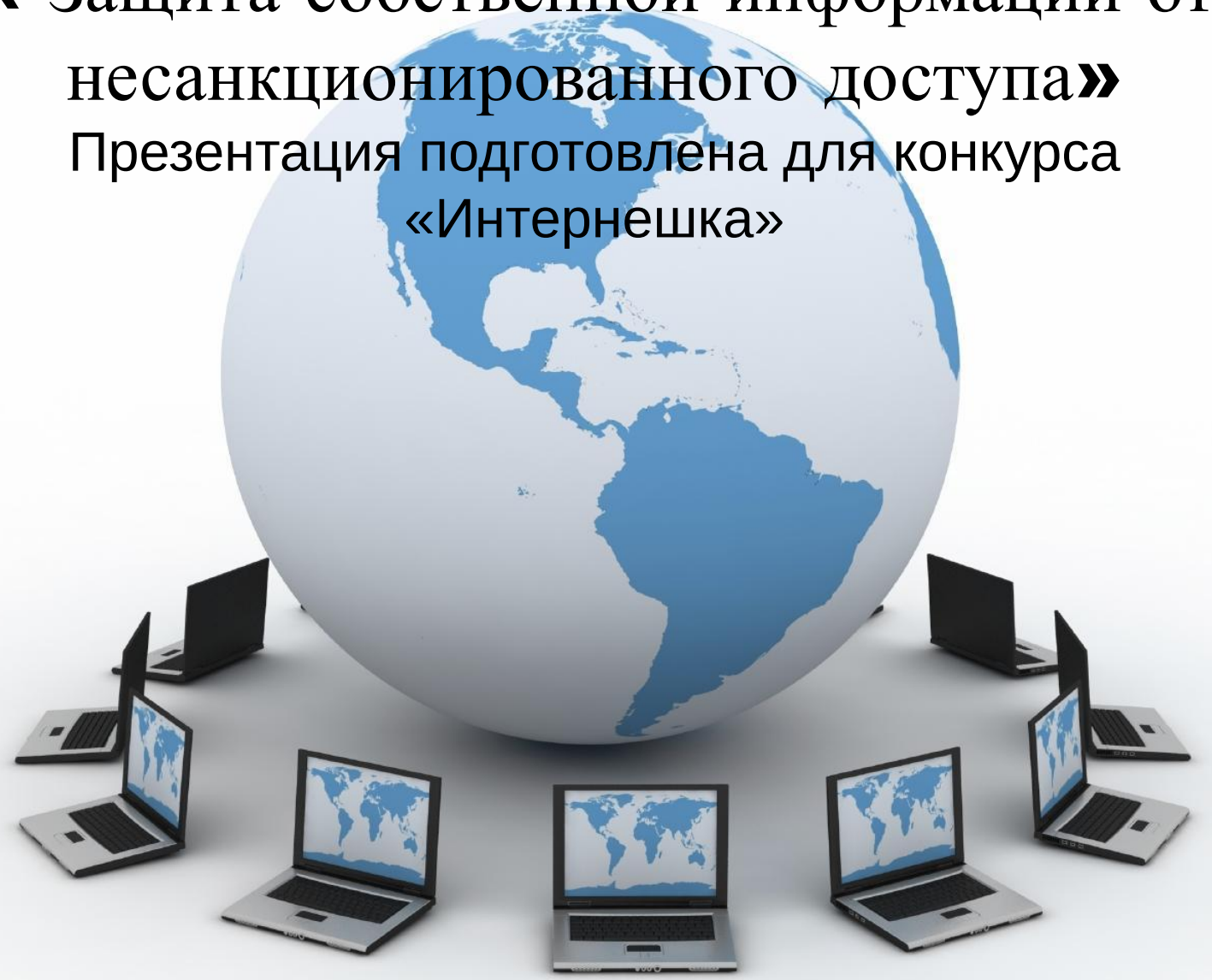
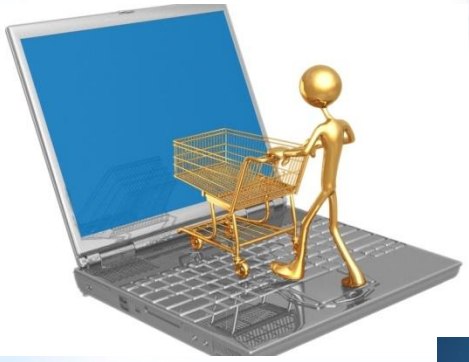
« Защита собственной информации от несанкционированного доступа»

