Вредоносные закладки в ПК и борьба с ними

К **основным** разновидностям вредоносного воздействия относятся воздействие на информацию (уничтожение, искажение, модификация) и воздействие на систему (вывод из строя, ложное инициирование действия, модификация содержания выполняемых функций, создание помех в работе).

Классификация закладок и их общие характеристики

Известные в настоящее время закладки осуществляются **аппаратным** или **программным** путем.

Аппаратные закладки могут быть осуществлены в процессе изготовления ПК, ее ремонта или проведения профилактических работ. Реальная угроза таких закладок создается массовым и практически неконтролируемым распространением ПК. Особая опасность аппаратных закладок заключается в том, что они могут длительное время не проявлять своих вредоносных воздействий, а затем начать их осуществление или по истечении определенного времени, или при наступлении некоторого состояния ПК.


lenovo

Программные закладки с точки зрения массового пользователя представляются особо опасными в силу сравнительной (относительно аппаратных) простоты их осуществления, высокой динамичности их распространения и повышенной трудности защиты от них.

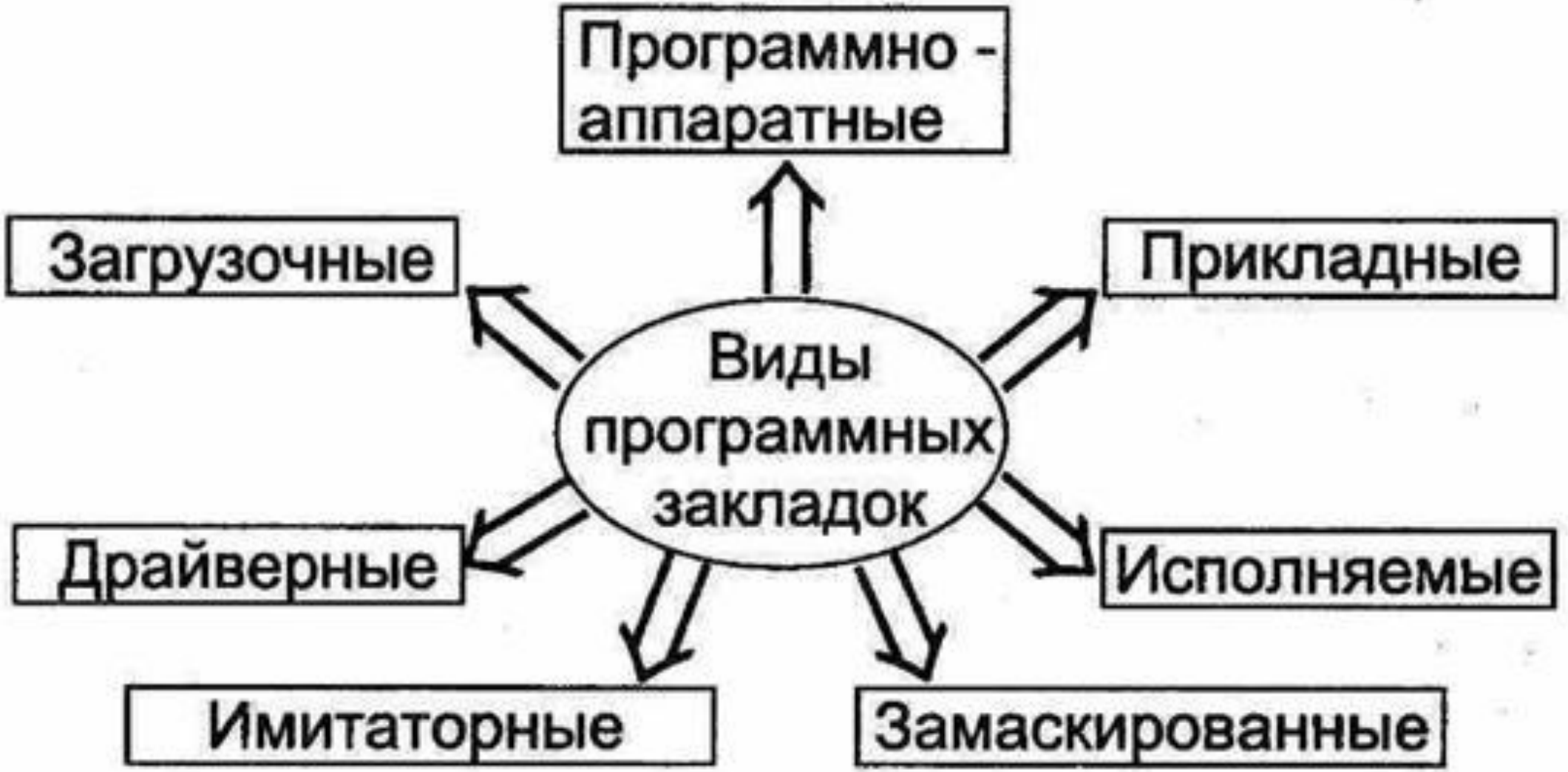

Рис. 2.23. Виды программныех закладки, классифицированныеок по методу их внедрения в сеть

Программные закладки могут появиться в любое время, чему особенно способствуют следующие обстоятельства:

1) массовый обмен информацией, принявший к настоящему времени характер броуновского движения (беспорядочное движение);

2) широкое распространение копий программ, приобретенных незаконным путем;

3) возможности дистанционного воздействия на ПК, подключенные к сети;

4) широкий и непрерывно растущий диапазон разновидностей закладок, что усложняет процессы их обнаружения и нейтрализации.

К настоящему времени известно значительное количество закладок, получивших такие условные наименования: троянский конь, бомба, ловушка, люк, вирус, червь.

Троянский конь — несаморазмножающееся РПС (разрушающие программные средства), способное осуществлять несанкционированное считывание данных, их уничтожение и другие деструктивные функции.

