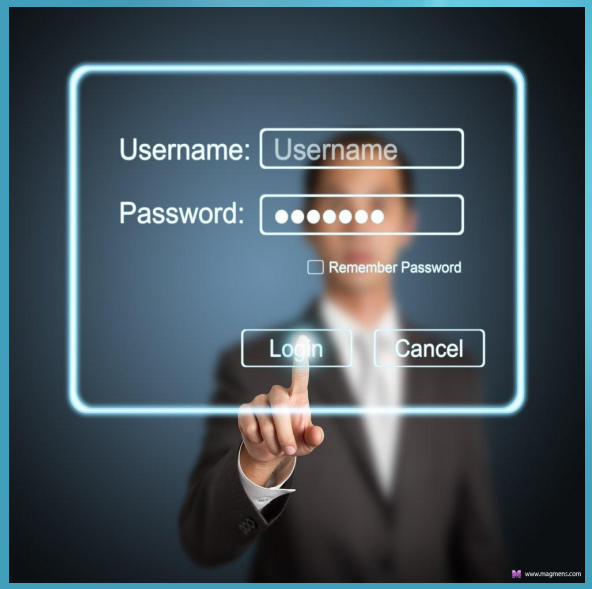
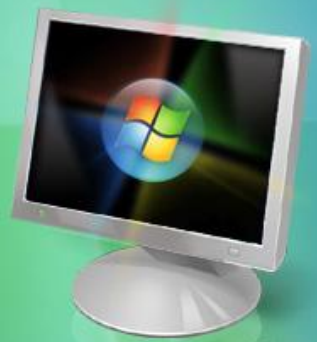
Защита собственной информации от несанкционированного доступа



Подготовила презентацию
Елена Петрова

Г. Майкопа СОШ № 10

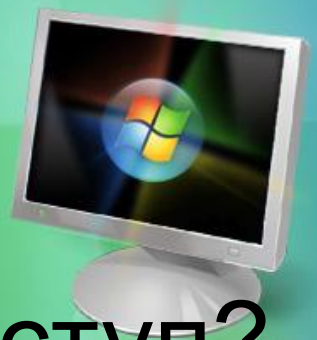


Что такое несанкционированный доступ к информации?

- **несанкционированный доступ**
  Доступ к информации или к ресурсам автоматизированной инф ормационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа.

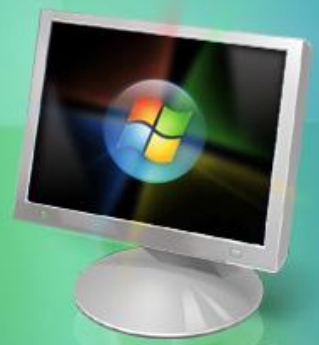
Несанкционированный доступ может быть осуществлен предна меренно или непреднамеренно.

Права и правила доступа к информации и ресурсам информац ионной системы устанавливаются для процессов обработки информации, обслуживания автоматизиро ванной информационной системы, изменения программных, технических и информационных ресур сов, а также получения информации о них

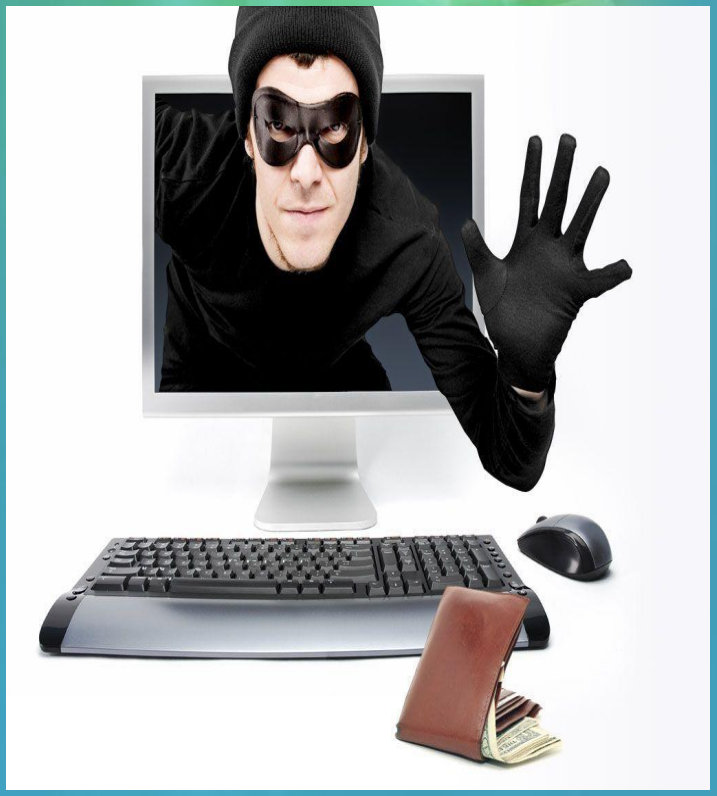


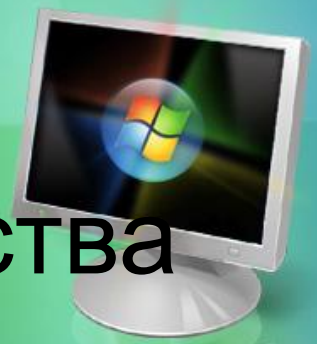
Чем опасен несанкционированный доступ?

