

## **Лицензионные, условно бесплатные и бесплатные программы.**

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. Довольно часто разработчики предоставляют существенные скидки при покупке лицензий на использование программы на большом количестве компьютеров или на использование программы в учебных заведениях. В соответствии с лицензионным соглашением 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 следующие:

- новые недоработанные (бета) версии программных продуктов (это позволяет провести их широкое тестирование);
- программные продукты, являющиеся частью принципиально новых технологий (это позволяет завоевать рынок);
- дополнения к ранее выпущенным программам, исправляющие найденные ошибки или расширяющие возможности;
- устаревшие версии программ;
- драйверы к новым устройствам или улучшенные драйверы к уже существующим.

## **Правовая охрана информации**

Правовая охрана программ и баз данных. 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.

Предоставляемая настоящим законом правовая охрана распространяется на все виды программ для ЭВМ (в том числе на операционные системы и программные комплексы), 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 для ЭВМ, в том числе на идеи и принципы организации интерфейса и алгоритма.

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.

Организация или пользователь, правомерно владеющий экземпляром программы (купивший лицензию на ее использование), вправе без получения дополнительного разрешения разработчика осуществлять любые действия, связанные с функционированием программы, в том числе ее запись и хранение в памяти ЭВМ. Запись и хранение в памяти ЭВМ допускаются в отношении одной ЭВМ или одного пользователя в сети, если другое не предусмотрено договором с разработчиком.

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 возмещения причиненных убытков и выплаты нарушителем компенсации в определяемой по усмотрению суда сумме от 5000-кратного до 50 000-кратного размера минимальной месячной оплаты труда.

### **Электронная подпись.**

В 2002 году был принят Закон РФ «Об электронно-цифровой подписи», который стал законодательной основой электронного документооборота в России. По этому закону электронная цифровая подпись в электронном документе признается юридически равнозначной подписи в документе на бумажном носителе.

При регистрации электронно-цифровой подписи в специализированных центрах корреспондент получает два ключа: секретный и открытый. Секретный ключ хранится на дискете или смарт-карте и должен быть известен только самому корреспонденту. Открытый ключ должен быть у всех потенциальных получателей документов и обычно рассылается по электронной почте.

Процесс электронного подписания документа состоит в обработке с помощью секретного ключа текста сообщения. Далее зашифрованное сообщение посылается по электронной почте абоненту. Для проверки подлинности сообщения и электронной подписи абонент использует открытый ключ.

### **Защита информации.**

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.

Защита пользовательских настроек имеется в операционной системе Windows (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 введен правильный пароль. Преодолеть такую защиту нелегко, более того, возникнут серьезные проблемы доступа к данным, если пользователь забудет этот пароль.

В настоящее время для защиты от несанкционированного доступа к информации все более часто используются биометрические системы авторизации и идентификации пользователей. Используемые в этих системах характеристики являются неотъемлемыми качествами личности человека и поэтому не могут быть утерянными и подделанными. К биометрическим системам защиты информации относятся 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 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.

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.

### **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.

Для обеспечения большей надежности хранения данных на жестких дисках используются RAID-массивы (Redundant Arrays of Independent Disks — избыточный массив независимых дисков). 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 (Инtranет-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 и др.

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

### **Вопросы:**

- В чем состоит различие между лицензионными, условно-бесплатными и бесплатными программами?
- Как можно зафиксировать свое авторское право на программный продукт? Какие используются способы идентификации личности при предоставлении доступа к информации?
- Почему компьютерное пиратство наносит ущерб обществу?
- Какие существуют программные и аппаратные способы защиты информации?
- Чем отличается простое копирование файлов от инсталляции программ?