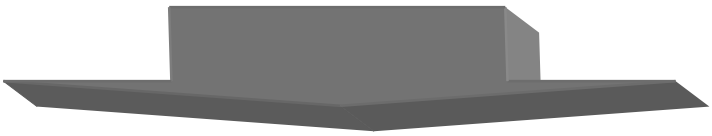
При определении угроз безопасности объекта следует различать:



1. угрозы, не являющиеся атакой
2. атаки.

структура угроз, не являющихся атаками:

угрозы, не связанные с деятельностью человека: стихийные бедствия и природные явления (землетрясения, наводнения, ураганы и т.д.);

угрозы социально–политического характера: забастовки, саботаж, локальные конфликты и т.д.;

ошибочные действия и (или) нарушения тех или иных требований лицами, санкционировано взаимодействующими с возможными объектами угроз

- непредумышленное искажение или удаление программных компонентов АСЗИ;
- внедрение и использование неучтенных программ;
- игнорирование организационных ограничений (установленных правил) при работе с ресурсами АСЗИ, включая средства защиты информации. **В частности:**
- нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (в частности, ключевой, парольной и аутентифицирующей информации);
- предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований;
- настройка и конфигурирование средств защиты информации, а также технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, в нарушение нормативных и технических документов;
- несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа.

угрозы техногенного характера, основными из которых являются:
- аварии (отключение электропитания, системы заземления, разрушение инженерных сооружений и т.д.);
- неисправности, сбои аппаратных средств, нестабильность параметров системы электропитания, заземления и т.д.;
- помехи и наводки, приводящие к сбоям в работе аппаратных средств.

Атаки являются наиболее опасными угрозами (что обусловлено их тщательной подготовкой, скрытностью проведения, целенаправленным выбором объектов и целей атак). Атаки готовятся и проводятся нарушителем, причем возможности проведения атак обусловлены возможностями нарушителя.

Основными каналами атак являются:

- **каналы связи (как внутри, так и вне контролируемой зоны), не защищенные от НСД к информации организационно-техническими мерами;**
- **штатные средства.**

Возможные каналы атак:

- **каналы непосредственного доступа к объекту атаки (акустический, визуальный, физический);**
- **машинные носители информации;**
- **носители информации, выведенные из употребления;**
- **технические каналы утечки;**
- **сигнальные цепи;**
- **цепи электропитания;**
- **цепи заземления;**
- **канал утечки за счет электронных устройств негласного получения информации;**
- **информационные и управляющие интерфейсы СВТ.**