Презентация подготовлена для конкурса «Интернешка»



Выполнила: Кулагина Екатерина,
МБОУ Гимназия №22

В последние годы сеть Интернет превратилась в глобальную среду передачи информации. В связи с этим возрастает роль механизмов регулирования информационных отношений в обществе, которые должны включать эффективное законодательство, предусматривающее, в частности, охрану авторского права, коммерческой и личной тайн, защиту потребителей от ложной информации, ответственность за пиратское распространение информации и защиту товарных знаков.

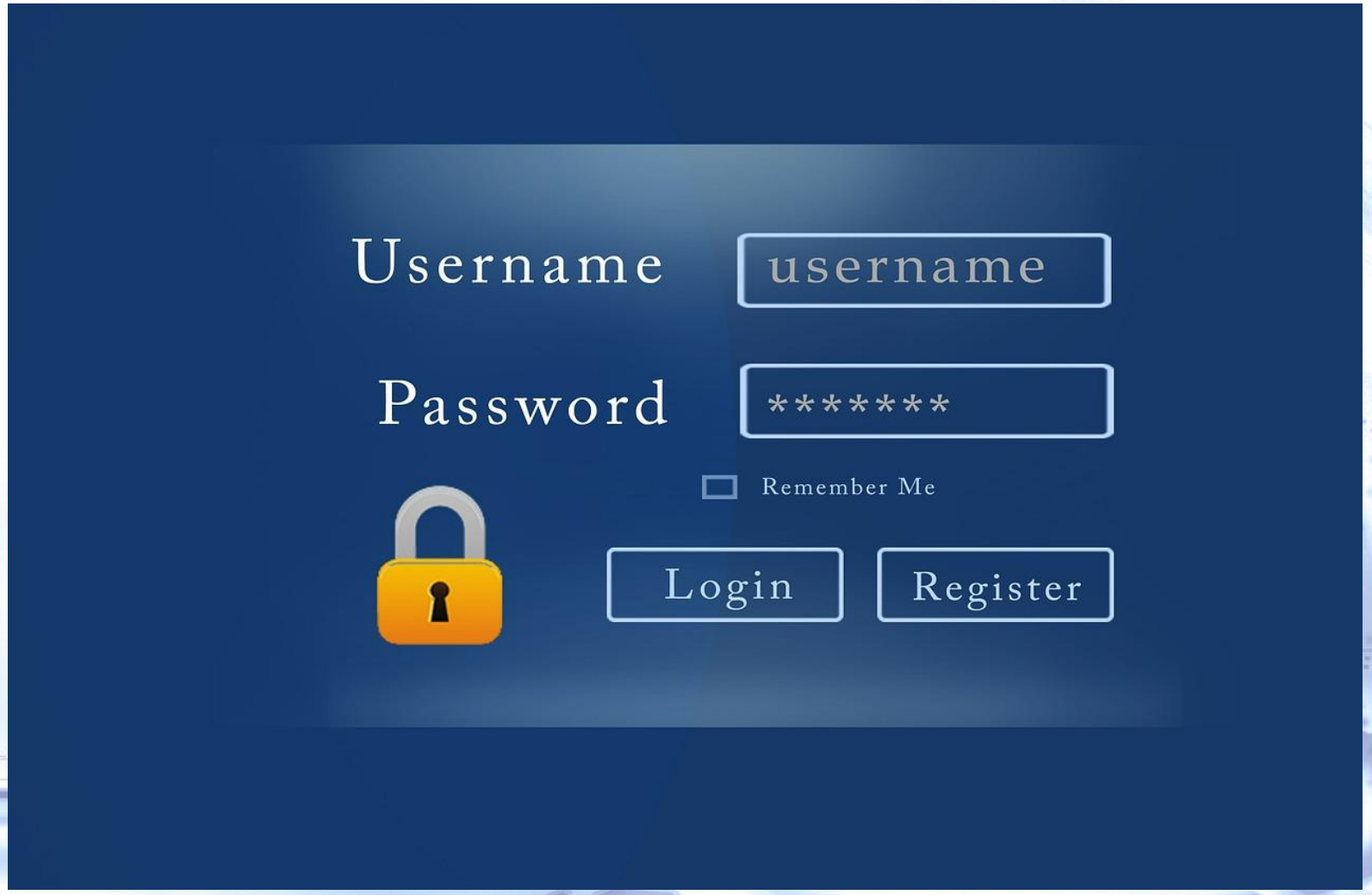


Цель работы: выяснить способы защиты личных данных в сети Интернет.

Материалы: интернет-ресурсы

