Вопрос 1

Правовая охрана информации (программ и данных).

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

В соответствии с федеральным законом "О правовой охране программ ЭВМ и баз данных" в решении проблемы защиты компьютерной информации выделя-ются следующие направления:

защита материальных объектов компьютерной собственности, выражен-ной в виде программных и аппаратных средств, а также связанного обо-рудования от кражи или утраты;

защита информационных и вычислительных ресурсов от несанкциониро ванного пользования;

защита конфиденциальной и ценной информации от несанкционирован ного доступа и модификации;

защита от утечки по каналам побочных электромагнитных излучений, специфических угроз, возникающих в системах связи;

защита интеллектуальной собственности, выраженной в виде алгоритмов и программ, электронных документов, а также ценных справочных баз данных;

защита информации от компьютерных вирусов и других опасных воздействий по каналам распространения программных средств.

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 организации интерфейса и алгоритма.

Для признания и осуществления авторского права на программы для ЭВМ не требуется её 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 трёх элементов:

Буквы "C" в окружности или круглых скобках (это выглядит так ©);

Наименования (имени) правообладателя;

Года первого выпуска программы в свет.

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 её использование), вправе без получения дополнительного разрешения разработчика осуществлять любые действия, связанные с функционированием программы, в том числе её 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 причинённых убытков и выплаты нарушителем компенсации в определяемой по усмотрению суда сумме от 5000-кратного до 50000-кратного размера минимальной месячной оплаты труда.

Так же одним из законов, касающихся защиты информации, является федеральный закон РФ "Об электронно-цифровой подписи",принятый в 2002 году, который стал законодательной основой электронного документооборота в Рос-сии. Целью является использования электронной цифровой подписи в элек-тронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной 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 смарткарте и должен быть известен только самому корреспонденту. Открытый ключ должен быть у всех потенциальных по-лучателей 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.