ПРАВОВАЯ ОХРАНА ПРОГРАММ И ДАННЫХ. ЗАЩИТА ИНФОРМАЦИИ

Виды программ.
Правовая охрана информации.
Защита информации.

Виды программ

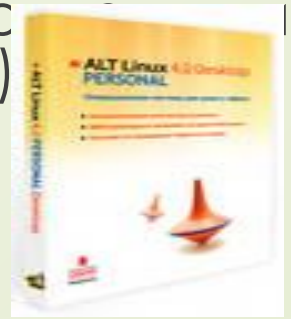
Программы по их юридическому статусу можно разделить на три большие группы

- Лицензионные
- Условно бесплатные или Shareware
- Свободно распространяемые программы или Freeware

Лицензионные программы

В данной области, лицензией называется **лицензионный договор,** то есть, договор между правообладателем и пользователем, по которому правообладатель передаёт пользователю ограниченные права на использование того или иного объекта интеллектуальной собственности. **В этом договоре указываются разрешённые виды использования, сроки передачи прав и иные условия**. При передаче прав на использование программ для ЭВМ возможен особый порядок заключения лицензионного договора — так называемая «обёрточная лицензия». При этом все существенные условия договора излагаются правообладателем так, чтобы они были доступны до приобретения товара (на упаковке, на обёртке), а пользователь эти условия принимает. (Согласие выражается фактом с[illegible]ли [illegible] использования прод[illegible]кта.)

Коробочные дистрибутивы ОС ALTLinux, GNULinux, Windows 7



Условно бесплатные

Shareware —в русском языке этот термин интерпретируется как «условно-бесплатное программное обеспечение». Основной принцип Shareware — «попробуй, прежде чем купить» (try before you buy). Программа, распространяемая как shareware, предоставляется пользователям бесплатно — **пользователь платит только за время загрузки файлов по Интернету или за носитель (дискету или CD-ROM)**. В течение определённого срока, составляющего обычно тридцать дней, он может пользоваться программой, тестировать её, осваивать её возможности. Если по истечении этого срока пользователь решит продолжить использование программы, он обязан купить программу (зарегистрироваться), заплатив автору определённую сумму. В противном случае пользователь должен прекратить ание программы ком

Диск бесплатных программ

Свободно распространяемые

Свободное программное обеспечение — программное обеспечение с открытым кодом, которое пользователь может легально запускать, модифицировать и распространять с небольшими ограничениями или вовсе без таковых. По законодательству практически всех стран, программный продукт и его исходный код по умолчанию является так называемой интеллектуальной собственностью его автора, которому даётся полная власть над распространением и изменением программы, даже в случае, когда исходные коды открыты для обозрения.

К таким программным средствам относятся:

-программы, поставляемые в учебные заведения в соответствии с государственными проектами;

-новые недоработанные (бета) версии программных продуктов;

-дополнения к ранее выпущенным програм исправляющие найденные ошибки или расшир возможности;

-драйвера к новым или улучшенные драйверы к существующим устройствам.

Правовая охрана информации

В соответствии с **ст. 1261 IVч. Гражданского кодекса**, авторские права 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 и объектный код, охраняются так же, как авторские права на произведения литературы. **Программой для ЭВМ** является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки **программы для ЭВМ**, и порождаемые ею аудиовизуальные отображения.

Правовая охрана информации

Для оповещения о своих правах разработчик программы использует знак охраны авторского права.

Знак охраны авторского права состоит из трёх элементов:

-буквы С в окружности © или круглых скобках (с);

наименования (имени) правообладателя;

-года первого выпуска программы в свет.

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. Секретный ключ хранится на дискете или смарт-карте и известен только корреспонденту. Открытый ключ должен быть у всех потенциальных получателей документов и обычно рассылается по электронной почте.

Защита информации

Защита от несанкционированного копирования

— система мер, направленных на противодействие несанкционированному копированию информации, как правило представленной в электронном виде (данных или программного обеспечения).

При защите от копирования используются различные меры: организационные, юридические, программные и программно-аппаратные.

Для защиты данных, хранящихся на компьютере, используются пароли.

Компьютер разрешает доступ к своим ресурсам только тем пользователям, которые зарегистрированы и ввели правильный пароль.

Защита информации

Организационные меры защиты от несанкционированного копирования

Основная идея организационных мер защиты заключается в том, что полноценное использование программного продукта невозможно без соответствующей поддержки со стороны производителя: **подробной пользовательской документации, «горячей линии», системы обучения пользователей, обновление версий со скидкой** и т. п. Организационные меры защиты применяются, как правило, крупными разработчиками к достаточно большим и сложным программным продуктам.

Защита информации

Организационные меры защиты от несанкционированного копирования

Для защиты доступа к информации всё чаще используют **биометрические системы идентификации**: идентификация по отпечаткам пальцев, системы распознавания речи, системы идентификации по радужной оболочке глаза, по изображен[illegible]ло
ометрии ладони руки.

Защита информации

Юридические меры защиты от несанкционированного копирования

Предусматривают ответственность, в соответствии с действующим законодательством, за использование контрафактных экзем ля ЭВМ или баз данных.

Защита информации

Физическая защита данных

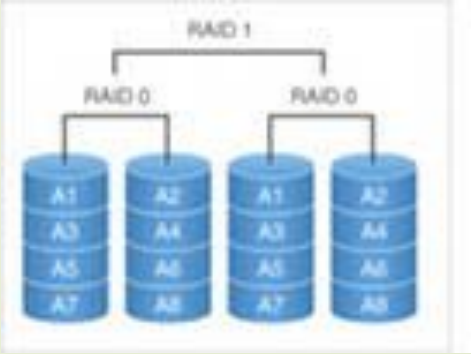
Для обеспечения большей надёжности хранения данных на жёстких дисках используют **RAID-массивы (избыточный массив независимых дисков)**.

Несколько жёстких дисков подключаются к RAID-контроллёру, 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.

Существует несколько разновидностей RAID-массивов:

RAID 0

RAID 1



Защита информации

Защита в Интернете

Для защиты информационных ресурсов компьютера, подключённого к Интернету используют антивирусные программы, например: Антивирус Касперского (Windows) и антивирус KlamAV(Linux).

Для защиты компьютеров, подключённых 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 несанкц