Методы: поиск, обработка и систематизация полученной информации.

Защита с помощью паролей

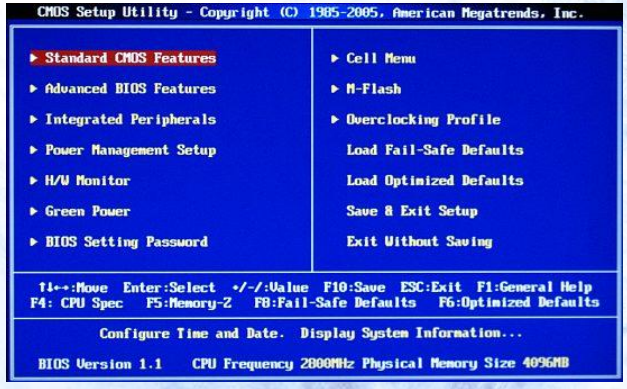


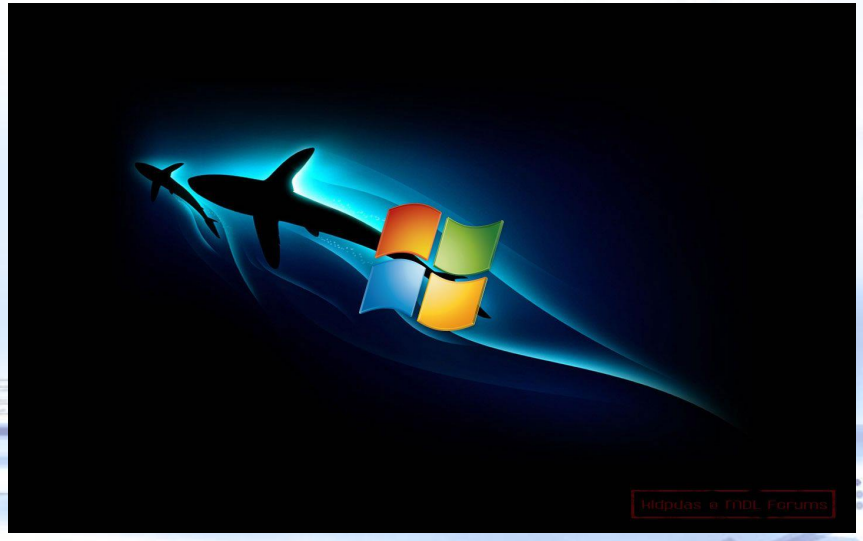
Для предотвращения несанкционированного доступа к данным, хранящимся на компьютере, используются пароли. Компьютер разрешает доступ к своим ресурсам только тем пользователям, которые зарегистрированы и ввели правильный пароль.

Пароль – это секретный набор символов, который защищает вашу учетную запись.

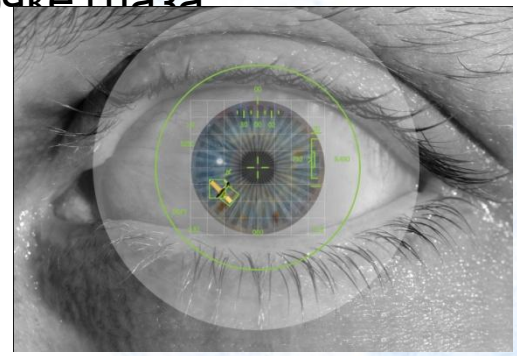
Защита пользовательских настроек имеется в операционной системе Windows, однако такая защита легко преодолима, так как пользователь может отказаться от введения пароля.

