

Антивирусные средства защиты.


Антивирусные средства защиты.


- Компьютерный вирус - это целенаправленно созданная программа, автоматически приписывающая себя к другим программным продуктам, изменяющая или уничтожающая их. Такая программа обладает способностью самовоспроизведения, распространения, внедрения в другие программы. Компьютерные вирусы могут заразить компьютерные программы, привести к потере данных и даже вывести компьютер из строя.


Виды вирусов и способы защиты от них

Вредоносные программы можно разделить на три класса:

- черви,
- вирусы
- тройные программы.

- 
- *Черви* - это класс вредоносных программ, использующих для распространения сетевые ресурсы. Название этого класса было дано исходя из способности «червей» переползать с компьютера на компьютер, используя сети, электронную почту и другие информационные каналы. Благодаря этому свойству «черви» обладают исключительно высокой скоростью распространения.

- 
- *Вирусы* - это программы, которые заражают другие программы - добавляют в них свой код, чтобы получить управление при запуске зараженных файлов. Основное действие, выполняемое вирусом, - **заражение**. Скорость распространения вирусов ниже, чем у «червей».

- 
- *Троянские программы* - программы, которые выполняют на поражаемых компьютерах несанкционированные пользователем действия, т. е. в зависимости от каких-либо условий уничтожают информацию на дисках, приводят систему к зависанию, воруют конфиденциальную информацию. Троянские программы не способны самостоятельно проникать на компьютеры и распространяются злоумышленниками под видом полезного программного обеспечения

Это интересно!

- В 1972 г. Агентство национальной безопасности США предупредило создателей компьютеров о возможности появления программ со «скрытой начинкой», которая может наносить вред компьютеру. Позднее они получили название «Троянский конь».



В зависимости от среды обитания вирусы можно

разделить на:


сетевые,

файловые,

загрузочные

файлово-загрузочные


-
- **Сетевые вирусы** распространяются по различным компьютерным сетям.
 - **Файловые вирусы** внедряются главным образом в исполняемые модули, т.е. в файлы, имеющие расширения **COM** и **EXE**. **Файловые вирусы** могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах они никогда не получают управление и, следовательно, теряют способность к размножению.

- 
- Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-сектор) или сектор, содержащий программу загрузки системного диска (Master Boot Record).
 - Файлово-загрузочные вирусы заражают файлы и загрузочные сектора дисков.



По способу заражения вирусы
разделяются на

резидентные
нерезидентные.

- 
- ~~*Резидентный вирус*~~ при заражении компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т.д.) и внедряется в них. **Резидентные вирусы** находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.
 - *Нерезидентные вирусы* не заражают память компьютера и являются активными ограниченное время.

По степени воздействия выделяют

- **неопасные вирусы,**
которые не мешают работе компьютера,
- **опасные вирусы,**
которые могут привести к различным нарушениям в работе компьютера
- **очень опасные вирусы,**
воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

развитие вируса проходит следующие этапы

- **скрытый этап**, когда действие вируса не проявляется и остается незамеченным;
- • **этап лавинообразного размножения**, но его действия при этом еще не активизированы;
- • **этап активного действия**, когда вирус начинает выполнять вредные действия, заложенные программистом.

К основным методам защиты от вирусов относятся:

- наличие многофункциональной **антивирусной программы**, включающейся автоматически при загрузке компьютера;
- • периодический поиск вирусов и антивирусная профилактика всех внешних носителей информации;
- • уничтожение обнаруженных вирусных программ;
- резервирование на диске областей системных файлов;
- общее резервирование существующих файлов;
- дефрагментация дисков.

Назначение антивирусных программ и их виды

Антивирусные программы предназначены для антивирусной защиты персональных компьютеров и выполняют следующие функции:

- ❑ **защита от вирусов и вредоносных программ**
- ❑ **постоянная защита компьютера**
- ❑ **проверка компьютера по требованию**
- ❑ **восстановление работоспособности после вирусной атаки**
- ❑ **проверка и «лечение» входящей-исходящей почты**
- ❑ **обновление антивирусных баз и программных модулей**
- ❑ **рекомендации по настройке программы и работе с ней**

Классификация антивирусных программ.

- *Программы-детекторы* осуществляют поиск характерной для конкретного вируса **сигнатуры** (последовательность байтов, которая вполне определенно его характеризует) в оперативной памяти и файлах и при обнаружении выдают соответствующее сообщение.

