Правовая охрана информации

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.

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.

Лицензионные, условно бесплатные и свободно распространяемые программы

Лицензионные программы.
В соответствии с лицензионным соглашением разработчики программы гарантируют ее нормальное функционирование в определенной операционной системе и несут за это ответственность.
Лицензионные программы разработчики продают пользователям обычно в форме коробочных дистрибутивов.
В коробке находятся CD-диски, с которых производится установка программы на компьютеры пользователей, и руководство пользователя по работе с программой

Условно бесплатные программы.

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 была произведена оплата) или версия программы с ограниченными функциональными возможностями (в случае оплаты пользователю сообщается код, включающий все функции).

Свободно распространяемые программы.

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

- 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;
- драйверы к новым или улучшенные драйверы к уже существующим устройствам.

Защита информации

Защита от несанкционированного доступа к информации.

Для защиты от 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.

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.

От несанкционированного доступа может быть защищен каждый диск, папка и файл локального компьютера. Для них могут быть установлены определенные права доступа (полный, только чтение, по паролю), причем права могут быть различными для различных пользователей.

В настоящее время для защиты от несанкционированного доступа к информации все чаще используются ***биометрические системы идентификации***. 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 идентификации ***по отпечаткам пальцев***, системы ***распознавания речи***, 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 ***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.

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.

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.

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.

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.