28.01.22

Сделать конспект и выучить

**1. Классификация путей утраты информации.**

### **Каналы утечки информации** (локальный уровень угроз компьютерной безопасности) - совокупность источников информации, материальных носителей или среды распространения несущих эту информацию сигналов и средств выделения информации из сигналов или носителей.

Каналы утечки информации подразделяются на:

* традиционные каналы утечки информации,
* каналы утечки информации непосредственно из средств компьютерной техники (СКТ).

**Традиционные каналы утечки информации**:

1. Контактное или бесконтактное подключение к электронным устройствам. Встроенные микрофоны, видео- и радиозакладки в стенах, мебели, предметах.
2. Съем акустической информации при помощи лазерных устройств с отражающих поверхностей.
3. Оптический дистанционный съем видеоинформации.
4. Применение узконаправленных микрофонов и диктофонов.
5. Утечки информации по цепям заземления, сетям громкоговорящей связи, охранно-пожарной сигнализации, линиям коммуникаций и сетям электропитания.
6. Высокочастотные каналы утечки информации в бытовой и иной технике.
7. Утечка за счет плохой звукоизоляции стен и перекрытий.
8. Исследование злоумышленником производственных и технологических отходов.
9. Утечка информации через телефонные и факсимильные аппараты.
10. Утечка информации через персонал - утечка акустических сигналов (речевая информация) и электромагнитных сигналов (в т.ч. оптического диапазона),
11. Утечка информации с носителей (либо с носителями).

**2.. Форс-мажорные обстоятельства.**

Бесперебойное функционирование современных организаций во многом зависит от надежной работы вычислительных комплексов, являющихся их «мозгом» и «нервной системой». Поэтому защите этих комплексов в чрезвычайных ситуациях: при пожарах, наводнениях, актах терроризма, и саботажа должно быть уделено особое внимание.

**Большие организации** имеются **специальные планы защиты** информационно-вычислительных систем (ИВС) и быстрого восстановления их работоспособности. В этих планах предусматривается, в частности, использование дублирующих комплексов из «горячего резерва», снабженных необходимым обеспечением и персоналом..

**Малые организации** не могут себе позволить такие планы и специальную службу. Но им также необходимо проводить анализ возможных последствий чрезвычайных происшествий: выявлять наиболее уязвимые места в информационно-вычислительных системах (ИВС), оценивать максимальные и минимальные сроки ликвидации последствий и необходимые для этого ресурсы, разрабатывать варианты планов, охватывающие наиболее опасные и вероятные из возможных чрезвычайных ситуаций.

Иногда в качестве панацеи от потерь вследствие ЧП называют страхование. Несомненно, оно сможет покрыть потери от большинства чрезвычайных ситуаций, однако нередко действительная стоимость потерь в несколько раз превышает размеры страхового возмещения, поскольку включает в себя непредвиденные административные расходы, затраты на проведение оценки потерь, потери позиции на рынках и другие деловые и коммерческие потери вследствие недостаточного (по объему и качеству) обслуживания, а также неполучение ожидаемых доходов. Таким образом, одного страхования недостаточно. Необходим целый комплекс мероприятий.

**1.2.2. Защита от форс-мажорных обстоятельств.**

**Основные этапы разработки плана защиты ИВС:**

1. **Анализ проблемы обеспечения работоспособности системы при ЧС**. Цель - выявление и оценка опасности возможных ЧС.

* + **Определение факторов воздействия на ИВС** (на практике весьма трудно оценить воздействие всех факторов и событий, да в этом и нет необходимости) и их классификацию: природные (наводнения и ураганы), и «человеческие», которые, в свою очередь, могут быть преднамеренными (взрывы, поджоги т.п.), случайными (протечки воды) и косвенными (выход из строя энергосистемы или системы телекоммуникации).
  + **Определение особенностей воздействия на ИВС** различных факторов ЧС, а также их последствия: невозможность доступа к ИВС, выход из строя компьютера и системы телекоммуникации, потерю баз данных и информационных массивов, а также «вывод из строя» обслуживающего персонала.

**2. Выработка мер по минимизации степени воздействия факторов ЧС.**

* **Взрывы** (повреждения от осколков стекол разбитых окон или внутренних стеклянных перегородок). Меры защиты – специально оборудованные взрывобезопасные помещения
* **Пожары** (повреждения от дыма, воды и химических смесей противопожарных средств. Меры защиты – как закрытие оборудования покрывалами, уборка дисков в запираемые хранилища.
* **Наличие планов защиты от вирусов**.
* **Дублирование файлов данных**. Файлы-копии хранятся отдельно от файлов данных.
* **Возможность использования других ИВС**.
* **Наличие правил работы персонала**, например принцип «чистого стола» (в конце рабочего дня все документы, дискеты и т.п. должны убираться в запираемые хранилища или сейфы).

Разработанные специальные планы по защите ИВС и обеспечению непрерывной работы организации в случае ЧС должны быть тщательно документированы, переданы для исполнения соответствующему персоналу. Их следует регулярно обновлять. Несколько копий таких планов должно храниться вне пределов помещений, в которых расположена ИВС.

Хорошо спланированная и отлаженная система защиты ИВС является залогом того, что вредные последствия от различных инцидентов будут минимизированы.