Информационная безопасность

Информационная безопасность

Информационная безопасность – совокупность мер по защите информационной среды общества и человека.

Информационная среда – это совокупность условий, средств и методов на базе компьютерных систем, предназначенных для создания и использования информационных ресурсов.

Совокупность факторов, представляющих опасность для функционирования информационной среды, называют информационными угрозами.

Основные цели и задачи информационной безопасности

- **Защита национальных интересов;**
- **Обеспечение человека и общества достоверной и полной информацией;**
- **Правовая защита человека и общества при получении, распространении и использовании информации.**

К объектам, которым следует обеспечить информационную безопасность, относятся:

- **Информационные ресурсы;**
- **Система создания, распространения и использования информационных ресурсов;**
- **Информационная инфраструктура структура общества информационные коммуникации, сети связи, центры анализа и обработки данных, системы и средства защиты информации);**
- **Средства массовой информации;**
- **Права человека и государства на получение, распространение и использование информации;**
- **Защита интеллектуальной собственности и конфиденциальной информации.**

Информационные угрозы

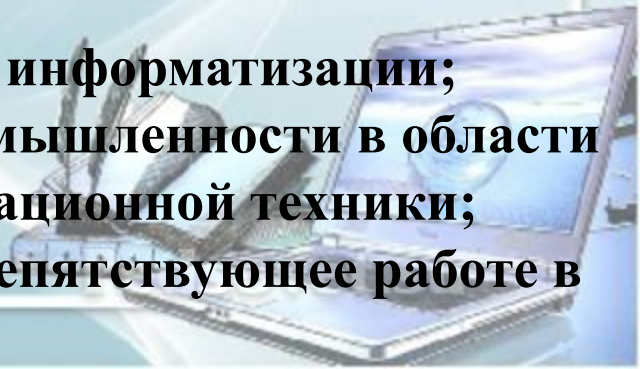
Источники информационных угроз

Внешние угрозы:

- **Политика стран, противодействующая доступу к мировым достижениям в области информационных технологий;**
- **«Информационная война», нарушающая функционирование информационной среды в стране;**
- **Преступная деятельность, направленная против национальных интересов**

Внутренние угрозы:

- **Отставание от ведущих стран мира по уровню информатизации;**
- **Технологическое отставание электронной промышленности в области производства информационной телекоммуникационной техники;**
- **Снижение уровня образованности граждан, препятствующее работе в информационной среде**



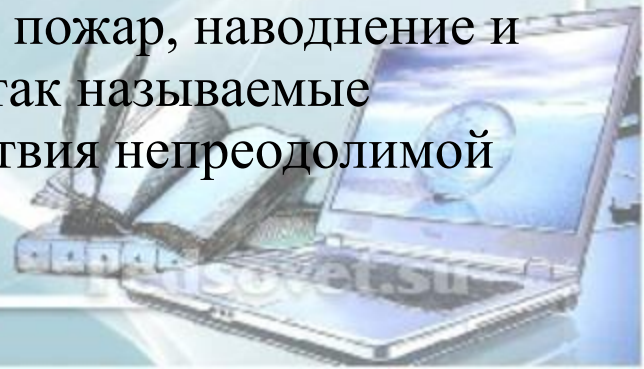
Виды информационных угроз

Преднамеренные:

- Хищение информации: несанкционированный доступ к документам и файлам (просмотр и копирование данных;
- Распространение компьютерных вирусов;
- Физическое воздействие на аппаратуру: внесение изменений в аппаратуру, подключение к каналам связи, порча или уничтожение носителей, преднамеренное воздействие магнитным полем.

Случайные:

- Ошибки пользователя компьютера;
- Ошибки профессиональных разработчиков информационных систем: алгоритмические, программные, структурные;
- Отказы и сбои аппаратуры, в том числе помехи и искажения сигналов на линиях связи;
- Форс-мажорные обстоятельства (авария, пожар, наводнение и другие так называемые воздействия непреодолимой силы).



Информационная безопасность для различных пользователей компьютерных систем

Наиболее уязвимые виды деятельности:

- Банковская деятельность
- Коммерческая деятельность
- Информационные услуги
- Управленческие задачи
- Прикладные задачи

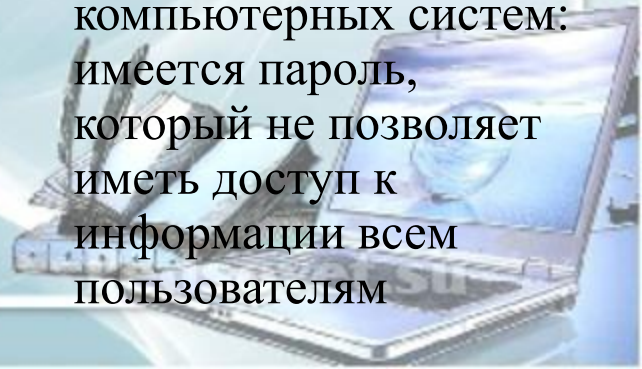
Методы защиты информации

Факторы и условия разработки методов защиты информации:

- Расширение областей использования компьютеров и увеличение темпа роста компьютерного парка (то есть проблема защиты информации должна решаться на уровне технических средств);
- Высокая степень концентрации информации в центрах ее обработки и, как следствие, появление централизованных баз данных, предназначенных для коллективного использования ;
- Расширение доступа пользователя к мировым информационным ресурсам (современные системы обработки данных могут обслуживать неограниченное число абонентов, удаленных на сотни и тысячи километров);
- Усложнение программного обеспечения вычислительного процесса на компьютере.

Ограничение доступа к информации осуществляется на двух уровнях:

- На уровне среды обитания человека: выдача допущенным лицам специальных пропусков, установки охранной сигнализации и системы видеонаблюдения;
- На уровне защиты компьютерных систем: имеется пароль, который не позволяет иметь доступ к информации всем пользователям



Контроль доступа к аппаратуре означает, что вся аппаратура закрыта и в местах доступа к ней установлены датчики, которые срабатывают при вскрытии аппаратуры.

Законодательные меры заключаются в исполнении существующих в стране законов, постановлений, инструкций, регулирующих юридическую ответственность должностных лиц – пользователей и обслуживающего персонала за утечку, потерю или модификацию доверенной им информации.

Защита от хищения информации

Защита от хищения информации осуществляется с помощью специальных программных средств. Для **защиты от компьютерных вирусов** применяются программы-анализаторы, предусматривающие разграничение доступа, самоконтроль и самовосстановление. Антивирусные средства самые распространенные средства защиты информации.

В качестве **физической защиты компьютерных систем** используется специальная аппаратура, позволяющая выявить устройства промышленного шпионажа, исключить запись или ретрансляцию излучений компьютера, а также речевых и других сигналов.