Информационные ресурсы общества. Основы информационной безопасности, этики и права.

1. Информационные ресурсы

Ресурс – это запас или источник некоторых средств. Традиционно различают следующие виды общественных ресурсов: материальные, энергетические, трудовые, финансовые.

Одним из важнейших видов ресурсов современного общества являются **информационные ресурсы**. Значимость информационных ресурсов постоянно растет; одним из свидетельств этого является то, что уже на нынешней фазе продвижения к информационному обществу информационные ресурсы становятся **товаром**, совокупная стоимость которого на рынке сопоставима со стоимостью традиционных ресурсов.

Между информационными и другими ресурсами существует одно важнейшее различие: **всякий ресурс после использования исчезает (сожженное топливо, израсходованные финансы), а информационный ресурс остается, им можно пользоваться многократно, он копируется без ограничения**. Более того, по мере использования информационный ресурс имеет тенденцию увеличиваться, так как использование информации чаще всего сопровождается созданием дополнительной информацией.

Любая попытка дать классификацию информационным ресурсам общества оказывается неполной. В основу классификации можно положить:

• отраслевой принцип (по виду науки, промышленности, социальной сферы, по тому, к чему относится информация);

• форму представления (по виду носителей, степени формализованности, наличию дополнительного описания и пр.).

Крупнейшей категорией информационных ресурсов являются национальные информационные ресурсы. Это понятие сформировалось не так давно, в начале 1980-х гг.

Национальные информационные ресурсы России:

- Библиотечные ресурсы (библиотечная сеть России насчитывает около 150 тыс. библиотек)
- Архивный фонд РФ (включает в себя около 460 млн. документов, ежегодно он пополняется на 1,6 млн. единиц)
- Государственная система научно-технической информации
- Информационные ресурсы Государственной системы статистики
- Государственная система правовой информации
- Информационные ресурсы органов государственной власти и местного самоуправления

- Информационные ресурсы отраслей материального производства
- Информация о природных ресурсах, явлениях и процессах
- Информационные ресурсы социальной сферы

2. Информационная безопасность

Информационная безопасность совокупность мер по защите информационной среды общества и человека, которые обеспечивают:

- конфиденциальность: доступ к информации только авторизованных пользователей;
- целостность: достоверность и полноту информации и методов ее обработки;
- доступность: доступ к информации.

Информационная безопасность предприятия - состояние защищенности информационных ресурсов и экономических интересов предприятия в информационной сфере.

Правовая охрана информации. Правовая охрана программ для ЭВМ и баз данных впервые в полном объеме введена в Российской Федерации Законом РФ «О правовой охране программ для электронных вычислительных машин и баз данных», который вступил в силу в 1992 году. Для признания и осуществления авторского права на программы для ЭВМ не требуется ее регистрация в какой-либо организации. Авторское право на программы для ЭВМ возникает автоматически при их 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 ©;
- наименования (имени) правообладателя;
- года первого выпуска программы в свет.

Например, знак охраны авторских прав на текстовый редактор Word выглядит следующим образом:

© Корпорация Microsoft, 1993-1997.

Автору программы принадлежит исключительное право осуществлять воспроизведение и распространение программы любыми способами, а также модификацию программы.

Юридический статус программ

Программы по их юридическому статусу можно разделить на три большие группы: **лицензионные**, **условно бесплатные** (shareware) и **свободно распространяемые программы** (freeware).

Дистрибутивы **лицензионных** программ (дискеты или диски CD-ROM, с которых производится установка программ на компьютеры пользователей) распространяются разработчиками на основании договоров с пользователями на платной основе, проще говоря, лицензионные программы продаются. Разработчики программы гарантируют ее нормальное функционирование в определенной операционной системе и несут за это ответственность.

Некоторые фирмы-разработчики программного обеспечения предлагают пользователям **условно бесплатные программы** в целях их рекламы и продвижения на рынок. Пользователю предоставляется версия программы с ограниченным сроком действия (после истечения указанного срока программа перестает работать, если за нее не произведена оплата) или версия программы с ограниченными функциональными возможностями (в случае оплаты пользователю сообщается код, включающий все функции).

