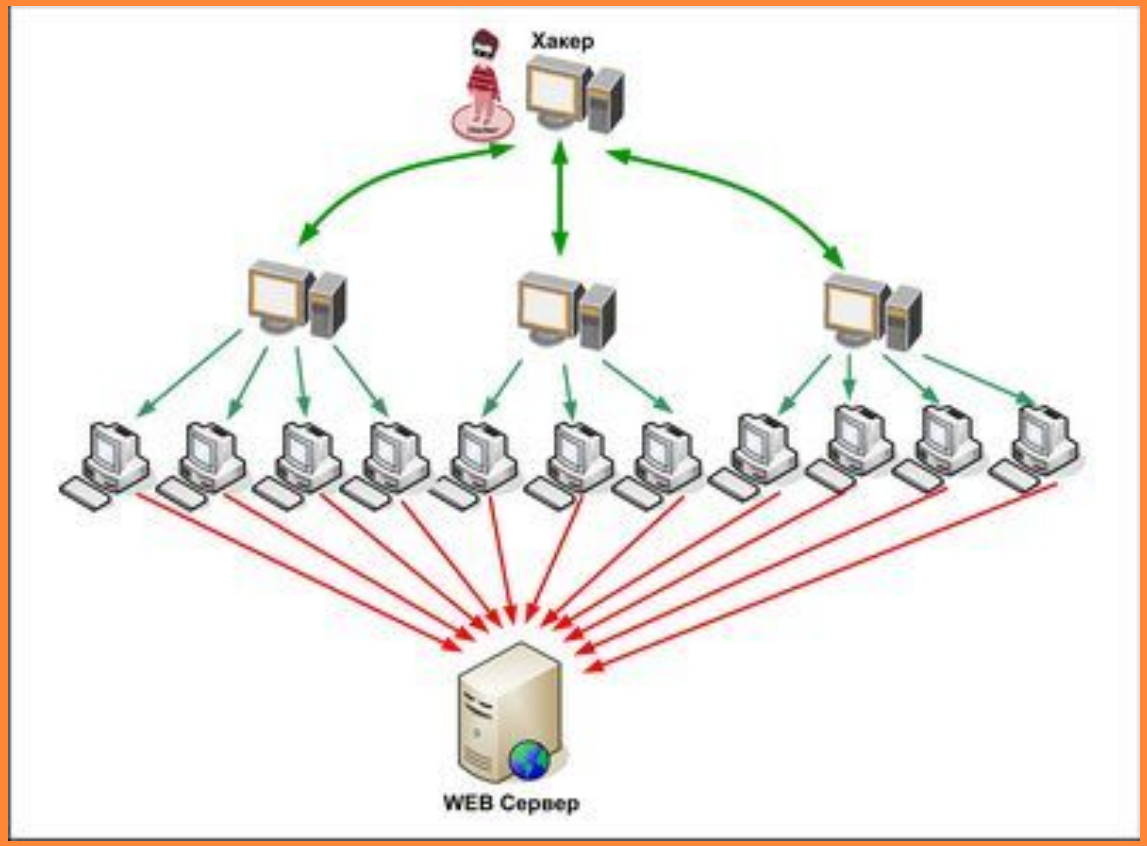
Загруженные без ведома пользователя из Интернета программы либо запускаются на выполнение, либо включаются троянцем в автозагрузку операционной системы.

СЕТЕВЫЕ АТАКИ

Сетевые атаки - направленные действия на удаленные серверы для создания затруднений в работе или утери данных

Сетевые атаки на удаленные серверы реализуются с помощью специальных программ, которые посылают на них специфические запросы.
Это может приводить к отказу в обслуживании «зависанию» сервера.

СЕТЕВЫЕ АТАКИ



Чаще всего при проведении DDoS-атак злоумышленники используют трехуровневую архитектуру

ЗАЩИТА ОТ ХАКЕРСКИХ АТАК И СЕТЕВЫХ ЧЕРВЕЙ

Защита компьютерных сетей или отдельных компьютеров от несанкционированного доступа может осуществляться с помощью межсетевого экрана, или брандмауэра *(от англ. firewall).*

Межсетевой экран позволяет:

1. *блокировать хакерские DoS-атаки, не пропуская на защищаемый компьютер сетевые пакеты с определенных серверов (определенных IP-адресов или доменных имен);*
2. *не допускать проникновение на защищаемый компьютер сетевых червей (почтовых, Web и др.);*
3. *препятствовать троянским программам отправлять конфиденциальную информацию о пользователе и компьютере.*

Межсетевые экраны ZyXEL - защита сети от вирусов, спама, **сетевых атак**.

Межсетевой экран может быть реализован как аппаратно, так и программно.