Классификация антивирусных программ.

- *Программы-доктора (фаги), а также программы-вакцины* не только находят зараженные вирусами файлы, но и возвращают файлы в исходное состояние.

Наиболее известны программы **Norton AntiVirus, DrWeb, Антивирус Касперского.**

Классификация антивирусных программ

- *Программы-ревизоры* запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаружение изменения выводится на экран монитора.

К числу программ-ревизоров относится широко распространенная в России программа **Adinf**.

Классификация антивирусных программ.

Программы-фильтры, или *сторож*, представляют собой небольшие **резидентные** программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:

- попытка коррекции файлов с расширениями **COM** и **EXE**;
- изменение атрибутов файла;
- прямая запись на диск по абсолютному адресу;
- запись в загрузочные сектора диска;
- загрузка резидентной программы.

Но они не «лечат» файлы и диски.

Примером программы-фильтра является программа **Vsafe**.

Классификация антивирусных программ.

- *Вакцины или иммунизаторы*, - это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют **программы-доктора**, «лечащие» этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрятся

Российские антивирусные программы.

В России антивирусными проблемами уже много лет профессионально занимаются в основном две фирмы:

- «Диалог Наука» (www.dialognauka.ru) создатель программ **Aidstest**, **Doctor WEB**, **ADinf**, комплекса **Sheriff**,
- «Лаборатория Касперского» (www.kaspersky.ru) создатель **Kami** и программ серии «Антивирус Касперского».

Web- страница фирмы «ДиалогНаука»

Dr. Web, Sophos, Antigen и др. антивирусы, антиспам, персональные и офисные сетевые экраны (Fire - ...)

www.dialognauka.ru

ДиалогНаука
На страже здоровья и безопасности Ваших компьютеров

«ДиалогНаука» разработала политику антивирусной защиты ОАО «МТС» **ПОДРОБНЕЕ**

Главная Справка Новости Контакты Политика конфиденциальности Мировые Партнеры Пресс-релизы О нас

купить со скидкой Авторизация Новый пользователь Онлайн-проблема на экране

РЕШЕНИЯ

- Малому и среднему бизнесу
- Корпоративным клиентам
- Предприятиям
- Решениям для сетевых ресурсов

УСЛУГИ

- Проведение аудита безопасности
- Разработка Политики информационной безопасности
- Внедрение комплексных систем защиты
- Техническое сопровождение
- Обучение

ПРОДУКТЫ

- Купить продукты
- Описание продуктов
- Получить каталог продуктов

Решения

Для комплексной защиты от информационных угроз компания «ДиалогНаука» предлагает высокоэффективные решения для малого и среднего бизнеса, а также крупных коммерческих и государственных организаций. [Подробнее](#)

Услуги

Компания «ДиалогНаука» предлагает широкий спектр услуг по разработке, внедрению и сопровождению комплексных систем защиты, включая: аудит безопасности, разработку концепций информационной и антивирусной безопасности, техническую поддержку и другие. [Подробнее](#)

Продукты

Продукты мировых лидеров информационной безопасности, предлагаемые компанией «ДиалогНаука», обеспечивают высокий уровень конфиденциальности, доступности и целостности информационных ресурсов предприятия. [Подробнее](#)

ПОДРОБНЕЕ

10.11.2006 «ДиалогНаука» представила на российском рынке локализованный антивирус Sophos Small Business Edition 2.0

01.10.2006 10 ноября в гостинице «Рэдиссон САС Славянская» компания «ДиалогНаука» проведет открытый партнерский семинар-пресс-конференцию «Презентация русской версии Sophos Small Business Edition 2.0»

05.10.2006 Новость для лицензионных пользователей программных продуктов от «ДиалогНауки»: предложение скидки на получение высшего образования по программе MBA

01.10.2006 6 октября компания «ДиалогНаука» проведет тренинг по новой версии решений компании Sophos для SMB – Sophos Small Business Solutions v 2.0

Интернет

Web-страница «Лаборатория Касперского»

Лаборатория Касперского | Антивирус | Microsoft Internet Explorer

Адрес: <http://www.kaspersky.ru/>

Выберите сайт: **Russia** | Загрузить пробную версию | Купить Антивирус онлайн

лаборатория **КАСПЕРСКОГО**

Продукты
[Электронный магазин](#)
[Корпоративные решения](#)
[Угрозы](#)
[Сервис](#)
[Загрузить](#)
[Партнеры](#)
[О компании](#)

