Особенности защиты информации в персональных ЭВМ

Защита информации в персональных компьютерах

Персональные компьютеры (ПК) обладают всеми свойствами ЭВМ других классов, поэтому все проблемы защиты информации в построенных на их основе системах и подходы к защите аналогичны. Однако персональным компьютерам присущ ряд таких свойств, которые, с одной стороны, благоприятствуют защите, а с другой — затрудняют ее и усложняют.

К таким свойствам относятся:

• малые габариты и вес, что делает их не просто транспортабельными, а легко переносимыми;
• наличие встроенного внутреннего ЗУ большого объема, сохраняющего записанные данные после выключения питания;
• наличие сменного ЗУ большого объема и малых габаритов;
• наличие устройств сопряжения с каналами связи;
•оснащенность программным обеспечением с широкими функциональными возможностями;
• массовость производства и распространения;
• относительно низкая стоимость.

Особенностями защиты обусловлена необходимость самостоятельного рассмотрения вопросов защиты информации в персональных ЭВМ.

На формирование множества возможных подходов к защите информации в ПК и выбор наиболее целесообразного из них в конкретных ситуациях определяющее влияние оказывают следующие факторы:

1) цели защиты;
2) потенциально возможные способы защиты;
3) имеющиеся средства защиты.

Основные цели защиты информации:

- обеспечение физической целостности;
- обеспечение логической целостности;
- предупреждение несанкционированного получения;
- предупреждение несанкционированной модификации;
- предупреждение несанкционированного копирования.

Физическая целостность информации в ПК зависит от целостности самого ПК, целостности дисков, целостности информации на дисках и полях оперативной памяти. В широком спектре угроз целостности, информации в ПК следует обратить особое внимание на угрозы, связанные с недостаточно высокой квалификацией большого числа владельцев ПК.

Предупреждение **несанкционированного получения** информации, находящейся в ПК, приобретает особую актуальность в тех случаях, когда хранимая или обрабатываемая информация содержит тайну того или иного характера (государственную, коммерческую и т. п.).

Весьма опасной разновидностью **несанкционированной модификации** информации в ПК является действие вредоносных программ (компьютерных вирусов), которые могут разрушать или уничтожать программы или массивы данных.

Актуальность предупреждения **несанкционированного копирования** определяется следующими тремя обстоятельствами:

- накопленные массивы информации все больше становятся товаром;
- все более широкое распространение получает торговля компьютерными программами;
- оптические дисководы с перезаписью создают весьма благоприятные условия для широкомасштабного копирования информации ПК.

Угрозы информации в персональных ЭВМ

Характерные для ПК каналы утечки информации принято классифицировать по типу средств, которые используются в целях несанкционированного получения по ним информации, причем выделяются три типа средств: человек, аппаратура, программа.

Группу каналов, в которых основным средством несанкционированного получения информации является человек, составляют:

- хищение носителей информации (магнитных дисков, распечаток и т. д.);
- чтение или фотографирование информации с экрана;
- чтение или фотографирование информации с распечаток.

В группе каналов, основным средством использования которых служит аппаратура, выделяют:

• подключение к устройствам ПК специальной аппаратуры, с помощью которой можно уничтожать или регистрировать защищаемую информацию;
• регистрацию с помощью специальных средств электромагнитных излучений устройств ПК в процессе обработки защищаемой информации.

Третью группу каналов (основное средство использования которых — программы) образуют:

• программный несанкционированный доступ к информации;
• уничтожение (искажение) или регистрация защищаемой информации с помощью программных закладок или ловушек;
• чтение остаточной информации из ОЗУ;
• программное копирование информации с магнитных носителей.

Для разработки мероприятий защиты информации необходимы следующие исходные характеристики элементов защиты:

- возможные объемы находящейся в них информации;
- возможная продолжительность пребывания информации;
- возможные угрозы информации;
- возможные средства защиты.

Обеспечение целостности информации в ПК

Угрозы целостности информации в ПК, как и в любой другой автоматизированной системе, могут быть случайными и преднамеренными.

Основными разновидностями **случайных угроз** являются отказы, сбои, ошибки, стихийные бедствия и побочные явления, а конкретными источниками их проявления — технические средства, программы и пользователи.

Преднамеренные угрозы, создаваемые людьми в злоумышленных целях. Такая угроза может быть непосредственной, если злоумышленник получает доступ к ПК, и опосредованной, когда угроза создается с помощью промежуточного носителя, чаще всего с помощью флеш-накопителя.