Правовое обеспечение ИС и защита информации.

Лекция

Информация с точки зрения информационной безопасности обладает следующими категориями:

- ***конфиденциальность*** - гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена; нарушение этой категории называется хищением либо раскрытием информации;
- ***целостность*** - гарантия того, что информация существует в ее исходном виде, т. е. при ее хранении или передаче не было произведено несанкционированных изменений; нарушение этой категории называется фальсификацией сообщения;
- ***аутентичность*** - гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор; нарушение этой категории называется фальсификацией автора сообщения;
- ***апеллируемость*** - категория, часто применяемая в электронной коммерции, - гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно заявленный человек, и не может являться никто другой; отличие этой категории от предыдущей в том, что при фальсификации автора кто-то другой пытается заявить, что он автор сообщения, а при нарушении апеллируемости - сам автор пытается «откреститься» от своих слов, подписанных им однажды.

В отношении ИС применяются иные категории:

- ***надежность*** - гарантия того, что система ведет себя в нормальном и внештатном режимах так, как запланировано;
- ***точность*** - гарантия точного и полного выполнения всех команд;
- ***контроль доступа*** - гарантия того, что различные группы лиц имеют различный доступ к информационным объектам и эти ограничения доступа постоянно выполняются;
- ***контролируемость*** - гарантия того, что в любой момент может быть произведена полноценная проверка любого компонента программного комплекса;
- ***контроль идентификации*** - гарантия того, что клиент, подключенный в данный момент к системе, является именно тем, за кого себя выдает;
- ***устойчивость к умышленным сбоям*** - гарантия того, что при умышленном внесении ошибок в пределах заранее оговоренных норм система будет вести себя так, как оговорено заранее.

Защита информации

Защитить информацию – это значит:

- обеспечить физическую целостность информации, т.е. не допустить искажений или уничтожения элементов информации;
- не допустить подмены (модификации) элементов информации при сохранении ее целостности;
- не допустить несанкционированного получения информации лицами или процессами, не имеющими на это соответствующих полномочий;
- быть уверенным в том, что передаваемые (продаваемые) владельцем информации ресурсы будут использоваться только в соответствии с обговоренными сторонами условиями.

Способы воздействия на автоматизированную систему

Существует достаточно много способов несанкционированного доступа к информации:

- просмотр;
- копирование и подмена данных;
- ввод ложных программ и сообщений в результате подключения к каналам связи;
- чтение остатков информации на ее носителях;
- прием сигналов электромагнитного излучения и волнового характера;
- использование специальных программных и аппаратных "заглушек" и т.п.

Причины искажения информации

- отказы и сбои аппаратуры в случае ее некачественного исполнения и физического старения;
- помехи в каналах и на линиях связи от воздействия внешней среды;
- аварийные ситуации (пожар, наводнение, выход из строя электропитания и др.);
- схемные и системотехнические ошибки и просчеты разработчиков и производителей ПК;
- алгоритмические и программные ошибки;
- ошибки человека в работе с ПК.

Объекты и элементы защиты

В качестве ***объектов защиты*** информации в СОД выступают:

- терминалы пользователей (ПК, рабочие станции);
- терминал администратора сети или групповой абонентский узел;
- узел связи;
- средства отображения информации;
- средства документирования информации;
- машинный (компьютерный) зал и хранилище носителей информации);
- внешние каналы связи и сетевое оборудование;
- накопители и носители информации.

В качестве ***элементов защиты*** выступают блоки (порции, массивы, потоки и др.) информации в объектах защиты, в частности:

- данные и программы в основной памяти компьютера;
- данные и программы на внешнем накопителе;
- данные, отображаемые на экране монитора;
- данные, выводимые на принтер;
- пакеты данных, передаваемые по каналам связи;
- данные, размножаемые с помощью копировально-множительного оборудования;
- отходы обработки информации в виде бумажных и магнитных носителей;
- журналы назначения паролей и приоритетов зарегистрированным пользователям;
- служебные инструкции по работе с комплексами задач;
- архивы данных и программного обеспечения и др.

Комплексы защитных мер

- *Организационно – административные средства защиты;*
- *Технические средства защиты;*
- *Программные средства и методы защиты;*
- *Технологические средства защиты информации;*
- *правовым и морально-этическим мерам и средствам защиты.*

Защита паролями

- ***Пароль*** – это совокупность символов, определяющая объект (субъекта).
- · не хранить пароли в вычислительной системе в незашифрованном виде;
- · не печатать и не отображать пароли в явном виде на терминале пользователя;
- · не использовать в качестве пароля свое имя или имена родственников, а также личную информацию (дата рождения, номер домашнего или служебного телефона, название улицы и др.);
- · не использовать реальные слова из энциклопедии или толкового словаря;
- · выбирать длинные пароли;
- · использовать смесь символов верхнего и нижнего регистров клавиатуры;
- · использовать комбинации из двух простых слов, соединенных специальными символами(например, +, = и др.);
- · придумывать новые слова (абсурдные или даже бредового содержания);
- · чаще менять пароль.

Идентификация и аутентификация

- ***Идентификация*** – это присвоение какому-либо объекту или субъекту уникального имени или образа.
- ***Аутентификация*** – это установление подлинности, т.е. проверка, является ли объект (субъект) действительно тем, за кого он себя выдает.

Компьютерные вирусы и антивирусные программные средства

Понятие вируса и признаки его проявления

- ***Компьютерным вирусом*** принято называть специально написанную, обычно небольшую по размерам программу, способную самопроизвольно присоединяться к другим программам

К признакам появления вируса можно отнести:

- § замедление работы компьютера;
- § невозможность загрузки операционной системы;
- § частые "зависания" и сбои в работе компьютера;
- § прекращение работы или неправильная работа ранее успешно функционировавших программ;
- § изменение размеров файлов;
- § периодическое появление на экране монитора неуместных сообщений;
- § уменьшение объема свободной оперативной памяти;
- § возрастание времени доступа к жесткому диску;
- § изменение даты и времени создания файлов;
- § разрушение файловой структуры (исчезновение файлов, искажение каталогов и др.);
- § загорание сигнальной лампочки дисковода, когда к нему нет обращения.

Виды вирусов

- В зависимости от среды обитания вирусы подразделяются на загрузочные, файловые, системные, сетевые, файлово-загрузочные.
- По способу заражения среды обитания вирусы подразделяются на резидентные и на нерезидентные.
-

Защита программных продуктов

- Защита программных продуктов преследует следующие цели:
- § ограничить несанкционированный доступ отдельных категорий пользователей к работе с ними;
- § исключить преднамеренную порчу программ с целью нарушения нормального хода обработки данных;
- § исключить преднамеренную модификацию программы с целью порчи репутации производителя программной продукции;
- § исключить несанкционированное тиражирование (копирование) программ;
- § исключить несанкционированное изучение содержания, структуры и механизма работы программы.