1.2. Анализ угроз информационной безопасности

Рассмотрение возможных угроз информационной безопасности приводится с целью определения полного набора требований к разрабатываемой системе защиты.

По цели воздействия различают три основных типа угроз безопасности АСОИ:

- угрозы нарушения конфиденциальности информации;
- угрозы нарушения целостности информации;
- угрозы нарушения работоспособности системы (отказы в обслуживании).

Классификация возможных угроз информационной безопасности АСОИ может быть приведена по ряду базовых признаков:

1. По *природе возникновения* различают:
    - естественные угрозы;
    - искусственные угрозы.
2. По *степени преднамеренности проявления* различают:
    - угрозы, вызванные ошибками или халатностью персонала;
    - угрозы преднамеренного действия.
3. По *непосредственному источнику угроз*. Источниками угроз могут быть:
    - природная среда;
    - человек;
    - санкционированные программно-аппаратные средства;
    - несанкционированные программно-аппаратные средства.
4. По *положению источника угроз*. Источник угроз может быть расположен:
    - вне контролируемой зоны АСОИ;
    - в пределах контролируемой зоны АСОИ;
    - непосредственно в АСОИ.
5. По *степени зависимости от активности* АС. Угрозы проявляются:
    - независимо от активности АСОИ;
    - только в процессе обработки данных.
6. По *степени воздействия на* АСОИ различают:
    - пассивные угрозы;
    - активные угрозы.
7. По *этап доступа пользователей или программ к ресурсам* АСОИ различают:
    - угрозы, проявляющиеся на этапе доступа к ресурсам АСОИ;
    - угрозы, проявляющиеся после разрешения доступа к ресурсам АСОИ.
8. По *способу доступа к ресурсам* АСОИ различают:
    - угрозы, с использованием стандартного пути доступа к ресурсам АСОИ;

- угрозы с использованием скрытого нестандартного пути доступа к ресурсам АСОИ.

9. По *текущему месту расположения информации, хранимой и обрабатываемой в* АСОИ, различают:
   - угрозы доступа к информации на внешних запоминающих устройствах;
   - угрозы доступа к информации в оперативной памяти;
   - угрозы доступа к информации, циркулирующей в линиях связи;
   - угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере.

Опасные воздействия на АСОИ можно подразделить на *случайные* и *преднамеренные*.

Исходя из возможности возникновения наиболее опасной ситуации, обусловленной действиями нарушителя, можно составить гипотетическую модель потенциального нарушителя:

- квалификация нарушителя может быть на уровне разработчика данной системы;
- нарушителем может быть как постороннее лицо, так и законный пользователь системы;
- нарушителю известна информация о принципах работы системы;
- нарушитель выберет наиболее слабое звено в защите.

Несанкционированный доступ (НСД) является наиболее распространенным и многообразным видом компьютерных нарушений. Суть НСД состоит в получении пользователем (нарушителем) доступа к объекту в нарушение правил разграничения доступа, установленных в соответствии с принятой в организации политикой безопасности. НСД использует любую ошибку в системе защиты и возможен при нерациональном выборе средств защиты, их некорректной установке и настройке. НСД может быть осуществлен как штатными средствами АСОИ, так и специально созданными аппаратными и программными средствами.

Перечислим основные каналы несанкционированного доступа, через которые нарушитель может получить доступ к компонентам АСОИ и осуществить хищение, модификацию и/или разрушение информации:

- все штатные каналы доступа к информации (терминалы пользователей, оператора, администратора системы; средства отображения и документирования информации; каналы связи) при их использовании нарушителями, а также законными пользователями вне пределов их полномочий;
- технологические пульты управления;
- линии связи между аппаратными средствами АСОИ;
- побочные электромагнитные излучения от аппаратуры, линий связи, сетей электропитания и заземления и др.

Из всего разнообразия способов и приемов несанкционированного доступа остановимся на следующих распространенных и связанных между собой нарушениях:

- перехват паролей;
- "маскарад";
- незаконное использование привилегий.