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, но возникнут серьезные проблемы доступа к данным, если пользователь забудет этот пароль.





Также в настоящее время для защиты от несанкционированного доступа к информации все более часто используются биометрические системы авторизации и идентификации пользователей. К биометрическим системам защиты информации относятся системы распознавания речи, системы идентификации по отпечаткам пальцев, а также системы идентификации по радужной оболочке глаза.



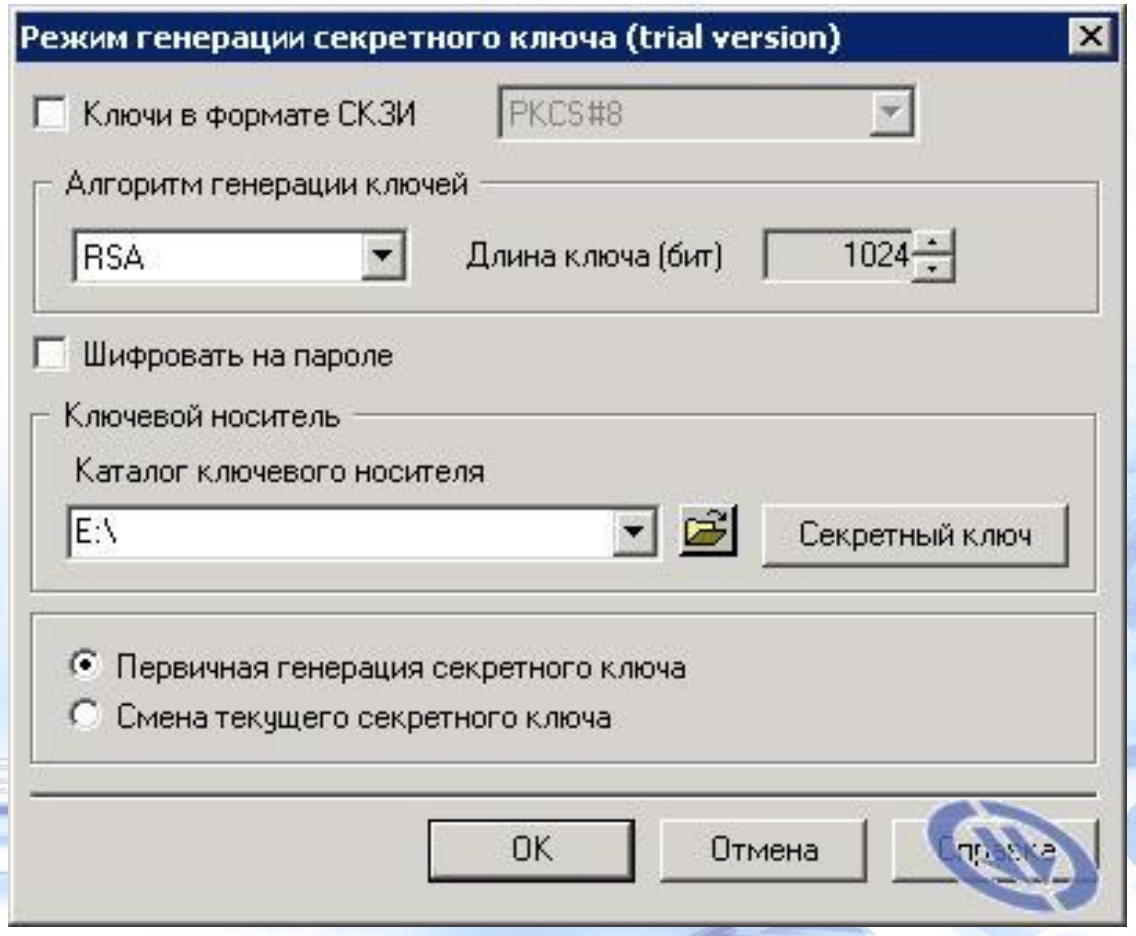
Защита от пиратских копирований

Компьютерные пираты, нелегально тиражируя программное обеспечение, обесценивают труд программистов, делают разработку программ экономически невыгодным бизнесом. Кроме того, компьютерные пираты нередко предлагают пользователям недоработанные программы, программы с ошибками или их демоверсии.