НОВОЕ ПОКОЛЕНИЕ ПРОДУКТОВ

Версия 5.0
Антивирус Касперского
Kaspersky Internet Security

ПОДРОБНЕЕ
НОВЫЕ ТЕХНОЛОГИИ
ДОМАШНИЕ ПОЛЬЗОВАТЕЛИ | МАЛЫЙ И СРЕДНИЙ БИЗНЕС | КОРПОРАТИВНЫЕ КЛИЕНТЫ

Viruslist
Крупнейшая вирусная энциклопедия

Вирусная эпидемия
[Email-Worm Win32/Warezov](#)
Статус: средняя опасность

[Онлайн-проверка на вирусы](#)

[Вирусная энциклопедия](#)
[Веблог "Лаборатории Касперского"](#)
[Вирусные новости](#)

Постоянная защита

[Обновление баз](#)
[Обновление продуктов](#)
[Бесплатные утилиты](#)
[Техподдержка](#)
[База знаний](#)
[Форум](#)
[Прислать вирус](#)

[Продлить лицензию](#)
[Купить у партнеров](#)
[Купить онлайн](#)

Новости

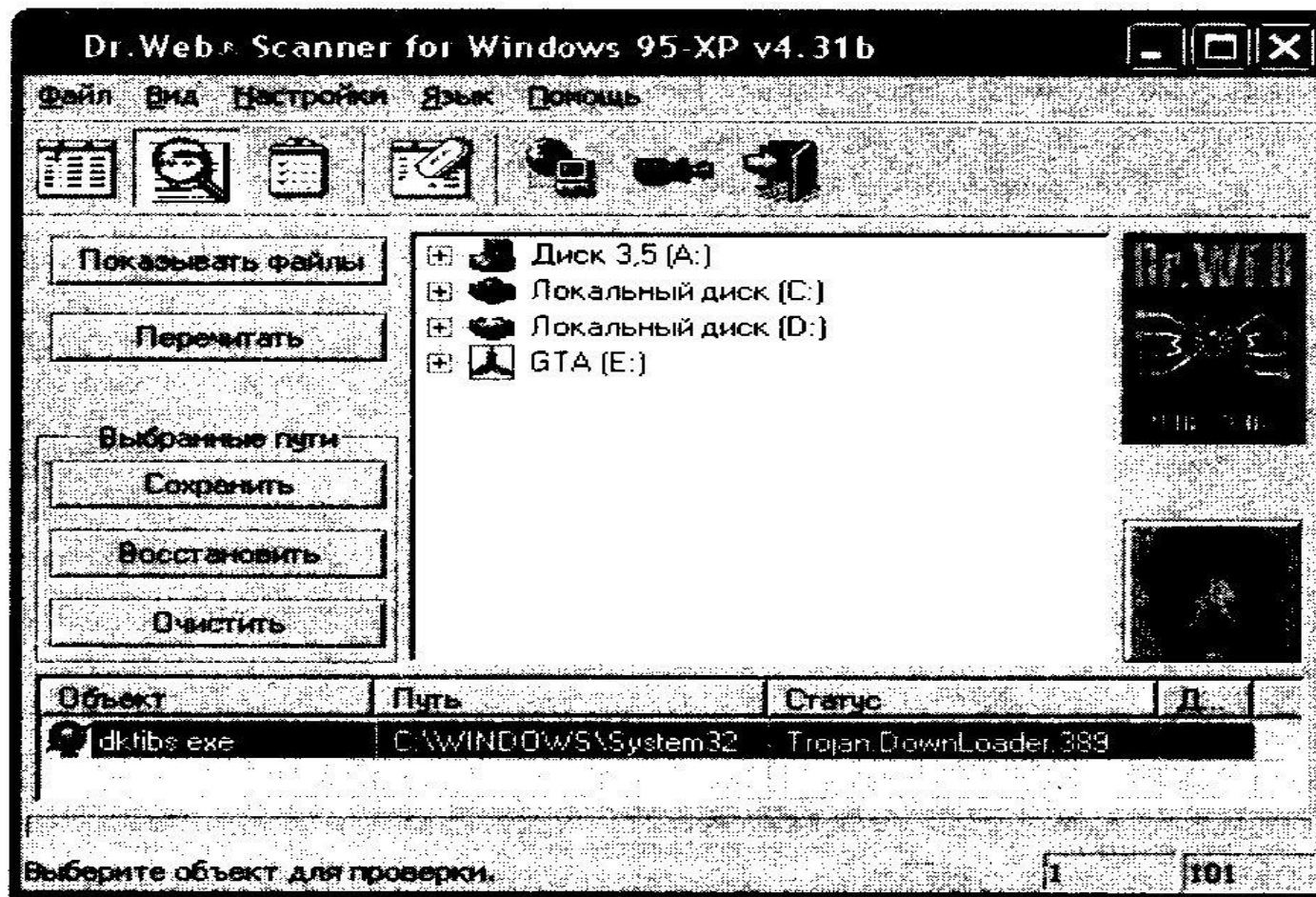
13.11
[Kaspersky Internet Security 6.0 – победитель теста немецкого журнала PC Magazin](#)

