**ЗАДАНИЕ 2**

**Материалы для служебного пользования на твердых носителях и на электронных носителях на закрытом предприятии**

## 2.1. Виды угроз

## Угроза — это любое действие, направленное на нарушение конфиденциальности, целостности и доступности информации, а также нелегальное использование других ресурсов системы.

## хищение носителей информации (Кража злоумышленником оригинала документа из хранилища);

## несанкционированный доступ (Проникновение в систему и похищение электронных версий материалов при помощи компьютерных вирусов или хакерских атак);

## разглашение информации (Нарушение конфиденциальности данных материала сотрудником);

## - копирование данных (Как при помощи хакерских атак и взломов отдельно стоящих компьютеров/серверов, так и копирование бумажных носителей материалов).

## 2.2. Характер происхождения угроз

## По характеру воздействия: случайные или преднамеренные, действия природного характера.

## Случайные угрозы (Неумышленные). Для материалов, хранимых на бумажных носителях. случайной угрозой будет являться случайное уничтожение бумажных носителей, порча их водой или поджег. Для электронных – баг в системе, приводящий к стиранию данных.

Преднамеренные (Умышленные). Электронные носители (сервера или компьютеры) могут подвергнуться хакерской атаке со стороны злоумышленников. Также злоумышленники могут специально испортить электронный носитель информации. Твердые носители злоумышленники также могут уничтожить путем воды или поджога.

## 2.3. Классы каналов несанкционированного получения информации

## Под несанкционированным доступом понимается получение лицами в обход системы защиты с помощью программных, технических и других средств, а также в силу случайных обстоятельств доступа к обрабатываемой и хранимой на объекте информации.

## К первому классу относятся каналы от источника информации при несанкционированного доступа к нему.

## 1. Хищение носителей информации (Кража твердого носителя (бумаг) либо кража накопителя с информацией).

## 2. Копирование информации с носителей.

## 3. Выведывание информации обслуживающего персонала на объекте (сговори и нарушение конфиденциальности через сотрудников).

## 4. Фотографирование или видеосъемка носителей информации внутри помещения (материальных).

## Ко второму классу относятся каналы со средств обработки информации при несанкционированном доступа к ним.

## 1. Ввод программных продуктов, позволяющих злоумышленнику получать информацию (трояны, вирусы).

## 2. Копирование информации с технических устройств отображения (фотографирование с мониторов и др.).

## К третьему классу относятся каналы от источника информации без несанкционированного доступа

## 1. Использование технических средств оптико-электронной разведки (внешних телекамер, приборов ночного видения и т. д.). т

## 2. Осмотр отходов и мусора.

## 3. Выведывание информации у обслуживающего персонала за пределами объекта.

## К четвертому классу относятся каналы со средств обработки информации без несанкционированного доступа к ним.

## 1. Подключения к линиям связи.

## 2. Подключение к базам данных.

## 2.4. Источники появления угроз

## Источник угрозы — это непосредственный исполнитель угрозы в плане ее негативного воздействия на информацию угроз. Источниками могут быть: люди; технические устройства; модели, алгоритмы, программы; технологические схемы обработки; внешняя среда.

## Источники угроз бывают двух видов. Внешние и внутренние.

## Внешними угрозами для твердых и электронных материалов являются кража, похищение и уничтожение злоумышленниками из вне. Такие угрозы как часто имеют определённую цель и замысел.

## Внутренними угрозами являются случайные обстоятельства, приводящие к уничтожению носителей, также человеческий фактор, недостаточная разработка нормативно-правовой среды у организации и критическое состояние организации, способное привести к уничтожению материалов.

## 2.5. Виды угроз

Причин нарушения целостности информации на разных носителях может быть несколько:

– Личные интересы злоумышленника. Под этим пунктом даже сотрудник организации, наносящий вред целостности информации будет считаться злоумышленником.

– Случайные обстоятельства. Природные катаклизмы или нарушение правил безопасности, могут привести к утрате информации с электронных носителей и потери твёрдых.

– Плохой контроль хранения и неправильные условия могут привести к преждевременному старению информации (как в прямом смысле, так и в потере актуальности данных), преждевременным поломках, разрушения.

– Хранение информации на устаревшем языке или оборудовании. Примером такой причины может стать хранение электронной информации на устаревших устройствах ( дискеты и перфокарты, теряющие свой смысл в цифровом 21 веке), а также хранение информации путем записывания ее на старых языках программирования ( для твёрдых материалов причина тоже является актуальной, примером является латынь).