ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Над презентацией работала
Васильева Дарья
Студентка 105 А группы

- **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.**

- **Противоправные воздействия на информационную среду могут наносить ущерб интересам человека и общества, поэтому одной из задач информатизации является обеспечение информационной безопасности. Должна быть обеспечена защита информационной среды от информационных угроз, то есть не только защита информации, но и информационная безопасность самого человека и всего общества.**

ОСНОВНЫЕ ЦЕЛИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЩЕСТВА

- **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 общества (информационные коммуникации, сети связи, центры анализа и обработки данных, системы и средства защиты информации);**
- **средства массовой информации;**
- **права человека и государства на получение, распр и использование информации;**
- **защита интеллектуальной собственности и конфиденциальной информации.**

ИНФОРМАЦИОННЫЕ УГРОЗЫ

К источникам основных внешних угроз для России относятся:

- **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.**

К источникам основных внутренних угроз для России относятся:

- **отставание от ведущих стран мира по уровню информатизации;**
- **технологическое отставание электронной промышленности в области производства информационной и телекоммуникационной техники;**
- **снижение уровня образованности граждан, препятствующее работе в информационной среде.**

ИНФОРМАЦИОННЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ МОЖНО РАЗДЕЛИТЬ НА ПРЕДНАМЕРЕННЫЕ (НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП) И СЛУЧАЙНЫЕ

- **Преднамеренные угрозы часто называют несанкционированным доступом, атакой, нападением. Эти угрозы связаны с действиями человека, причинами которых могут быть: самоутверждение своих способностей (хакеры), недовольство своей жизненной ситуацией, материальный интерес, развлечение и т. п.**

Преднамеренные угрозы в компьютерных системах могут осуществляться через каналы доступа к информации:

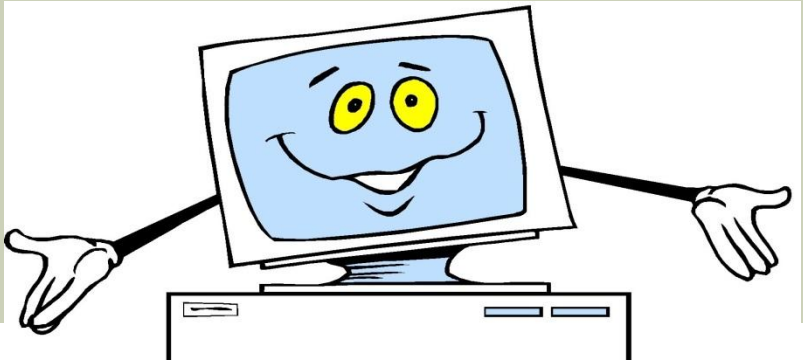
- **компьютерное рабочее место служащего;**
- **компьютерное рабочее место администратора компьютерной системы;**
- **внешние носители информации (диски, ленты, бумажные носители);**
- **внешние каналы связи.**

НАИБОЛЕЕ СЕРЬЕЗНАЯ УГРОЗА ИСХОДИТ ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ.

- **Ущерб от компьютерных вирусов может быть разнообразным, начиная от посторонних надписей, возникающих на экране монитора, и заканчивая хищением и удалением информации, находящейся на зараженном компьютере.**
- **Среди вредоносных программ особое место занимают «троянские кони», которые могут быть незаметно для владельца установлены и запущены на его компьютере. Различные варианты «троянских коней» делают возможным просмотр содержимого экрана, перехват вводимых с клавиатуры команд, кражу и изменение паролей и файлов и т. п.**

СЕТЕВЫЕ АТАКИ

- **В последнее время среди распространенных компьютерных угроз стали фигурировать сетевые атаки. Атаки злоумышленников имеют целью выведение из строя определенных узлов компьютерной сети. Эти атаки получили название «отказ в обслуживании» («denial of service»). Выведение из строя некоторых узлов сети даже на ограниченное время может привести к очень серьезным последствиям. Например, отказ в обслуживании сервера платежной системы банка приведет к невозможности осуществления платежей и, как следствие, к большим прямым и косвенным финансовым потерям.**



СЛУЧАЙНЫЕ УГРОЗЫ

- **Случайные угрозы проявляются в том, что информация в процессе ввода, хранения, обработки, вывода и передачи подвергается различным воздействиям. Случайные факторы, определяющие подобные воздействия, связаны как с непредвиденными ситуациями (форс-мажорные обстоятельства), так и с человеческим фактором (ошибками, халатностью, небрежностью при работе с информацией). Так, например, в компьютерных системах причинами случайных воздействий могут быть:**

- **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).**

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

- **Политика безопасности — это совокупность технических, программных и организационных мер, направленных на защиту информации в компьютерной сети.**
- **Защита от хищения информации обычно осуществляется с помощью специальных программных средств. Несанкционированное копирование и распространение программ и ценной компьютерной информации является кражей интеллектуальной собственности. Защищаемые программы подвергаются предварительной обработке, приводящей исполняемый код программы в состояние, препятствующее его выполнению на «чужих» компьютерах (шифрование файлов, вставка парольной защиты, проверка компьютера по его уникальным характеристикам и т. п.). Другой пример защиты: для предотвращения несанкционированного доступа к информации в локальной сети вводят систему разграничения доступа как на аппаратном, так и на программном уровнях. В качестве аппаратного средства разграничения доступа может использоваться электронный ключ, подключаемый, например, в разъем принтера.**

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

- **Для защиты от компьютерных вирусов применяются «иммуностойкие» программные средства (программы-анализаторы), предусматривающие разграничение доступа, самоконтроль и самовосстановление. Антивирусные средства являются самыми распространенными средствами 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 несущих информацию сигналов. Это позволяет предотвратить утечку информативных электромагнитных сигналов за пределы охраняемой территории. Наиболее эффективным средством защиты информации в каналах связи является применение специальных протоколов и криптографии (шифрования).**

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

- **Для защиты информации от случайных информационных угроз например, в компьютерных системах, применяются средства повышения надежности аппаратуры:**

- **повышение надежности работы электронных и механических узлов и элементов;**
- **структурная избыточность — дублирование или утроение элементов, устройств, подсистем;**
- **функциональный контроль с диагностикой отказов, то есть обнаружение сбоев, неисправностей и программных ошибок и исключение их влияния на процесс обработки информации, а также указание места отказавшего элемента.**