Бомба — несаморазмножающееся РПС одноразового использования, приводящееся в действие в определенных условиях (в заданное время, в заданном состоянии ЭВМ, по команде извне) и осуществляющее крупномасштабное уничтожение информации.

Ловушка — несаморазмножающаяся программа, осуществляющая несанкционированный перехват информации и запись ее в соответствующее поле ЗУ или выдачу в канал связи.

Люк — несаморазмножающаяся программа, обеспечивающая злоумышленнику возможности несанкционированного Доступа к защищаемой информации.

Вирус — саморазмножающееся РПС, способное уничтожать или изменять данные и/или программы, находящиеся в ЭВМ.

Червь — саморазмножающееся РПС, способное уничтожать элементы данных или программ.

Принципиальные подходы и общая схема защиты от закладок

Для **защиты** от закладок должны использоваться методы анализа, синтеза и управления, организационно-правовые, аппаратные и программные средства.

Средства борьбы с вредоносными закладками можно разделить на юридические, организационно-административные, аппаратные и программные.

Юридические средства сводятся к установлению ответственности за умышленное создание и распространение закладок в целях нанесения ущерба.

Организационно-административная защита от вредоносных программ заключается в выработке и неукоснительном осуществлении организационных и организационно-технических мероприятий, направленных на предупреждение заражения компьютеров этими программами.

Основными мероприятиями по защите программ и данных в организациях, использующих **программы**, представляются следующие:

1) приобретение только законным путем необходимых технических средств и программ, сертифицированных на отсутствие вредоносных закладок;

2) создание эталонных копий основных программ и резервирование баз данных;

3) организация автоматизированной обработки данных с соблюдением всех приемов и правил;

4) периодическая тщательная проверка состояния программного обеспечения и баз данных;

5) проверка психологических особенностей сотрудников при приеме на работу;

6) создание и поддержание в коллективах здорового морально-психологического климата.