Для того чтобы программное обеспечение компьютера могло функционировать, оно должно быть установлено (инсталлировано). Программное обеспечение распространяется фирмами-производителями в форме дистрибутивов на CD-ROM. Каждый дистрибутив имеет свой серийный номер, что препятствует незаконному копированию и установке программ.

Дистрибутив – это файл или файлы, предназначенные для установки какой-либо программы. Обычно дистрибутив представляет собой один файл, имеющий расширение *.exe* или *.msi*.

Для предотвращения нелегального копирования программ и данных, хранящихся на CD-ROM, может использоваться специальная защита. На CD-ROM может быть размещен закодированный программный ключ, который теряется при копировании и без которого программа не может быть установлена.

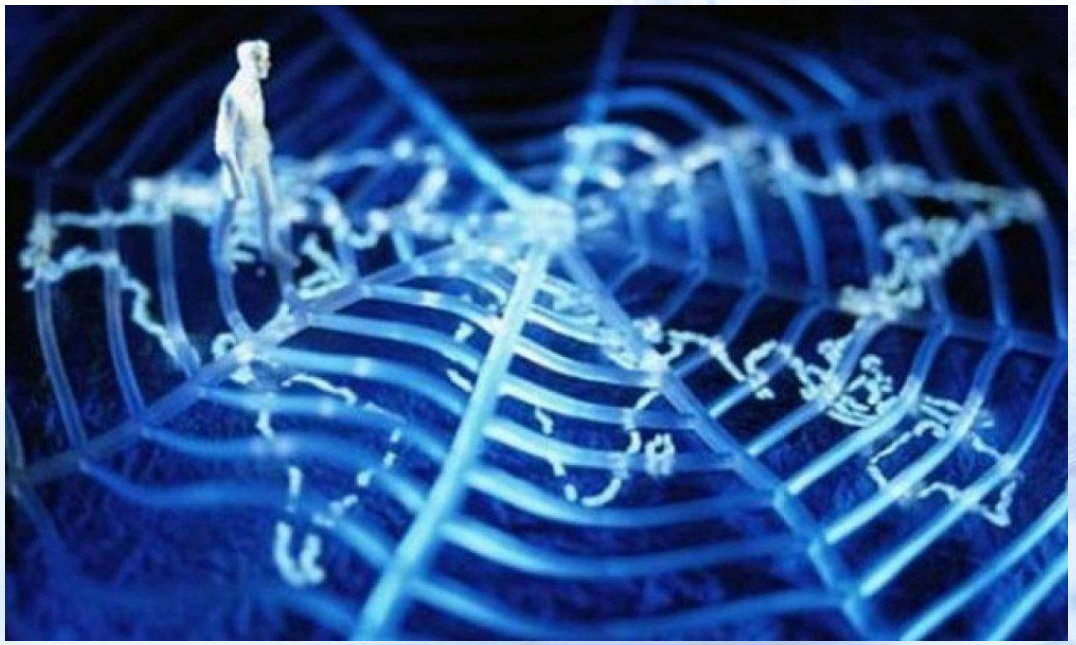


Защита от нелегального использования программ может быть реализована с помощью аппаратного ключа, который присоединяется обычно к параллельному порту компьютера. Защищаемая программа обращается к параллельному порту и запрашивает секретный код; если аппаратный ключ к компьютеру не присоединен, то защищаемая программа определяет ситуацию нарушения защиты и прекращает свое выполнение.

Для обеспечения большей надежности хранения данных на жестких дисках используются RAID-массивы (Redantant Arrays of Independent Disks). Несколько жестких дисков подключаются к специальному 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.