Многие производители программного обеспечения и компьютерного оборудования заинтересованы в широком **бесплатном** распространении программного обеспечения. К таким программным средствам можно отнести:

- дополнения к ранее выпущенным программам, исправляющие найденные ошибки или расширяющие возможности;
- драйверы к новым устройствам или улучшенные драйверы к уже существующим.

Защита доступа к компьютеру.

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. Каждому конкретному пользователю может быть разрешен доступ только к определенным информационным ресурсам. При этом может производиться регистрация всех попыток несанкционированного доступа.

В настоящее время для защиты от несанкционированного доступа к информации все более часто используются биометрические системы авторизации и идентификации пользователей (системы распознавания речи, системы идентификации по отпечаткам пальцев, а также системы идентификации по радужной оболочке глаза).

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 их демоверсии.

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 данных на дисках

Каждый диск, папка и файл локального компьютера, а также компьютера, подключенного к локальной сети, может быть защищен от несанкционированного

доступа. Для них могут быть установлены определенные права доступа (полный, только чтение, по паролю), причем права могут быть различными для различных пользователей.

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.

Для того чтобы этого не происходило, устанавливается программный или аппаратный барьер между Интернетом и компьютером 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.

3. Этика и право

Этика пытается разделить совершаемые человеком действия на хорошие и плохие. Современное общество имеет свободный доступ к информации. Интернет стал частью нашей жизни, он помогает нам работать и учиться, получать вдохновение и делиться идеями, устраивать свою личную жизнь и строить карьеру.

Уже сейчас информационные технологии затрагивают фундаментальные права человека, касаясь защиты авторских прав, интеллектуальной свободы, ответственности и безопасности. Информационная этика рассматривает проблемы собственности, доступа, неприкосновенности частной жизни, безопасности и общности информации.

Интернет - это наше настоящее и будущее. И с каждым днем вопрос об этических нормах в Сети приобретает все большую актуальность. И если бы общение в Интернете не основывалось на этических нормах, то Интернет стал бы лишь инструментом для мошенников, преступников, душевнобольных.

Во многих организациях правила поведения пользователя в локальных сетях представляются в форме инструкций либо официальных правил:

* Не передавайте никому ваше имя и пароль для входа в сеть: любые деяния, совершенные в сети под вашим именованием, позже могут быть соотнесены конкретно с вами;
* Если вы оставляете компьютер более чем на 10 минут, перед уходом прекратите выполнение всех программ с сетевой поддержкой (либо связанных с обменом данных по сети).
* Старайтесь без необходимости не запускать несколько программ с сетевой поддержкой;
* Пользуясь общим (системным) почтовым ящиком, старайтесь не отправлять сообщения чрезмерно большого размера;

* Перед установкой на ваш компьютер нового программного обеспечения с сетевой поддержкой либо с вероятным коллективным внедрением проконсультируйтесь с сетевым администратором и проверьте устанавливаемое программное обеспечение на лицензионную чистоту и на не зараженность вирусами;

* Смотрите за тем, чтоб работающие у вас программы не наносили вред общим (сетевым) ресурсам и ресурсам остальных пользователей сети.

накладывает на членов локальной сети определенные дополнительные правила:

* При наличии коллективного принтера смотрите, чтоб не распечатывались лишние копии отправленного вами задания; Смотрите за тем, чтоб ваши распечатки не скапливались у принтера, забирайте их сразу после окончания печати.

Все большее количество детей получает возможность работать в сети Интернет. Но вместе с тем все острее встает проблема обеспечения безопасности наших детей в сети Интернет. Так как изначально Интернет развивался вне какого-либо контроля, то теперь он представляет собой огромное количество информации, причем далеко не всегда безопасной.

Существуют основные **правила интернет безопасности**:

* Никогда не давайте частной информации о себе (фамилию, номер телефона, адрес), без полной уверенности.

* Встреча в реальной жизни со знакомыми по Интернет общению не является очень хорошей идеей, поскольку люди могут быть разными в электронном общении и при реальной встрече.

