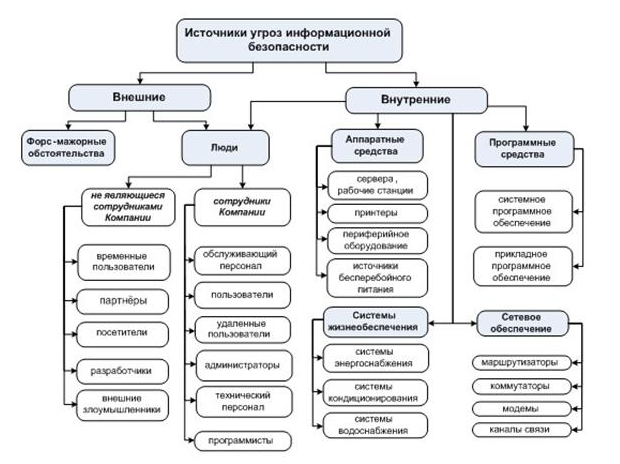
**Угроза**— это потенциальная возможность определённым образом нарушить ИБ. Попытка реализации угрозы называется**атакой**, а тот, кто предпринимает такую попытку, — **злоумышленником**, или **злонамеренным пользователем**. Чаще всего угроза является следствием наличия уязвимых мест в защите ИС.

Моделирование и классификацию источников угроз и их проявлений, целесообразно проводить на основе анализа взаимодействия логической цепочки:   
  
**источник угрозы - фактор (уязвимость) - угроза (действие) - последствия (атака).**  


Под этими терминами будем понимать:

**Источник угрозы** - это потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.

**Угроза (действие)** [Threat] - это возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику, владельцу или пользователю, проявляющегося в опасности искажения и потери информации.

**Фактор (уязвимость)** [Vulnerability] - это присущие объекту информатизации причины, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные недостатками процесса функционирования объекта информатизации, свойствами архитектуры автоматизированной системы, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации.

**Последствия (атака)** - это возможные последствия реализации угрозы (возможные действия) при взаимодействии источника угрозы через имеющиеся факторы (уязвимости).

Как видно из определения, атака - это всегда пара "источник - фактор", реализующая угрозу и приводящая к ущербу. При этом анализ последствий предполагает проведение анализа возможного ущерба и выбора методов парирования угроз безопасности информации.

Промежуток времени от момента, когда появляется возможность использовать слабое место, до момента, когда пробел ликвидируется, называется **окном опасности**. Для большинства уязвимых мест окно опасности существует сравнительно долго (несколько дней или недель), поскольку за это время должны произойти следующие события:

* должно стать известно о средствах использования пробела в защите;
* должны быть выпущены соответствующие исправления;
* исправления должны быть установлены в защищаемой ИС

Некоторые угрозы являются следствием каких-то ошибок или просчётов, другие существуют в силу самой природы современных ИС. Например, угроза отключения электричества или выхода его параметров за допустимые границы существует в силу зависимости аппаратного обеспечения ИС от качественного электропитания.

Подчеркнем, что само понятие " *угроза* " в разных ситуациях зачастую трактуется *по*-разному. Например, для подчеркнуто открытой организации *угроз* конфиденциальности может просто не существовать - вся *информация* считается общедоступной; однако в большинстве случаев нелегальный *доступ* представляется серьезной опасностью. Иными словами, *угрозы*, как и все в ИБ, зависят от интересов *субъектов информационных отношений* (и от того, какой *ущерб* является для них неприемлемым).

**Ущерб как категория классификации угроз**

Проявления возможного ущерба могут быть различны:

* моральный и материальный ущерб деловой репутации организации;
* моральный, физический или материальный ущерб, связанный с разглашением персональных данных отдельных лиц;
* материальный (финансовый) ущерб от разглашения защищаемой (конфиденциальной) информации;
* материальный (финансовый) ущерб от необходимости восстановления нарушенных защищаемых информационных ресурсов;
* материальный ущерб (потери) от невозможности выполнения взятых на себя обязательств перед третьей стороной;
* моральный и материальный ущерб от дезорганизации деятельности организации;
* материальный и моральный ущерб от нарушения международных отношений.

Ущерб может быть причинен каким-либо субъектом и в этом случае имеется на лицо правонарушение, а также явиться следствием независящим от субъекта проявлений (например, стихийных случаев или иных воздействий, таких как проявления техногенных свойств цивилизации). В первом случае налицо вина субъекта, которая определяет причиненный вред как состав преступления, совершенное по злому умыслу (умышленно, то есть деяние совершенное с прямым или косвенным умыслом) или по неосторожности (деяние, совершенное по легкомыслию, небрежности, в результате невиновного причинения вреда) и причиненный ущерб должен квалифицироваться как состав преступления, оговоренный уголовным правом.   
  