10.11
[Завершилась IV конференция «Проблема спама и ее решения»](#)

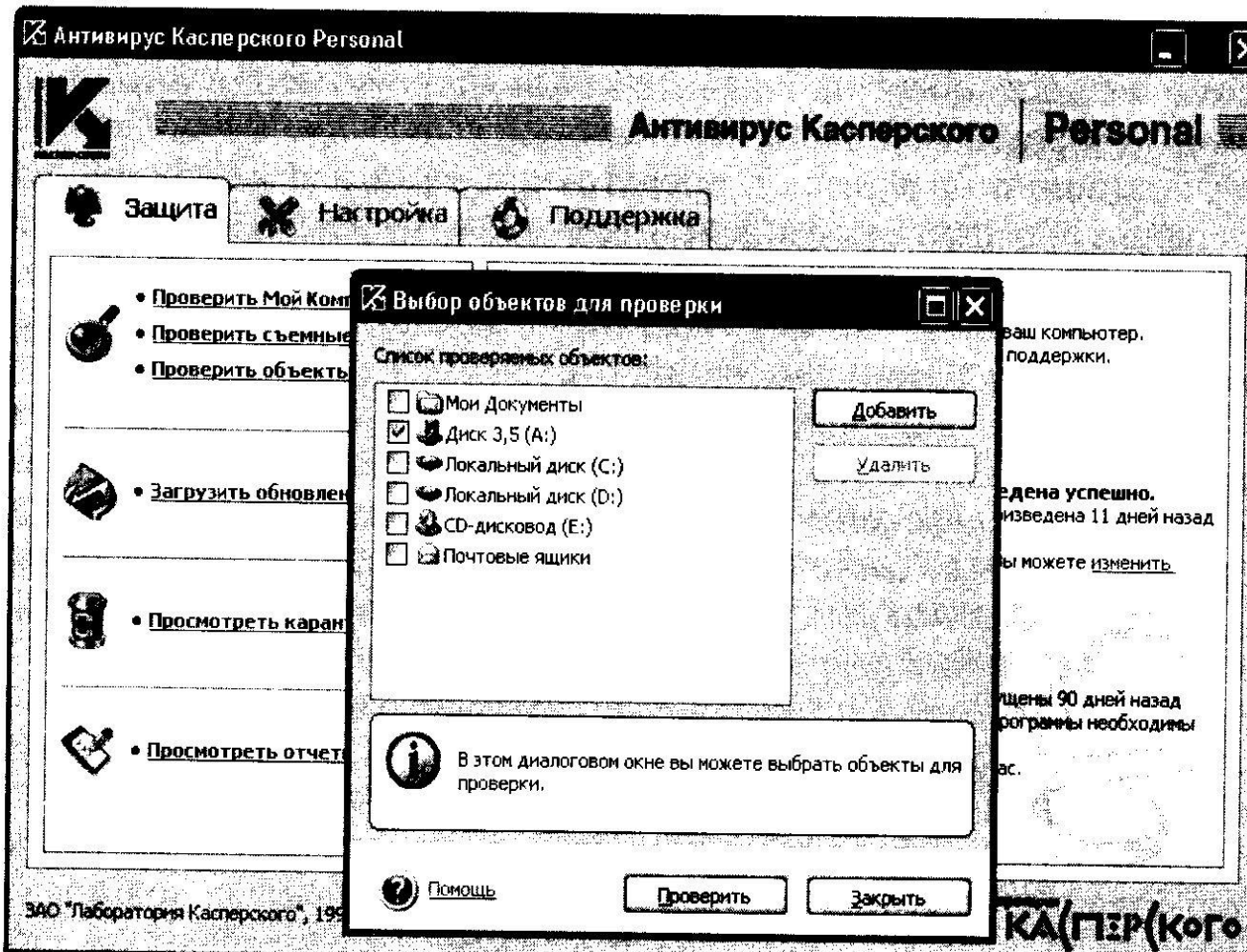
[Все новости](#) | [Подписаться](#)

Kaspersky Security Bulletin | Задай вопрос Евгению Касперскому

Интерфейс антивирусной программы Doctor Web




Окно программы «Антивирус Касперского»



Российские антивирусные программы.

