# Защита информации

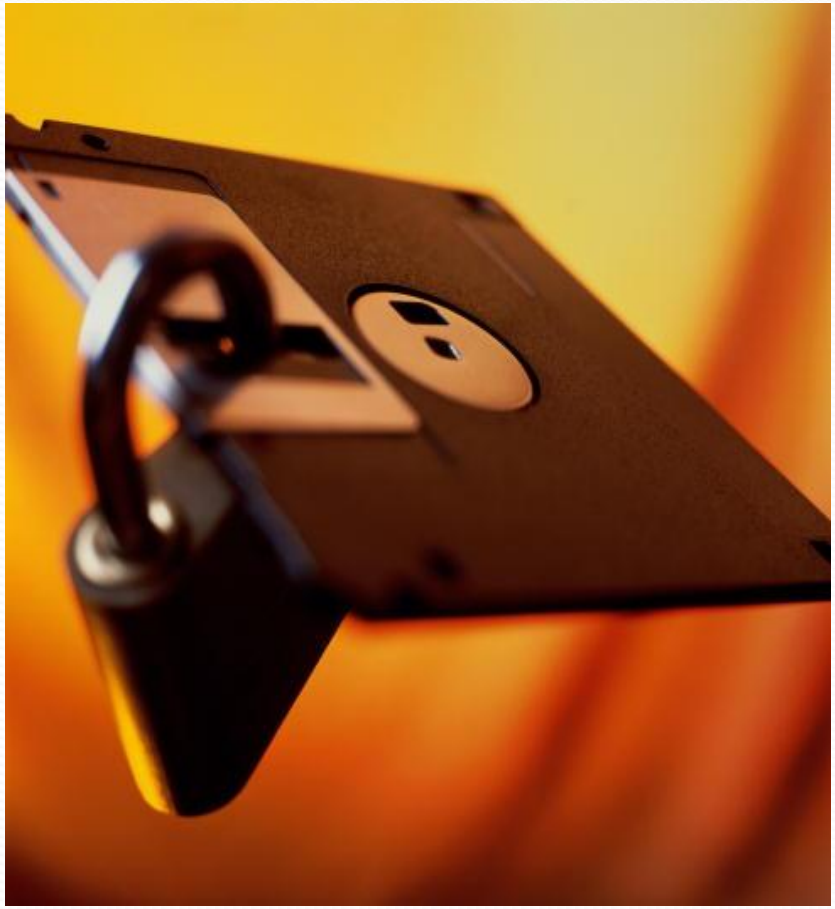
# Содержание работы

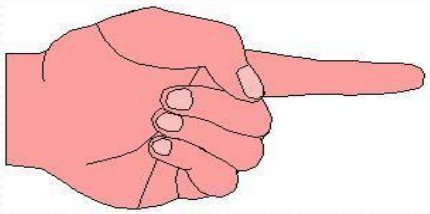
- Защита информации.
  1. Защита с использованием паролей.
  2. Биометрические системы защиты.
- Физическая защита данных на дисках.
- Защита от вредоносных программ.
  1. Вредоносные и антивирусные программы.
  2. Компьютерные вирусы и защита от них.
  3. Троянские программы и защита от них.

# Защита информации

***Защита*** - система мер по обеспечению безопасности с целью сохранения государственных и коммерческих секретов. Защита обеспечивается соблюдением режима секретности, применением охранных систем сигнализации и наблюдения, использованием шифров и паролей.

***Защита информации*** представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.





# Безопасность

Конфиденциальность

Целостность

Доступность

***Информационная безопасность*** — это состояние защищённости информационной среды.

В вычислительной технике понятие безопасности подразумевает

- надежность работы компьютера,
- сохранность ценных данных,
- защиту информации от внесения в нее изменений неуполномоченными лицами,
- сохранение тайны переписки в электронной связи.

# 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.

***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

- каждый диск,
- каждая папка,
- каждый файл локального компьютера.

Для них могут быть установлены определенные права доступа

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

Права могут быть различными для различных пользователей.

# Биометрические системы защиты

В настоящее время для защиты от несанкционированного доступа к информации все более часто 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 идентиф

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

# 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.

# 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, соот нтраста (брови, глаза, нос, у

# 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).

# Физическая защита данных на дисках

Для обеспечения большей скорости чтения, записи и надежности хранения данных на жестких дисках используются RAID-массивы (Redundant Arrays of Independent Disks - избыточный массив независимых дисков). Несколько жестких дисков подключаются к RAID - контроллеру, который рассматривает их как единый логический носитель информации.

