АРМ – автоматизированное рабочее место.

**Этапы обеспечения режима информационной безопасности**

По ФСТЕК:

**Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующей информационную технологию выполнения заданных действий.

1. Определение политики безопасности
2. Определение сферы системы управления информационной безопасности и конкретизация целей ее создания
3. Оценка рисков
4. Выбор контрмер обеспечивающих режим ИБ
5. Управление рисками
6. Аудит системы управления информационной безопасности

**Определение политики безопасности**

Практические шаги по определению политики безопасности:

1. Выбор национальных и международных руководящих документов и стандартов в области информационной безопасности и определение на их основе основных требований и положений политики ИБ компании, включая:
   1. Общедоступную информацию
   2. Информацию в ограниченном доступе
      1. Государственная тайна
      2. Коммерческая тайна
      3. Персональные данные
      4. Остальные виды тайн (банковская, расследования, врачебная)
2. Управление доступом к СВТ, программам и данным
3. Вопросы резервного копирования
4. Проведение ремонтных и восстановительных работ
5. Информирование об инцидентах в области ИБ
6. Определение подходов к управлению информационными рисками

Уровень защищенности может быть:

1. Минимальный (базовый)
2. Повышенный
3. Структуризация контрмер по следующим основным принципам
   1. Нормативно-правовому
   2. Организационно-управленческому
   3. Технологическому
   4. Аппаратно-программному
4. Определение порядка сертификации и аккредитации ИС на соответствие стандартам в области ИБ

План описания

1. Структура организации
   1. Описание существующей структуры
   2. Изменений, которые планируется выполнить в организации

Контролируемая зона – пространство, в котором исключено неконтролируемое пребывание оператора и любых его посетителей.

1. Ресурсы информационной системы, подлежащие защите
   1. СВТ
   2. Данные
   3. Системное и прикладное ПО

Ресурсы по ФСТЕК – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

1. Размещение средств СВТ и поддерживающей инфраструктуры

Эксперты:

1. Специалисты ИБ
2. Персонал, работающих с данной информацией
3. Администраторы систем, поддерживающие обработку данной информации

4 этап – управление рисками:

1. Уменьшение риска
2. Уклонение от риска
3. Изменение характера риска

5 этап - выбор контрмер:

Выполняется комплекс мер структурированный по организационно-управленческому, технологическому и аппаратно-программному уровням.

6 этап – аудит:

Проверяется соответствие выбранных контрмер целям и задачам бизнеса.

**Структура политики информационной безопасности и процесс её разработки**

Политика ИБ – комплекс документов, отражающих все основные требования к обеспечению защиты информации и направления работы предприятия в этой сфере. При построении политики безопасности можно выделить 3 основных уровня:

1. Верхний
2. Средний
3. Нижний

Верхний уровень служит для:

1. Формулирования и демонстрации отношения руководства предприятия к вопросам

Общий цикл политики ИБ

1. Проведение предварительного исследования состояния ИБ
2. Собственная разработка политики безопасности
3. Внедрение разработанных политик безопасности