- Сегодняшняя версия программа **Doctor WEB** имеет удобный, интуитивно понятный и наглядный графический интерфейс. Что касается возможностей по поиску вирусов, то их высокая оценка подтверждается победами в тестах авторитетного международного журнала **Virus Bulletin**.
- «**Лаборатория Касперского**» является крупнейшим российским разработчиком антивирусных систем безопасности, ведь примерно половина российских пользователей выбрала качество и надежность антивирусных программ этой фирмы. Разработка основного продукта «**Лаборатории Касперского**» - антивирусного комплекса «**Антивирус Касперского**» серии **AVP** - началась в **1989г.**
- «**Лаборатория Касперского**» - признанный лидер в антивирусных технологиях .



**Лучший способ лечения - это профилактика заболевания.
Желательно установить на компьютере антивирусный
монитор (сторож) - резидентную антивирусную
программу, которая постоянно находится в
оперативной памяти и контролирует операции
обращения к файлам и секторам.**

**Примерами таких программ является McAfee VirusShield
(антивирусный комплект McAfee VirusScan) и AVP
Monitor (AntiViral Toolkit Pro. Касперского).**

Признаки заражения компьютера вирусом.

- • вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- неожиданное открытие и закрытие лотка CD-ROM-устройства;
- • произвольный, без вашего участия, запуск на компьютере каких-либо программ;
- • вывод на экран предупреждения о попытке какой-либо из программ вашего компьютера выйти в Интернет, хотя вы никак не инициировали такое ее поведение

Защита информации от несанкционированного доступа

- **Окинавская хартия глобального информационного общества от 22.07.2000 г.** подписана руководителями восьми развитых стран мира, в том числе Президентом
- Подписание **Окинавской хартии** глобального информационного общества продемонстрировало совпадение представлений руководства России и других развитых государств об информационно коммуникационных технологиях как важном факторе формирования общества XXI в.

Цели защиты информации.

- • предотвращение утечки, хищения, утраты, искажения, подделки информации;
- • предотвращение угроз безопасности личности, общества, государства;
- • предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
- • защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющих в информационных системах;
- • сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
- • обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Классификация мер защиты информации.

Меры защиты информации подразделяются на три уровня:

- законодательный,**
- административный и процедурный;**
- программно-технический.**

Законодательный уровень.

**В гл. 28 «Преступления в сфере компьютерной информации» УК РФ содержатся три статьи:
СТ. 272 «Неправомерный доступ к компьютерной информации», СТ. 273
«Создание, использование и распространение вредоносных программ для ЭВМ», СТ. 274
«Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети».**

Административный и процедурный уровень.

На административном и процедурном уровне формируется политика безопасности и комплекс процедур, определяющих действия персонала в штатных и критических условиях. Этот уровень защиты информации зафиксирован в руководящих документах, выпущенных Гостехкомиссией РФ .

Программно-технический уровень

- К этому уровню защиты информации относятся **программные и аппаратные средства**, которые составляют технику информационной безопасности. К программным и аппаратным средствам относятся и **идентификация** пользователей, и **управление доступом**, и **криптография**, и **экранирование**, и многое другое.



Это интересно !

1976г. - год рождения компьютерного пиратства. В печати публикуется открытое письмо Билла Гейтса, который жалуется на незаконное использование обладателями первых микрокомпьютеров программного обеспечения, выпускаемого фирмой Microsoft.


Системы и средства защиты информации.

- • **системы защиты информации от несанкционированного доступа в локальных сетях и из сети Интернет;**
- **системы антивирусной защиты информации;**
- **криптографические системы защиты информации;**
- **средства анализа защищенности информационных систем;**
- **технические средства защиты информации;**
- **технические средства обнаружения каналов утечки информации**


Защита информации от несанкционированного доступа


Среди методов защиты информации от несанкционированного доступа можно выделить следующие:

- **ограничение доступа;**
- **разграничение доступа;**
- **разделение доступа (привилегий) и др.**



Ограничение доступа предполагает, что удовлетворить свои информационные потребности в той или иной вычислительной системе может лишь пользователь, имеющий на это право (зарегистрированный пользователь). Доступ в систему для незарегистрированного пользователя запрещен. Получив доступ в систему (пройдя процедуру идентификации и аутентификации), каждый пользователь реализует свои информационные потребности в соответствии со спектром возможностей, определенных для данной группы пользователей.

- 
- *Разграничение доступа* в вычислительной системе заключается в разделении циркулирующей в ней информации на модули и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями. (т. е. защита информации от нарушителей среди тех пользователей, которым разрешен доступ в систему.) Для реализации такого разграничения используется **идентификация пользователей (создается система идентификаторов личности)**.). При этом широко распространено применение **кодов** (паролей) .

- 
- *Разделение доступа (привилегий)* - это принцип реализации механизма защиты данных, когда для доступа к ним необходимо указать не один, а несколько паролей (несколькими пользователями). Разделение привилегий на доступ к информации заключается в том, что из числа допущенных к ней должностных лиц (пользователей) выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.

Идентификация пользователей.

- **Идентификация** - это присвоение какому-либо объекту или субъекту, реализующему доступ к вычислительной системе, уникального имени (**логина**), **образа** или **числового значения**.

Установление подлинности (**аутентификация**) заключается в проверке, является ли данный объект (субъект) на самом деле тем, за кого себя выдает. Конечная цель **идентификации** и установления подлинности объекта (субъекта) в вычислительной системе - его допуск к информации ограниченного пользования в случае положительного результата проверки или отказ в допуске в случае *отрицательного* результата. **Любая процедура идентификации пользователя предполагает ввод логина и пароля.**

Криптография.

- *Криптография* (от гр. *kryptos* - тайный + *grapho* - пишу)- _ тайнопись, система изменения письма с целью сделать текст непонятным для непосвященных лиц. Для шифрования используют специальные программы, шифрующие информацию перед ее передачей. Для **дешифрования** принимающая сторона должна иметь **специальный код (ключ)**, позволяющий вернуть информации первоначальный вид. Одной из известных систем шифрования является программа **PGP**, позволяющая надежно защитить от прочтения файлы, хранящиеся на диске, и электронную почту, находящуюся на пути к адресату.

Защита компьютеров, подключенных к сети

- Существует особый класс программ для защиты компьютеров, подключенных к сети. Такие программы называются **брандмауэрами** (от нем. **brandmauer** - **противопожарная стена**). Есть у этих программ и другое не менее распространенное английское название - **firewall**, что означает «специальная перегородка в автомобиле, которая защищает пассажирский салон от огня в случае воспламенения двигателя».

Наиболее распространены системы **Internet Connection Firewall**, **Kaspersky Anti-Hacker**, **Outpost Firewall Pro**, **Internet Connection Firewall**.

Брандмауэр Internet Connection Firewall входит в стандартную поставку Windows XP.

Он довольно успешно защищает пользователей от хакерских атак, однако не контролирует деятельность программ, установленных на компьютере, предоставляя «троянским коням», шпионским модулям и вирусам свободу действий. К тому же он не предоставляет пользователю вспомогательной информации, такой как данные об адресе, с которого производилась атака.

Поэтому предпочтительней установить брандмауэр типа Kaspersky Anti- Hacker.

Правила защиты данных.

- Подготовьте дискету аварийной загрузки**
- Следите за состоянием жесткого диска**
- Делайте резервные копии наиболее важных данных**
- Помните о вирусах**
- Аккуратно обращайтесь с программами**
- Пользуйтесь последними версиями драйверов.**
- Не допускайте загрязнения оборудования**
- Соблюдайте процедуру выключения компьютера**

Вопросы для самоконтроля.

- **Что такое компьютерный вирус?**
- **Как защититься от вирусной атаки?**
- **Какие виды вирусов вы знаете?**
- **Перечислите классы антивирусных программ.**
- **Перечислите признаки вирусного заражения компьютера.**
- **Какие мероприятия следует проводить для профилактики вирусного заражения компьютера?**
- **каковы цели защиты информации?**
- **перечислите меры защиты информации.**
- **перечислите системы и средства защиты информации.**
- **Перечислите методы защиты информации.**
- **Что такое идентификация?**
- **Что такое криптография?**
- **Как защитить компьютеры , подключенные к сети?**