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

Настоящий РД устанавливает классификацию АС, подлежащий к защите от НСД и требования к защите АС различных классов.

Основные этапы классификации АС:

1. Разработка и анализ исходных данных
2. Выявление признаков АС для классификации
3. Сравнение выявленных признаков АС с классифицируемыми
4. Присвоение АС соответствующего класса защиты информации от НСД

Базируется на:

1. Перечень лиц имеющих доступ к штатным средствам АС с указанием их уровня полномочий.
2. Перечень лиц, имеющих доступ к средствам АС с указанием из уровня полномочий.
3. Матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС.
4. Режим обработки данных в АС:
   1. Коллективный
   2. Индивидуальный

К числу определяющих признаков по которым производится группировка АС относится:

1. Наличие в АС информации различного уровня конфиденциальности
2. Уровень полномочий субъектов доступа АС на доступ к КИ
3. Режим обработки данных в АС

Устанавливается 9 классов защищенности АС, которые подразделяются на 3 группы (в пределах группы соблюдается иерархия требований по защите в зависимости от ценности информации):

1. АС в которых работает 1 пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности.
2. АС в которых пользователи, имеющие одинаковые права доступа ко всей информации АС на носителях разных уровней конфиденциальности.
3. Многопользовательские АС в которых обрабатывается и хранится информация разных уровней. Не все пользователи имеют права доступа ко всей информации АС.

Определение критериев приемки новых информационных систем, модернизированных/новых версий. Должны быть выполнены подходящие испытания системы в ходе разработки и до приёмки.

1. Реализация средств управления обнаружением, предотвращение и восстановлением защиты против злонамеренного кода, а так же процедуры ознакомления соответствующих пользователей.
   1. Создание официальной политики, запрещающей использование не разрешенного программного обеспечения;
   2. Создание официальной политики для защиты от рисков, связанных с получением файлов и ПО из внешних сетей или же любом другом носителе
2. Проведение регулярного анализа ПО и содержание данных систем, относящихся к критическим деловым процессам.
3. Создание четко определенной политики в отношении мобильного кода
4. Резервное копирование
   1. Реализация выполнения резервного копирования в соответствии с политикой резервирования
   2. Резервный копирование необходимого уровня

Процедуры для использования беспроводных средств связи.

1. Использование криптографических методов защиты
2. Сохранение и ликвидация всей деловой корреспонденции
3. Не оставлять уязвимую или критическую на средствах печати
4. Защита передаваемой информации, которая имеет форму приложения
5. Процедура уведомления отправителя о передаче, отправке и получении
6. Процедура для обеспечения прослеживаемости и неотрекаемости

Услуги электронной торговли

1. Степень уверенности
2. Определение и выполнение требований конфиденциальности
3. Исключение потери или дублирование информации о сделке

**Удаленный доступ**

Должна включать в себя требования:

1. Физической защите
2. Методам шифрования
3. Резервному копированию
4. Защите от вирусов

также включать правила и советы по подключению мобильных средств к сети. И руководящие указания по использованию этих средств в общедоступных местах.

При удаленном доступе следует обратить внимание на следующее:

1. Физическая защита места удаленного доступа
2. Требования защиты связи при удаленном доступе к внутренним системам организации
3. Уязвимость информации к которой будет осуществляться доступ
4. Уязвимость внутренней системы
5. Угроза неразрешенного доступа к ресурсам других лиц (семья, друзья)
6. Использование домашних сетей и требования или ограничения использования на конфигурацию услуг беспроводной сети
7. Требования к брандмауэру

Определение угроз безопасности, нарушение которых может привести к ошибкам: