Этические и правовые аспекты информационной деятельности. Правовая охрана программ и данных. Защита информации. Компьютерные вирусы.

Этические и правовые аспекты информационной деятельности.

Существуют определенные проблемы развития информационной сферы регионов: проблемы индустриализации получения и обработки информации, психологические, правовые, экономические и социальные.

Этические и правовые аспекты информационной деятельности.

К психологическим проблемам следует отнести в первую очередь проблему готовности населения к переходу в информационное общество.
Этот переход в настоящее время затрудняется недостаточным уровнем информационной культуры населения, недостаточной компьютерной неграмотностью, а отсюда низкими информационными потребностями, а также отсутствием желания их развивать.
Необходимо отметить, что информатизация общества предполагает организацию компьютерного ликбеза населения, подготовку и переподготовку кадров – специалистов по ЭВМ и неспециалистов, формирование особенно у молодежи, новой информационной культуры, расширение математического образования, преодоление барьеров на пути к ПЭВМ, машинным языкам и т. д.

Этические и правовые аспекты информационной деятельности.

Правовые проблемы возникают в связи с превращением информации в основные ресурсы развития общества. Возникают новые виды правонарушений, которые свойственные лишь информационной сфере. Социальные проблемы связаны с коренным изменением образа жизни общества под воздействием информатизации. К этим проблемам также можно отнести коммуникационные проблемы и проблемы гуманизации развития инфосферы.

Правовая охрана программ и данных

Правовая охрана программ и баз данных. Охрана интеллектуальных прав, а также прав собственности распространяется на все виды программ для компьютера, которые могут быть выражены на любом языке и в любой форме, включая исходный текст на языке программирования и машинный код. Однако правовая охрана не распространяется на идеи и принципы, лежащие в основе программы, в том числе на идеи и принципы организации интерфейса и алгоритма.

Правовая охрана программ для ЭВМ и баз данных впервые в полном объеме введена в Российской Федерации Законом "О правовой охране программ для электронных вычислительных машин и баз данных", который вступил в силу в 1992 году.

Правовая охрана программ и данных

Автору программы принадлежит исключительное право осуществлять воспроизведение и распространение программы любыми способами, а также модифицировать программу. Организация или пользователь, правомерно владеющие экземпляром программы (купившие лицензию на ее использование), могут осуществлять любые действия, связанные с функционированием программы, в том числе ее запись и хранение в памяти компьютера.

Необходимо знать и выполнять существующие законы, запрещающие нелегальное копирование и использование лицензионного программного обеспечения. В отношении организаций или пользователей, которые нарушают авторские права, разработчик может потребовать через суд возмещения причиненных убытков и выплаты нарушителем компенсации.

Правовая охрана программ и данных

Для признания авторского права на программу для компьютера не требуется ее регистрации в какой-либо организации.

Авторское право на программу возникает автоматически при ее создании. Для оповещения о своих правах разработчик программы может, начиная с первого выпуска в свет программы, использовать знак охраны авторского права, состоящий из трех элементов:
- буквы "С" в окружности © или круглых скобках (с);
- наименования (имени) правообладателя;
- года первого выпуска программы в свет.

Например, знак охраны авторских прав на текстовый редактор Word выглядит следующим образом: © Корпорация Microsoft, 1983-2003.

Правовая охрана программ и данных

Электронная подпись. Электронная цифровая подпись в электронном документе признается юридически равнозначной подписи в документе на бумажном носителе.

В 2002 году был принят Закон "Об электронно-цифровой подписи", который стал законодательной основой электронного документооборота в России.

При регистрации электронно-цифровой подписи в специализированных центрах корреспондент получает два ключа: **секретный** и **открытый**.

Защита информации

Защита от несанкционированного доступа к информации. Для защиты от несанкционированного доступа к данным, хранящимся на компьютере, используются пароли. Компьютер разрешает доступ к свсим ресурсам только тем пользователям, которые зарегистрированы и ввели правильный пароль. Каждому конкретному пользователю может быть разрешен доступ только к определенным информационным ресурсам. При этом может производиться регистрация всех попыток несанкционированного доступа.

Защита с использованием пароля используется при загрузке операционной системы (при загрузке системы пользователь должен ввести свой пароль). 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 был введен правильный пароль. Преодолеть такую защиту нелегко, более того, возникнут серьезные проблемы доступа к данным, если пользователь забудет этот пароль.

Защита информации

Защита программ от нелегального копирования и использования. 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 демоверсии программ.

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.

Защита информации

Физическая защита данных на дисках. Для обеспечения большей надежности хранения данных на жестких дисках используются RAID-массивы (Reduntant Arrays of Independent Disks - избыточный массив независимых дисков). Несколько жестких дисков подключаются к 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 злоумышленник, также подключенный к Интернету, может получить доступ к информационным ресурсам этого компьютера. Если сервер, имеющий соединение с Интернетом, одновременно является сервером локальной сети, то возможно несанкционированное проникновение из Интернета в локальную сеть.

Защита информации

Для доступа к данным на компьютере, подключенном к Интернету, часто используется особо опасная разновидность компьютерных вирусов - **троянцы**. Троянцы распространяются по компьютерным сетям и встраиваются в операционную систему компьютера. В течение долгого времени они могут незаметно для пользователя пересылать важные данные (пароли доступа к Интернету, номера банковских карточек и т. д.) злоумышленнику.

Такие компьютерные вирусы были названы троянцами по аналогии с троянским конем. В поэме Гомера описана осада древними греками города Трои (около 1250 года до н. э.). Греки построили громадного коня, поместили в нем воинов и оставили его у ворот города. Ничего не подозревающие троянцы втащили коня в город, а ночью греки вышли из коня и захватили город.

Для защиты от троянцев и других компьютерных вирусов используются антивирусные программы.

Защита информации

Большую опасность для серверов Интернета представляют **хакерские атаки**. Во время таких атак на определенный сервер Интернета посылаются многочисленные запросы со многих Интернет-адресов, что может привести к "зависанию" сервера.

Для защиты компьютера, подключенного к Интернету, от сетевых вирусов и хакерских атак между Интернетом и компьютером устанавливается аппаратный или программный **межсетевой экран**. Межсетевой экран отслеживает передачу данных между Интернетом и локальным компьютером, выявляет подозрительные действия и предотвращает несанкционированный доступ к данным.

Компьютерные вирусы

Компьютерный вирус — Это специально написанная программа или сборка алгоритмов которые пишутся с целью: пошутить, навредить чьему либо компьютеру, получение доступа к вашему компьютеру, для перехвата паролей или вымогания денег. Вирусы могут само-копироваться и заражать вредоносным кодом ваши программы и файлы, а так же загрузочные сектора.

Компьютерные вирусы

Виды вредоносных программ.
Разделить вредоносные программы можно на два основных вида.
Вирусы и черви.

Компьютерные вирусы

Вирусы - распространяются через вредоносный файл, который вы могли скачать в интернете, или может оказаться на пиратском диске, или часто передают их по скайпу под видом полезных программ (заметил что на последнее часто попадаются школьники, им передают якобы мод для игры или читы а на самом деле может оказаться вирусом который может навредить).
Черви заражают уже множество файлов вашем компьютере, например все exe файлы, системные файлы, загрузочные сектора и тд.
Черви чаще всего проникают в систему уже сами, используя уязвимости вашей ОС, вашего браузера, определенной программы. Они могут проникать через чаты, программы для общения такие как skype, icq , могут распространяться через электронную почту.

Компьютерные вирусы

Вирусы бывают :
— **Файловые** — находятся в зараженном файле, активируются когда пользователь включает эту программу, сами не могут активироваться.
— **Загрузочные** — могут загружаться при загрузке windows попав в автозагрузку, при вставке флешки или подобное.
- **Макро вирусы** - это различные скрипты которые могут находиться на сайте, могут прислать их вам по почте или в документах Word и Excel, выполняют определенные функции заложенные в компьютере. Используют уязвимости ваших программ.

Компьютерные вирусы

Типы вирусов.
-Троянские программы
— Шпионы
— Вымогатели
— Вандалы
— Руткиты
— Botnet
— Кейлогеры

Компьютерные вирусы

— **Троянские программы**. Название происходит от троянского коня. Проникает в ваш компьютер под видом безвредных программ, потом может открыть доступ к вашему компьютеру или переслать ваши пароли хозяину.
— **Шпионы (spyware)** отслеживают действия пользователя. Какие сайты посещает или что делает пользователь на своём компьютере.
— **Вымогатели**. К ним относятся Винлокеры (winlocker). Программа полностью, или полностью блокирует доступ к компьютеру и требует деньги за разблокировку, на пример положить на счет или тд.

Компьютерные вирусы

— **Вандалы** могут блокировать доступы к сайтам антивирусов и доступ к антивирусам и многим другим программам.
— **Руткиты** (rootkit) — вирусы гибриды. Могут содержать в себе различные вирусы. Могут получать доступ к вашему пк, и человек будет полностью иметь доступ к вашему компьютеру, причем могут слиться на уровень ядра вашей ОС. Пришли из мира Unix систем. Могут маскировать различные вирусы, собирать данные о компьютере и обо всех процессах компьютера.
— **Botnet** достаточно неприятная вещь. Ботнеты это огромные сети из зараженных компьютеров «зомби», которые могут использоваться для ддоса сайтов и прочих кибер атак, используя зараженные компьютеры.

Компьютерные вирусы

Основные пути заражения.
— Уязвимость операционной системы.
— Уязвимость в браузере
— Качество антивируса хромает
— Глупость пользователя
— Сменные носители.

Контрольные вопросы

1. Как можно зафиксировать свое авторское право на программу?
2. Какие способы идентификации личности используются при предоставлении доступа к информации?
3. Почему компьютерное пиратство наносит ущерб обществу?
4. Чем отличается копирование файлов от инсталляции программ? Для чего каждый дистрибутив имеет серийный номер?
5. Какие существуют программные и аппаратные способы защиты информации?
6. Что такое электронная подпись?
7. Суть физической защиты данных?
8. Что такое троян?
9. Как распространяется троян?
10. Что такое шпионы?