# Способы реализации RAID-массива

***Аппаратный***

Аппаратный дисковый массив состоит из нескольких жестких дисков, управляемых при помощи специальной платы контроллера RAID-массива.

***Программный***

Программный RAID-массив реализуется при помощи специального драйвера. В программный массив организуются дисковые разделы, которые могут занимать как весь диск, таки его часть. Программные RAID-массивы, как правило, менее надежны, чем аппаратные, но обеспечивают более высокую скорость работы с данными.

# Защита от вредоносных программ

**Вредоносная программа** (буквальный перевод англоязычного термина **Malware**, **mal***icious* — злонамеренный и *soft***ware** — программное обеспечение, жаргонное название — «малварь», «маловарь», «мыловарь» и даже «мыловарня») — злонамеренная программа, то есть программа, созданная со злым умыслом и злыми намерениями.

# Вредоносные программы

**Вирусы, черви, троянские и хакерские программы**

**Шпионское, рекламное программное обеспечение**

**Потенциально опасное программное обеспечение**

# 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

***Для поиска известных вредоносных программ*** используются сигнатуры. ***Сигнатура*** — это некоторая постоянная последовательность программного кода, специфичная для конкретной вредоносной программы. Если антивирусная программа обнаружит такую последовательность в каком-либо файле, то файл считается зараженным вирусом и подлежит лечению или удалению.

***Для поиска новых вирусов*** используются алгоритмы эвристического сканирования, т. е. анализа последовательности команд в проверяемом объекте. Если «подозрительная» последовательность команд обнаруживается, то антивирусная программа выдает сообщение о возможном заражении объекта.

# Признаки заражения компьютера

- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- неожиданное открытие и закрытие лотка CD/DVD дисковода;
- произвольный запуск на компьютере каких-либо программ;
- частые зависания и сбои в работе компьютера;
- медленная работа компьютера при запуске программ;
- исчезновение или изменение файлов и папок;
- частое обращение к жесткому диску (часто мигает лампочка на системном блоке);
- зависание или неожиданное поведение браузера (например, окно программы невозможно закрыть).

# Действия при наличии признаков заражения компьютера

Прежде чем предпринимать какие-либо действия, необходимо сохранить результаты работы на внешнем носителе (дискете, CD- или DVD-диске, флэш-карте и пр.).

Далее необходимо:

- отключить компьютер от локальной сети и Интернета, если он к ним был подключен;
- если симптом заражения состоит в том, что невозможно загрузиться с жесткого диска компьютера (компьютер выдает ошибку, когда вы его включаете), попробовать загрузиться в режиме защиты от сбоев  или с диска аварийной загрузки Windows;
- запустить антивирусную программу.

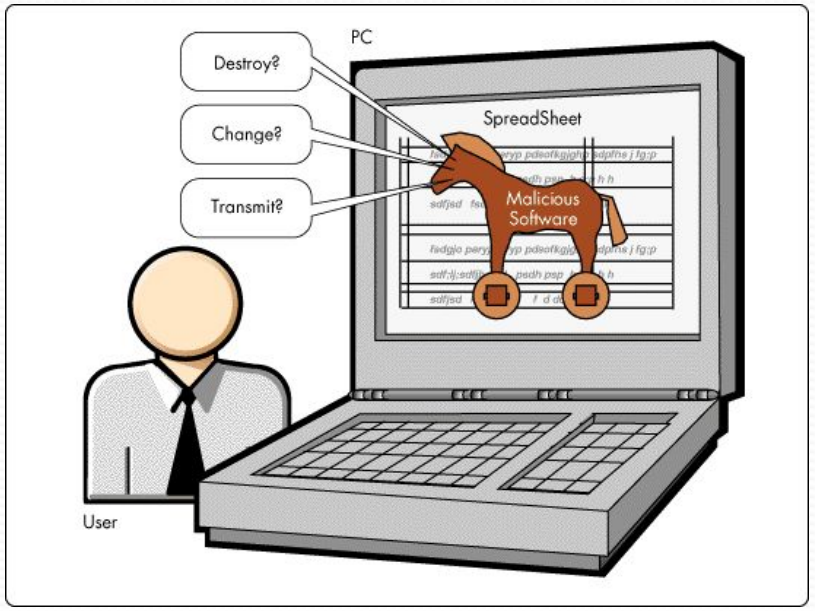
# Компьютерные вирусы и защита от них

***Компьютерные вирусы*** являются вредоносными программами, которые могут «размножаться» (самокопироваться) и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

***По «среде обитания» вирусы*** можно разделить на загрузочные, файловые и макровирусы.

# Троянские программы и защита от них

***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 - шпионы

***Троянские программы — шпионы*** 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.