1. **Основные виды угроз**

* Угрозы конфиденциальности – несанкционированный доступ к данным.
* Угрозы целостности – несанкционированное искажение или уничтожение данных.
* Угрозы доступности – ограничение или блокирование доступа к данным.
* Хакерская атака она может иметь конечную цель, быть т.н. целевой атакой, либо атака носит бессистемный характер, по принципу — атакую все подряд, что-нибудь да сломается.

1. **Характер происхождения угроз.**

**1)**Случайные или природные факторы

**2)**Умышленные факторы.

К первым факторам относятся:

* Несчастные случаи и стихийные бедствия. Они могут уничтожить всю информацию, которая хранится на твердых или/и электронных носителях.
* Ошибки в процессе обработки информации. Они могут привести к искажению достоверной информации.

К умышленным факторам относятся:

* Хищение носителей информации;
* Несанкционированный доступ;
* Копирование данных;
* Разглашение информации.

1. **Источники появления угроз.**

1 источник - люди:

* Посторонние лица;
* Пользователи;
* Персонал;

К 1 источнику относятся лица имеющие прямой или косвенный доступ к информации, которая хранится на носителях.

2 источник - технические устройства

3 источник – случайные реакции при реализации

* Отрешение и сбои аппаратурных устройств;
* Критичные ситуации из-за стихийных несчастий и отключений электрического питания;
* Упущении в работе обслуживающих сотрудников и других служащих;
* Огрехи в программном обеспечении

1. **Потенциально возможные злоумышленные действия.**

Осуществление угроз информационным ресурсам может быть произведено:

* через имеющиеся агентурные источники в органах государственного управления, коммерческих структур, имеющих доступ к конфиденциальной информации;
* -через подкуп лиц, работающих с основными документами;
* -путем перехвата информации в средствах и системах связи и хранения информации при несанкционированном доступе.

1. **Рекомендации повышения защищенности ИС**

* Делать бекап сайта как можно чаще
* Проверка сайта на наличие вирусов
* Использовать безопасный протокол https (или пользоваться внешними сервисами оплаты) при использовании на сайте функции оплаты
* Проводить анализ выполненных работ по защите сайта на наличие “Дыр” в системе