Программно-технические меры обеспечения ИБ

- ▶ Под программно-техническими мерами понимается совокупность информационных систем и технологий направленных на обеспечение задач по защите информации.
- ▶ Данные меры позволяют автоматизировать многие задачи по обеспечению информационной безопасности

Программно-технические меры

- ▶ При рассмотрении информационной системы на начальном уровне детализации она может быть рассмотрена как совокупность информационных сервисов, обеспечивающих выполнение основных функциональных задач ИС.
- ▶ К числу сервисов безопасности можно отнести:
 - Идентификация и аутентификация
 - Управление доступом
 - Протоколирование и аудит
 - Шифрование
 - Контроль целостности
 - Экранирование
 - Анализ защищенности
 - Обеспечение отказоустойчивости
 - Обеспечение безопасного восстановления

Программно-технические меры

- ▶ Классификация мер безопасности на основе сервисов безопасности и их места в общей архитектуре ИС:
 - Превентивные
 - Меры обнаружения нарушений
 - Локализирующие зону воздействия
 - Меры по выявлению нарушений
 - Меры восстановления режима безопасности

Особенности современных ИС

- ▶ С точки зрения информационной безопасности наиболее существенными являются следующие аспекты:
 - Корпоративная сеть является распределенной, связи между отдельными частями обеспечиваются внешними провайдерами
 - Корпоративная сеть имеет одно или несколько подключений к Internet
 - Критически важные серверы могут располагаться на различных площадках
 - Для доступа пользователей используются как компьютеры так и другие мобильные устройства
 - В течение одного сеанса работы пользователь обращается к нескольким информационным сервисам
 - Требования доступности информационных сервисов выдвигаются достаточно жесткие
 - Информационная система представляет собой сеть с активными агентами, в процессе работы программные модули передаются с сервера на компьютеры пользователя и т.п.
 - Не все пользовательские системы контролируются администраторами ИС
 - Программное обеспечение и модули полученные по сети не могут рассматриваться как надежные
 - Конфигурация ИС постоянно изменяется на уровнях администрирования данных, программ, аппаратуры