Методы и средства защиты компьютерной информации

Информация – сведения независимо от формы их представления.

Информация – мера устранения неопределенности.

Информация – система идеальных (субъективных) образов объектов, процессов и явлений окружающего мира в сознании человека, а так же множество признаков, присущих материи и формирующих идеальные образы.

Информационная безопасность (ИБ) – *состояние защищенности* основных интересов личности, общества и государства в информационном пространстве, учитывая информационно-телекоммуникационную структуру и собственно информацию.

Объект информатизации – совокупность ***информационных ресурсов, средств и систем обработки информации***, используемых в соответствии с заданной информационной технологией, ***средств обеспечения*** объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или ***помещения*** и ***объекты***, предназначенные для ведения конфиденциальных переговоров.

Автоматизированная система (АС) – система, состоящая из ***данных***, ***алгоритма*** обработки данных, ***средства вычислительной техники*** и ***персонала***

Информация

Общедоступная	Ограниченного доступа
Свободное распространение Подлежит распространению или предоставлению в соответствии с ФЗ РФ	Предоставляется по согласованию лиц, участвующих в соответствующих отношениях Распространение ограниченно или хапрещено

Свойства защищаемой информации

1. Конфиденциальность
2. Целостность
3. Доступность

Угроза ИБ – потенциально существующая *возможность* какого-либо воздействия на вычислительную систему или обрабатываемую информацию, в результате которой может быть нарушена информационная безопасность.

Классификация угроз ИБ

1. По природе возникновения
   - Естественные
   - Исскуственные

2. По степени преднамеренности
   - Случайные
   - Преднамеренные

3. По положению источника угроз
   - Внешние
   - Внутренние

4. По степени воздействия на АС
   - Пассивные
   - Активные

5. По способу доступа к ресурсам АС
   - Санкционированный доступ
   - Несанкционированный доступ

Факторы, воздействующие на защищаемую информацию

Факторы – явления, действия или процессы, результатом которых могут быть утечка, искажение, уничтожение защищаемой информации либо блокировка доступа к ней.

Факторы, воздействующие на защищаемую информацию

По отношению к природе воздействия
- объективные
- субъективные

По отношению к объекту воздействия
- внешние
-внутрение

Внутренние объективные факторы

- Передача сигналов по проводам, линиям связи, по оптоволоконным линиям связи и т.д.
- Излучение сигналов, функционально присущих техническим средствам обработки информации
- ПЭМИН элементов технических средств, обработки информации
- Наличие акустоэлектрических преобразователей в элементах ТС ОИ
- Дефекты, сбои, отказы, аварии ТС, либо ПО

Внутренние субъективные факторы

- Разглашение защищаемой информации лицами, имеющими доступ
- Неправомерные действия со стороны лиц, имеющих права на информацию
- Недостатки в организации защиты информации
- Ошибки обслуживающего персонала при обработки информации

Внешние объективные факторы

- Явление техногенного характера
- Природные явления, стихийные бедствия

Внешние субъективные факторы

- Доступ к защищаемой информации с использованием технических средств разведки
- НСД к защищаемой информации:
- Блокирование доступа к защищаемой информации путем перегрузки ТС обработки информации ложными заявками на ее обработку
- Действия криминальных групп или отдельных субъектов
- Искажение, уничтожение либо блокирование информации с применением технических средств

Принципы обеспечения ИБ

1. Невозможность создания идеальной системы защиты (СЗ)
2. Принцип неопределенности
3. Принцип минимального риска
4. Принцип минимального ущерба
5. Принцип минимального времени
6. Принцип защиты от всех
7. Принцип законности
8. Принцип персональной ответственности
9. Принцип разграничения полномочий
10. Принцип взаимодействия и сотрудничества

Принципы обеспечения ИБ

11. Принцип комплексности и индивидуальности
12. Принцип последовательных рубежей безопасности
13. Принцип равноправности и равномощности рубежей защиты
14. Принцип адекватность и эффективность
15. Принцип адаптивности
16. Принцип экономичности
17. Принцип эффективности контроля
18. Принцип регистрации действий
19. Принцип защиты средств обеспечения защиты

Принципы построения систем защиты АС

- системности;
- комплексности;
- непрерывности защиты;
- разумной достаточности;
- гибкости управления и применения;
- простоты применения защитных мер и средств.

Порядок обеспечения ЗИ объекта информатизации

1. Разработка модели угроз
2. Оценка рисков и принятие решений по управлению рисками
3. Разработка модели нарушителя
4. Разработка и внедрение предложений по защите
5. Практическая проверка, оценка адекватности СЗ модели угроз
6. Коррекция средств защиты, модели угроз, рисков

Модель угроз – формализованное описание возможных угроз информации, сведения о методах и средствах осуществления угроз информации.

Риск – вероятность реализации того или иного вида угроз. При реализации СЗ необходимо стремится минимизировать риски защищаемой системы.

Меры противодействия угрозам безопасности

- правовые (законодательные),
- морально-этические,
- организационные (административные),
- физические,
- технические (аппаратурные, программные или программно-аппаратные).