Во втором случае ущерб носит вероятностный характер и должен быть сопоставлен, как минимум с тем риском, который оговаривается гражданским, административным или арбитражным правом, как предмет рассмотрения.   
  
В теории права под ущербом понимается невыгодные для собственника имущественные последствия, возникшие в результате правонарушения. Ущерб выражается в уменьшении имущества, либо в недополучении дохода, который был бы получен при отсутствии правонарушения (упущенная выгода).   
  
При рассмотрении в качестве субъекта, причинившего ущерб какую-либо личность, категория "ущерб" справедлива только в том случае, когда можно доказать, что он причинен, то есть деяния личности необходимо квалифицировать в терминах правовых актов, как состав преступления. Поэтому, при классификации угроз безопасности информации в этом случае целесообразно учитывать требования действующего уголовного права, определяющего состав преступления.

Вот некоторые примеры составов преступления, определяемых Уголовным Кодексом Российской Федерации.

**Хищение** - совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившее ущерб собственнику или владельцу имущества.

**Копирование компьютерной информации** - повторение и устойчивое запечатление информации на машинном или ином носителе.

**Уничтожение** - внешнее воздействие на имущество, в результате которого оно прекращает свое физическое существование либо приводятся в полную непригодность для использования по целевому назначению. Уничтоженное имущество не может быть восстановлено путем ремонта или реставрации и полностью выводится из хозяйственного оборота.

**Уничтожение компьютерной информации** - стирание ее в памяти ЭВМ.

**Повреждение** - изменение свойств имущества, при котором существенно ухудшается его состояние, утрачивается значительная часть его полезных свойств и оно становится полностью или частично непригодным для целевого использования.

**Модификация компьютерной информации** - внесение любых изменений, кроме связанных с адаптацией программы для ЭВМ или баз данных.

**Блокирование компьютерной информации** - искусственное затруднение доступа пользователей к информации, не связанное с ее уничтожением.

**Несанкционированное уничтожение, блокирование модификация, копирование информации** - любые не разрешенные законом, собственником или компетентным пользователем указанные действия с информацией.

**Обман (отрицание подлинности, навязывание ложной информации)** - умышленное искажение или сокрытие истины с целью ввести в заблуждение лицо, в ведении которого находится имущество и таким образом добиться от него добровольной передачи имущества, а также сообщение с этой целью заведомо ложных сведений.

Однако, говорить о злом умысле личности в уничтожении информации в результате стихийных бедствий не приходится, как и тот факт, что вряд ли стихия сможет воспользоваться конфиденциальной информацией для извлечения собственной выгоды. Хотя и в том и в другом случае собственнику информации причинен ущерб. Здесь правомочно применение категории "причинение вреда имуществу". При этом, речь пойдет не об уголовной ответственности за уничтожение или повреждение чужого имущества, а о случаях подпадающих под гражданское право в части возмещения причиненного ущерба (риск случайной гибели имущества - то есть риск возможного нанесения убытков в связи с гибелью или порчей имущества по причинам, не зависящим от субъектов). По общему правилу в этом случае убытки в связи с гибелью или порчей имущества несет собственник, однако, гражданское право предусматривает и другие варианты компенсации причиненного ущерба.

При рассмотрении в качестве субъекта, причинившего ущерб какое-либо природное или техногенное явление, под ущербом можно понимать невыгодные для собственника имущественные последствия, вызванные этими явлениями и которые могут быть компенсированы за счет средств третьей стороны (страхование рисков наступления события) или за счет собственных средств собственника информации.

Например, страхование представляет собой отношения по защите имущественных интересов физических и юридических лиц при наступлении определенных событий (страховых случаев) за счет денежных фондов, формируемых из уплачиваемых ими страховых взносов. Объектами страхования могут быть не противоречащие законодательству Российской Федерации имущественные интересы, связанные с возмещением страхователем причиненного им вреда личности или имуществу физического лица, а также вреда, причиненного юридическому лицу.

**Критерии классификации**

Угрозы можно классифицировать по нескольким критериям:

1. По аспекту ИБ (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;
2. По компонентам ИС, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
3. По способу осуществления (случайные/преднамеренные действия природного/техногенного характера);
4. По расположению источника угроз (внутри/вне рассматриваемой ИС).

В качестве основного критерия возьмём первый (по аспекту ИБ), привлекая при необходимости остальные.