* Не открывайте письма электронной почты, файлы или Web-страницы, полученные от людей, которых вы реально не знаете или не доверяете им.

* Всегда будьте вежливыми в электронной переписке, и ваши корреспонденты будут вежливыми с вами.

* В электронных письмах не применяйте текст, набранный в ВЕРХНЕМ РЕГИСТРЕ, это воспринимается в сети как крик, и может расстроить вашего собеседника.

* Не присылайте в письме информацию большого объема (картинки, фотографии и т.п.) без предварительной договоренности с вашим собеседником.

* Не рассылайте писем с какой-либо информацией незнакомым людям без их просьбы, это воспринимается как "спам", и обычно досаждает пользователям сети.

Такими образом, можно сделать вывод, что, выполняя элементарные правила поведения, можно быть в безопасности, огородить себя от вирусов и мошенников, а так же прослыть в глазах собеседника воспитанным человеком.

Десять компьютерных заповедей

1) Не используй компьютер во вред другим людям.

Заповедь называет аморальным как программный вред (создание вредоносных программ, уничтожение чужой информации иным способом и т.п.), так и использование компьютера в качестве оружия (например, для взрыва его хозяина), то есть для применения физического насилия.

2) Не вмешивайся в работу других пользователей на компьютере.

Неэтично запускать программы для слежения за работой пользователя (хотя в некоторых странах подобное слежение разрешено правоохранительным органам, но только при наличии у них на то разрешения) либо влияющие без его желания на информацию.

3) Не лезь в компьютерные файлы других.

Подобное поведение равносильно чтению чужих ежедневников или корреспонденции. Кроме файлов, заповедь отрицательно относится и к чтению чужой электронной почты.

4) Не укради посредством компьютера.

Эта заповедь, к счастью, уже нашла свое применение на практике благодаря Уголовному кодексу. И действительно, чем хищение с использованием чужих кредитных карточек в Интернете отличается от кражи из универсама? Только что суммы в Интернете побольше будут...

5) Не создавай посредством компьютера ложное свидетельство.

Интернет переполнен различной информацией, но надежность этой информации никто проверить не может. Поэтому, выкладывая в Сеть недостоверные факты или клеветнические сведения, вы направляете человека по ложному следу.

6) Не копируй и не пользуйся программным обеспечением, за которое не уплатил.

Создавая программный продукт, человек тратит много своих творческих сил, а иногда и денежных средств. И неужели, с удовольствием пользуясь чудесной программой, вы не вознаградите ее создателя? Нарушение этой заповеди то же самое, что не уплатить за хлеб в магазине или за прелестную прическу в парикмахерской.

7) Не используй ресурсы чужого компьютера без разрешения или надлежащей компенсации.

Хорошо, если вы просто сядете за чужой компьютер и поработаете, не сделав ничего плохого. Но очень неэтично, мягко говоря, вскрывать защищенные паролем базы данных и компьютеры, используя их ресурсы.

8) Не присваивай продукты чужой интеллектуальной деятельности.

На защите восьмой заповеди стоят законы об авторских правах. Они работают даже в Интернете. Надо только очень захотеть восстановить свое авторство.

9) Думай о социальных последствиях написанной тобой программы или разработанной системы.

Задумайтесь, что будет, если ребенок с не сформировавшейся еще психикой зайдет на сайт, переполненный насилием или порнографией. А если таких детей тысячи? Последствия для общества, в котором будут жить, повзрослев, эти дети, непредсказуемы.

10) Всегда используй компьютер сознательно и уважительно по отношению к ближним.

Живя в обществе, как ни странно, приходится сталкиваться с другими его членами. Нравятся они вам или нет, но вы вынуждены ехать в переполненном общественном транспорте или стоять в очереди. Этика учит нас уступать место старшим, обходиться с людьми вежливо. Такие ситуации возможны и при использовании компьютера, хотя зачастую вы и не замечаете тех самых "других". Пользуясь какой-либо свободой, надо помнить, что она ограничивается свободой других людей.