Защита информации в интернете

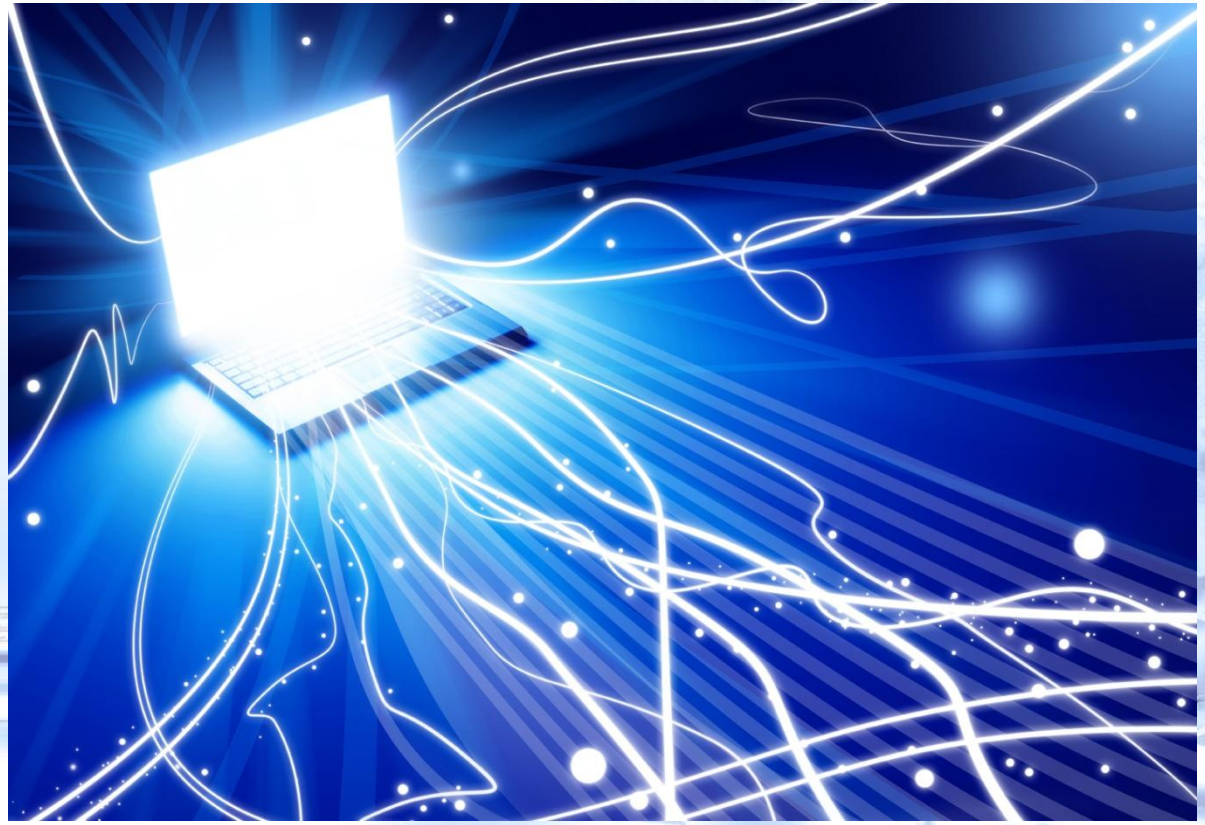
Если компьютер подключен к Интернету, то в принципе любой пользователь, также подключенный к Интернету, может получить доступ к информационным ресурсам этого компьютера. Если сервер имеет соединение с Интернетом и одновременно служит сервером локальной сети (Интранет-сервером), то возможно несанкционированное проникновение из Интернета в локальную сеть.



Механизмы проникновения из Интернета на локальный компьютер и в локальную сеть могут быть разными:

- загружаемые в браузер Web-страницы могут содержать активные элементы ActiveX или Java-апплеты , способные выполнять деструктивные действия на локальном компьютере;

- некоторые Web-серверы размещают на локальном компьютере текстовые файлы cookie, используя которые можно получить конфиденциальную информацию о пользователе локального компьютера;
- с помощью специальных утилит можно получить доступ к дискам и файлам локального компьютера.



Для того чтобы этого не происходило, устанавливается программный или аппаратный барьер с помощью брандмауэра (firewall — межсетевой экран). Брандмауэр отслеживает передачу данных между сетями, осуществляет контроль текущих соединений, выявляет подозрительные действия и тем самым предотвращает несанкционированный доступ из Интернета в локальную сеть.

Вывод:

Как вы видите защитить свою личною информацию от несанкционированного доступа можно разными действенными способами , в этом нет ничего сложного, поэтому есть смысл этими способами воспользоваться, предохранив себя от разных неприятностей в интернете.

Спасибо за внимание!