Лекция 14. Методы и средства защиты информации, обрабатываемой в АС, от технических разведок

1. Угрозы БИ в АС.
2. Меры противодействия угрозам БИ в АС.
3. Основные принципы построения систем ЗИ в АС.

1.Угрозы безопасности информации в АС.

1. **Угрозы природного воздействия на информацию:**

сбои и отказы технических средств (СВТ, сист. энергоснабжения, грозы, пожар, наводнение, э.м. несовместимость и т.д.).

2. Угрозы искусственного воздействия на информацию (участие человека).

а) неумышленные (ошибки человека):

- проектирования ПО;
- настройки средств ЗИ;

б) умышленные:

- НСД (результат: утрата (разрушение, уничтожение), утечка (извлечение, копирование), искажение (модификация, подделка) или блокирование, кража, .

Возможную совокупность и результаты реализации всех видов угроз нанесения ущерба для конкретной АС определить заранее трудно. Поэтому ***модель потенциальных угроз*** *нанесения ущерба АС и обрабатываемой информации должна создаваться совместно владельцем АС и специалистами по ЗИ на этапах разработки и создания АС и уточняться в ходе ее*

Меры по ЗИ от НСД:

- охрана и ограничение доступа посторонних лиц к ЭВМ и хранилищам носителей данных;
- создание барьеров безопасности путем оборудования помещений обычными, кодовыми и электронными замками, решетками, системами внутреннего телевидения и тревожной сигнализации;
- ограждение зданий и территорий заборами с электронными системами контроля проникновения;
- создание резервных вычислительных ресурсов и хранилищ носителей данных и т.п.

3. Угрозы информации в результате использования специальных средств, не входящих в состав АС.

- утечка за счет перехвата ПЭМИ, создаваемых СВТ АС в диапазоне частот от единиц Гц до 2,7 ГГц . Дальность распространения десятки – тысячи метров (дисплеи, проводные линии связи, накопители НМД и буквопечатающие аппараты последовательного типа).
- утечка за счет приема информационных сигналов, наведенных в цепях электропитания и заземления аппаратных средств АС, выходящих за пределы охраняемой (контролируемой) зоны - зоны безопасности.

2. Меры противодействия угрозам безопасности информации в АС.

- ✔ Потенциальный злоумышленник лицо социальное…
- ✔ Сложность управляющего органа должна быть не ниже сложности органа управления (закон Эшби).

Правовое обеспечение защиты информации в АС

- Первый уровень : законы о БИ, обеспечивают формирование и проведение политики в этой области.
- Второй уровень : президентские и правительственные акты, обес-печивают реализацию законодательства в области БИ.
- Третий уровень: различные стандарты, руководящие документы, нормы и классификаторы (классификаторы АС по степени секрет-ности обрабатываемой информации, …..).
- Четвертый уровень: комплект локальных норм, положений, инст-рукций, методических рекомендаций и других РД по комплексной защите информации в АС данной организации.

Б. **Организационные методы и средства защиты**

Организационно-технические мероприятия, осуществляются в процессе создания и эксплуатации АС с целью обеспечения ЗИ:

Охватывают элементы АС и системы ЗИ на всех этапах их жизненного цикла: строительство помещений, проектирование системы, монтаж и наладка обору-дования, испытания и проверка в эксплуатации АС. Позволяют полностью или частично перекрыть значительную часть каналов утечки информации, обеспечи-вают объединение подсистемы защиты в целостную систему защиты.