- ***Несанкционированный доступ (НСД) злоумышленника на компьютер опасен не только возможностью прочтения и/или модификации обрабатываемых электронных документов, но и возможностью внедрения злоумышленником управляемой программной закладки, которая позволит ему предпринимать следующие действия:***
  - Читать и/или модифицировать электронные документы, которые в дальнейшем будут храниться или редактироваться на компьютере.
  - Осуществлять перехват различной ключевой информации, используемой для защиты электронных документов.
  - Использовать захваченный компьютер в качестве плацдарма для захвата других компьютеров локальной сети.
  - Уничтожить хранящуюся на компьютере информацию или вывести компьютер из строя путем запуска вредоносного программного обеспечения.



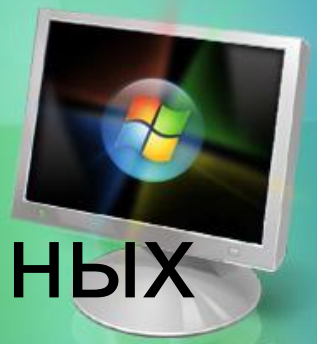
- Иногда интернет-пользователь может по своей наивности сообщить свой логин и пароль от аккаунта сам. Все это происходит в соцсети из-за невнимательного выбора людей,которые впоследствии будут значиться в списке «друзья». Мошенник даже может обокрасть вас таким образом.





Методы защиты или средства борьбы:

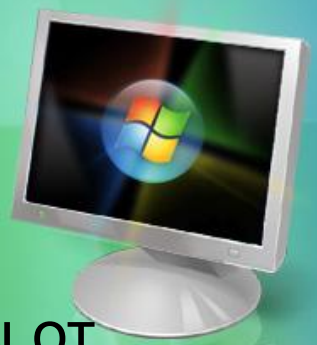
- **Средства ограничения физического доступа**
- обычно выполняемые ответственным лицом – Администратором по безопасности:
  - Создание списка пользователей, которым разрешен доступ на защищаемый компьютер. Для каждого пользователя формируется ключевой носитель (в зависимости от поддерживаемых конкретным замком интерфейсов – дискета, электронная таблетка iButton или смарт-карта), по которому будет производиться аутентификация пользователя при входе. Список пользователей сохраняется в энергонезависимой памяти замка.
  - Формирование списка файлов, целостность которых контролируется замком перед загрузкой операционной системы компьютера. Контролю подлежат важные файлы операционной системы, например, следующие:
    - системные библиотеки Windows;
    - исполняемые модули используемых приложений;
    - шаблоны документов Microsoft Word и т. д.



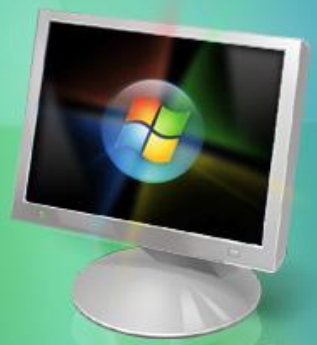
Использование электронных замков:

Существуют электронные замки, способные блокировать корпус системного блока компьютера изнутри специальным фиксатором по команде администратора – в этом случае замок не может быть изъят без существенного повреждения компьютера.

Довольно часто электронные замки конструктивно совмещаются с аппаратным шифратором. В этом случае рекомендуемой мерой защиты является использование замка совместно с программным средством прозрачного (автоматического) шифрования логических дисков компьютера. При этом ключи шифрования могут быть производными от ключей, с помощью которых выполняется аутентификация пользователей в электронном замке, или отдельными ключами, но хранящимися на том же носителе, что и ключи пользователя для входа на компьютер. Такое комплексное средство защиты не потребует от пользователя выполнения каких-либо дополнительных действий, но и не позволит злоумышленнику получить доступ к информации даже при вынутой аппаратуре электронного замка.



- Наиболее действенными методами защиты от несанкционированного доступа по компьютерным сетям являются виртуальные частные сети (VPN – Virtual Private Network) и межсетевое экранирование. Рассмотрим их подробно.
- *Виртуальные частные сети*
- Виртуальные частные сети обеспечивают автоматическую защиту целостности и конфиденциальности сообщений, передаваемых через различные сети общего пользования, прежде всего, через Интернет. Фактически, VPN – это совокупность сетей, на внешнем периметре которых установлены VPN-агенты.



- VPN-агент – это программа (или программно-аппаратный комплекс), собственно обеспечивающая защиту передаваемой информации путем выполнения описанных ниже операций. Перед отправкой в сеть любого IP-пакета VPN-агент производит следующее: