Введение

Современный мир невозможно представить без средств коммуникаций и вычислительной техники, в которых главенствующую роль играет программное обеспечение. Информационные технологии прогрессируют очень быстро, охватывая все более широкие области человеческой деятельности. Поэтому безопасность информационных технологий является одним из важнейших аспектов обеспечения их функционирования.

Статистика показывает, что с каждым годом растет финансовый ущерб, наносимый компьютерными преступниками. Рост числа пользователей, недостатки в программном обеспечении пользователей, наличие свободного доступа к зловредным программам, а также практическая ненаказуемость совершения проступков привели к тому, что организациям, компаниям и рядовым пользователям приходится уделять внимание и время обеспечению защиты.

Современные распределенные компьютерные системы не могут быть защищены только использованием организационных мер и средств физической защиты. Для безопасности функционирования информационных технологий необходимо использовать механизмы и средства сетевой защиты, которые обеспечивают конфиденциальность, целостность и доступность компьютерных систем, программного обеспечения и данных.

В последнее десятилетие сформировался рынок средств обеспечения информационной безопасности, все большее число различных организаций подключается к решению насущных задач обеспечения защиты. Решение этих задач осложняется рядом причин. Среди них необходимо отметить следующие: отсутствие единой терминологии и единой теории обеспечения защиты, использование, как правило, программных средств зарубежных производителей, высокую стоимость качественных средств защиты. Реализация защиты информации в современных корпоративных сетях опирается на использование средств защиты, реализованных программными, аппаратными и программно-аппаратными методами. Количество изданий и статей, посвященных различным вопросам обеспечения информационной безопасности, увеличивается с каждым годом.

Значимость обеспечения безопасности государства в информационной сфере подчеркнута в принятой в сентябре 2000 года «Док-

трине информационной безопасности Российской Федерации»: «Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать».

Остроту межгосударственного информационного противоборства можно наблюдать в оборонной сфере, высшей формой которой являются информационные войны. Элементы такой войны уже имели, а в ряде случаев до сих пор имеют место в локальных военных конфликтах на Ближнем Востоке, на Балканах, на территории бывших стран СНГ и т. д. Один из характерных примеров — вывод из строя войсками НАТО системы противовоздушной обороны Ирака с помощью информационного оружия. Эксперты предполагают, что войска альянса использовали программную закладку, внедренную заблаговременно в принтеры, которые были закуплены Ираком у французской фирмы и использовались в АСУ ПВО.

В настоящее время МО США (Объединённая доктрина информационных операций JP 3-13 от 27.11.2012) приняло следующее определение термина «информационная война» — *это действия, предпринимаемые для достижения информационного превосходства над противником путем воздействия на имеющуюся у него информацию, зависящие от информации процессы, информационные системы и компьютерные сети*.

Объектом внимания в такой войне становятся информационные системы, а также информационные технологии, используемые в системах вооружений. Информационным оружием в такой войне следует называть средства уничтожения, искажения или хищения информационных массивов, средства преодоления систем защиты, ограничения допуска законных пользователей, дезорганизации работы аппаратуры и компьютерных систем в целом. К ним относятся:

- компьютерные вирусы, способные размножаться, внедряться в программы, передаваться по линиям связи, сетям передачи данных, выводить из строя системы управления;
- логические бомбы — запрограммированные устройства, которые внедряют в информационно-управляющие центры военной или гражданской инфраструктуры, чтобы по сигналу или в установленное время привести их в действие;
- средства подавления информационного обмена в телекоммуникационных сетях, фальсификация информации в каналах государственного и военного управления;
- средства нейтрализации тестовых программ;
- ошибки различного рода, сознательно вводимые злоумышленниками в программное обеспечение объекта.

Мерами для предотвращения или нейтрализации последствий применения информационного оружия являются:

- защита материально-технических объектов, составляющих физическую основу информационных ресурсов;
- обеспечение нормального и бесперебойного функционирования баз и банков данных;
- защита информации от несанкционированного доступа, ее искажения и уничтожения;
- сохранение качества информации (своевременности, точности, полноты и необходимой доступности).

Обеспечение безопасности АС предполагает создание препятствий для любого несанкционированного вмешательства в процесс ее функционирования, а также для попыток хищения модификации, выведения из строя или разрушения всех ее компонентов.

Противоборство государств в области информационных технологий, стремление криминальных структур противоправно использовать информационные ресурсы, необходимость обеспечения прав граждан в информационной сфере, наличие множества случайных угроз вызывают острую необходимость обеспечения защиты информации в компьютерных системах (КС), являющихся материальной основой информатизации общества.

Проблема обеспечения информационной безопасности на всех уровнях может быть решена успешно только в том случае, если создана и функционирует комплексная система защиты информации, охватывающая весь жизненный цикл компьютерных систем от разработки до утилизации и всю технологическую цепочку сбора, хранения, обработки и выдачи информации.