**Объект** — пассивный компонент системы, хранящий, перерабатывающий, передающий или принимающий информацию; примеры объектов: страницы, файлы, папки, директории, компьютерные программы, устройства (мониторы, диски, принтеры и т. д.).

Под **субъектами** информационных отношений понимаются как владельцы, так и пользователи информации и поддерживающей инфраструктуры. **Субъект** — активный компонент системы, который может инициировать поток информации; примеры субъектов: пользователь, процесс либо устройство.

Угроза информационной безопасности объекта — возможные воздействия на него, приводящие к ущербу.

Природа воздействий на информационный объект бывают непреднамеренными и преднамеренными, однако все воздействия могут привести к последствиям 3-х видов:

– нарушение конфиденциальности;

– нарушение доступности;

– нарушение целостности.

Под **угрозами** информационной безопасности понимаются потенциально возможные негативные воздействия на защищаемую информацию, к числу которых относятся:

* + несанкционированное распространение (передача) персональных данных;
  + утрата сведений, составляющих конфиденциальную информацию, персональные данные Учреждения и иную защищаемую информацию, а также искажение такой информации;
  + утечка – несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение и т.д);
  + недоступность информации в результате ее блокирования, сбоя оборудования или программ, дезорганизации функционирования операционных систем рабочих станций, серверов, маршрутизаторов, систем управления баз данных, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств;
  + отсутствие планирования и контроля;
  + низкая степень надежности программного обеспечения;
  + недостаточная осведомленность персонала, низкая квалификация персонала и пользователей в области информационных технологий.

Источниками **внутренних угроз** могут являться:

* сотрудники организации;
* программное обеспечение;
* аппаратные средства.

**Внутренние угрозы** могут проявляться в следующих формах:

* ошибки системных администраторов;
* нарушения сотрудниками установленных регламентов сбора, обработки, передачи и уничтожения информации;
* ошибки в работе программного обеспечения;
* отказы и сбои в работе компьютерного оборудования.

К **внешним источникам** угроз относятся:

* компьютерные вирусы и вредоносные программы;
* организации и отдельные лица;
* стихийные бедствия.

**Внешние угрозы** могут проявляться в следующих формах:

* несанкционированный доступ к персональным данным клиентов агентства и сотрудников компании;
* неработоспособность компьютерного оборудования вследствие стихийных бедствий;
* кража денежных ресурсов компании;
* ущерб, связанный с разглашением персональных данных отдельных лиц.

По происхождению угрозы можно подразделить на преднамеренные и непреднамеренные.

**Непреднамеренные угрозы** — это действия, которые совершают люди по неосторожности, незнанию, невнимательности или из любопытства. К такому типу угроз относят установку программных продуктов, которые не входят в список необходимых для работы, и в последствии могут стать причиной нестабильной работы системы и потеря информации.

**Преднамеренные угрозы** — угрозы, связанные со злым умыслом преднамеренного физического разрушения, впоследствии выхода из строя системы. К преднамеренным угрозам относятся внутренние и внешние атаки.

В свою очередь, информационные угрозы могут быть обусловлены:

* Естественными факторами
* Человеческими факторами.

Человеческие факторы в свою очередь подразделяются на угрозы, несущие случайный неумышленный характер и угрозы умышленного характера, которые делятся на активные/неактивные и внутренние/внешние.

**Пассивные угрозы** направлены на несанкционированное использование информационных ресурсов (прослушивание).

**Активные угрозы** имеют цель: нарушение нормального процесса функционирования системы посредством целенаправленного воздействия на информационные ресурсы.

По способам воздействия на объекты информационной безопасности угрозы подлежат следующей классификации:

* информационные;
* программные;
* физические.

Снижение рисков за счет использования контрмер может осуществляться различными **способами**:

* уменьшением вероятностей осуществления угроз безопасности;
* ликвидацией уязвимостей или уменьшением их величин;
* уменьшением величины возможного ущерба;
* восстановлением ресурсов, которым был нанесен ущерб;
* выявлением атак и других нарушений безопасности.

Выбор варианта защиты активов осуществляется на основании результатов оценки рисков с учетом требований безопасности и существующих стоимостных и других ограничений.

**Система мер**, рекомендуемая для большинства компаний, перед которыми стоит вопрос защиты информации, призвана обеспечить соблюдение основных признаков ее безопасности:

− Доступность сведений. Под этим определением понимается возможность и для авторизованного субъекта в любое время получить требуемые данные, и для клиентов в регулярном режиме получать информационные услуги;

− Целостность информации. Это означает ее неизменность, отсутствие любых посторонних, неавторизованных вмешательств, направленных на изменение или уничтожение данных, нарушение системы их расположения;

− Конфиденциальность или абсолютная недоступность данных для неавторизованных субъектов;

− Отсутствие отказа или невозможность отрицать принадлежность действий или данных;

− Аутентичность или возможность достоверного подтверждения авторства информационных сообщений или действий в системе.