Информационные технологии во всех сферах общественной жизни быстро развиваются . Это общее стремления государств, организаций и отдельных граждан получить преимущества за счет овладения информацией, недоступной конкурентам .
Значимость обеспечения безопасности государства в информационной сфере подчеркнута в принятой в сентябре 2000 года "Доктрине информационной безопасности Российской Федерации"

Противостояние государств в области информационных технологий, стремление злоумышленников противоправно использовать информационные ресурсы, наличие множества случайных угроз вызывают острую необходимость обеспечения защиты информации в компьютерных системах.

В данной работе я хотел бы осветить тему несанкционированного доступа и утечки информации, а также совершенствование методов и средств несанкционированного получения информации.

1. Несанкционированный доступ к информации

Термин несанкционированный доступ к информации определен как доступ к информации, нарушающий правила доступа с использованием штатных средств вычислительной техники или автоматизированных систем.

Под правилами разграничения доступа понимается совокупность положений, регламентирующих права доступа лиц или процессов к единицам информации

Выполнение плана по разграничения доступа в компьютерных системах реализуется за счет создания системы разграничения доступа.

Несанкционированный доступ к информации возможен только с использованием штатных аппаратных и программных средств в следующих случаях:

отсутствует система разграничения доступа;

сбой или отказ в компьютерных системах;

ошибочные действия пользователей или обслуживающего персонала компьютерных систем;

ошибки в системе разграничения доступа;

фальсификация полномочий.

Если эта система отсутствует, то злоумышленник, имеющий навыки работы в компьютерных системах, может получить без ограничений доступ к любой информации.

2. Электромагнитные излучения и наводки

Процесс обработки и передачи информации техническими средствами компьютерных систем сопровождается электромагнитными излучениями в окружающее пространство . С помощью специального оборудования сигналы принимаются, выделяются, усиливаются и могут либо просматриваться, либо записываться в запоминающих устройствах.

3. Вредительские программы

Главным источником угроз безопасности информации в компьютерных системах является использование специальных программ, получивших название "вредительские программы".

Вредительские программы делятся на четыре класса:

1)логические бомбы

2)черви;

3)троянские кони;

4)компьютерные вирусы.

Заключение

Таким образом информация является неотъемлемой частью жизнедеятельности человека. Значимость какой-либо информации достигает национальных

масштабов, тем самым остро влияя на вопрос её защиты от утечки или уничтожения.

Защита информации должна иметь комплексный характер и не ограничиваться каким-либо одним из видов, но и ограничивать круг лиц имеющих доступ к этой информации , а также уровни доступа к защищаемой информации.
Тем самым, только после проведения полномасштабного комплекса мер по защите, уже можно будет говорить, что информация защищена, и ей ничто не угрожает.