ПРАВОВАЯ ОХРАНА ПРОГРАММ И ДАННЫХ

ЗАЩИТА ИНФОРМАЦИИ

ПРАВОВАЯ ОХРАНА ПРОГРАММ И ДАННЫХ

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 20 октября 1992 г.

Предоставляемая настоящим законом правовая охрана распространяется на все виды программ для компьютеров (в том числе на операционные системы и программные комплексы), которые могут быть выражены на любом языке и в любой форме. Для признания и реализации авторского права на компьютерную программу не требуется ее регистрация в какой-либо организации. Авторское право на компьютерную программу возникает автоматически при ее 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.

Автору программы принадлежит исключительное право на воспроизведение и распространение программы любыми способами, а также на осуществление модификации программы.

Для обеспечения безопасности информационных систем применяют системы защиты информации, которые представляют собой комплекс организационно - технологических мер, программно - технических средств и правовых норм, направленных на противодействие источникам угроз безопасности информации.

При комплексном подходе методы противодействия угрозам интегрируются, создавая архитектуру безопасности систем. Необходимо отметить, что любая системы защиты информации не является полностью безопасной. Всегда приходиться выбирать между уровнем защиты и эффективностью работы информационных систем.

ИНФОРМАЦИИ ИС ОТ ДЕЙСТВИЙ СУБЪЕКТОВ ОТНОСЯТСЯ:

средства защита информации от несанкционированного доступа;

защита информации в компьютерных сетях;

криптографическая защита информации;

электронная цифровая подпись;

защита информации от компьютерных вирусов.

СРЕДСТВА ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Получение доступа к ресурсам информационной системы предусматривает выполнение трех процедур: идентификация, аутентификация и авторизация.

Идентификация **- присвоение пользователю (объекту или субъекту ресурсов) уникальных имен и кодов (идентификаторов).**

Аутентификация **- установление подлинности пользователя, представившего идентификатор или проверка того, что лицо или устройство, сообщившее идентификатор является действительно тем, за кого оно себя выдает. Наиболее распространенным способом аутентификации является присвоение пользователю пароля и хранение его в компьютере.**

Авторизация **- проверка полномочий или проверка права пользователя на доступ к конкретным ресурсам и выполнение определенных операций над ними. Авторизация проводится с целью разграничения прав доступа к сетевым и компьютерным ресурсам.**

ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Локальные сети предприятий очень часто подключаются к сети Интернет. Для защиты локальных сетей компаний, как правило, применяются межсетевые экраны - брандмауэры (firewalls)

Экран (firewall) **- это средство разграничения доступа, которое позволяет разделить сеть на две части (граница проходит между локальной сетью и сетью Интернет) и сформировать набор правил, определяющих условия прохождения пакетов из одной части в другую.**

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Для обеспечения секретности информации применяется ее шифрование или криптография. Для шифрования используется алгоритм или устройство, которое реализует определенный алгоритм. Управление шифрованием осуществляется с помощью изменяющегося кода ключа.

Извлечь зашифрованную информацию можно только с помощью ключа. Криптография - это очень эффективный метод, который повышает безопасность передачи данных в компьютерных сетях и при обмене информацией между удаленными компьютерами.

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

Сообщение, зашифрованное с помощью закрытого ключа, называется электронной цифровой подписью. Отправитель передает незашифрованное сообщение в исходном виде вместе с цифровой подписью. Получатель с помощью открытого ключа расшифровывает набор символов сообщения из цифровой подписи и сравнивает их с набором символов незашифрованного сообщения.

При полном совпадении символов можно утверждать, что полученное сообщение не модифицировано и принадлежит его автору.

ЗАЩИТА ИНФОРМАЦИИ ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ

Компьютерный вирус – это небольшая вредоносная программа, которая самостоятельно может создавать свои копии и внедрять их в программы (исполняемые файлы), документы, загрузочные сектора носителей данных и распространяться по каналам связи. Источниками вирусного заражения могут быть съемные носители и системы телекоммуникаций. К наиболее эффективным и популярным антивирусным программам относятся: Антивирус Касперского 7.0, AVAST, Norton AntiVirus и многие другие.