Основываются на законодательных и нормативных документах по БИ, охватывают основные пути сохранения информационных ресурсов, включают:

А) ограничение физического доступа к объектам АС и реализацию режимных мер ;

Б) ограничение возможности перехвата информации вследствие существова-ния физических полей;

В) ограничение доступа к информационным ресурсам и другим элементам АС путем установления правил разграничения доступа, криптографическое зак-рытие каналов передачи данных, выявление и уничтожение "закладок";

Г) создание твердых копий важных с точки зрения утраты массивов

В) Технические меры

Современная система ЗИ ориентирована на широкое применения ТСЗИ:

- **Криптографические** средства защиты (ЗИ в ЛС, выходящих за пределы контр. зоны, защита во внешних носителях информации,…).
- **ЗИ от НСД**.
- **Генераторы зашумления** (ЗИ от утечки по ПЭМИН).
- **Инженерно-технические** (физические) средства защиты (физические объ-екты, механические, электрические и электронные устройства, элементы конструкции зданий, средства пожаротушения и целый ряд других сре-дств, обеспечивающих выполнение следующих задач: защита территории и помещений вычислительного центра или центра автоматизированной системы электронной обработки данных (АС) от проникновения злоумы-шленников; защита аппаратуры и носителей информации от поврежде-ния или хищения; предотвращение возможности наблюдения за работой персонала и функционированием оборудования из-за пределов терри-тории или через окна; предотвращение возможности перехвата электро-магнитных излучений работающего оборудования и линий передачи дан-ных; контроль за режимом работы персонала; организация доступа в помещения ВЦ сотрудников; контроль за перемещением в различных рабочих зонах; противопожарная защита помещений ВЦ; минимизация материального ущерба и потерь информации, которые могут возникнуть в результате стихийного бедствия.

3.Основные принципы построения систем ЗИ в АС.

Весь период работ по защите информации в АС делится на три этапа, каж-дый из них характеризуется своими особенностями в принципиальных подходах к защите информации.

Первый этап : (упрощенный) подход: сам факт представления инфор-мации в ЭВМ в закодированном виде и обработкой ее по специфическим алгоритмам уже является серьезным защитным средством, а потому впол-не достаточно включить в состав АС некоторые технические и программные средства и осуществить ряд организационных мероприятий, и этого будет достаточно для обеспечения защиты информации.

Второй этап: специалисты пришли к выводу о том, что для защиты ин-формации требуется некоторая вполне организованная система с своим управляющим элементом. Такой элемент получил название ядро защиты или ядро безопасности. Существенно повысилось внимание к организаци-онным мероприятиям.

Третий этап: Защиты информации в современных АС есть не одноразовая акция, а непрерывный процесс, целенаправленно осуществляемый во все время создания и функционирования систем с комплексным применением всех имеющихся средств, методов и мероприятий.

На основе сказанного, теоретических исследований и практических работ в области защиты ин-формации сформулирован так называемый системно-концептуальный подход к защите информации в АС.

Под системностью как составной частью системно-концептуального подхода понимается:

во-первых, системность целевая, т.е. защищенность информации рас-сматривается как составная часть общего понятия качества информации;

во-вторых, системность пространственная, предполагающая взаимо-увязанное решение всех вопросов защиты во всех компонентах отдельно взятой АС, во всех АС учреждение (заведения, ведомства), расположен-ных на некоторой территории;

в-третьих, системность временная, означающая непрерывность работ по защите информации, осуществляемых по взаимоувязанным планам;

в-четвертых, системность организационная, означающая единство организации всех работ по защите информации и управления их осуще-ствлением. Она предопределяет объективную необходимость создания в общегосударственном масштабе стройной системы органов, профес-сионально ориентированных на защиту информации, несущих полную ответственность за оптимальную организацию надежной защиты инфор-мации во всех АС и обладающей для этого необходимыми полномочи-ями. Главной целью указанной системы органов должна быть реализа-ция в общегосударственном масштабе принципов системно-концептуаль-ного подхода к защите информации как государственного, так и коммер-ческого характера.

Принципы ЗИ в АС:

- системность (представление как единое целое);
- комплексность (учитывать разнообразие и множественность угроз);
- непрерывность защиты;
- разумная достаточность;
- гибкость управления и применения;
- открытость алгоритмов и механизмов защиты;
- простота применения защитных мер и средств.