ТЕМА 7.

Основы защиты информации

1. Основные понятия и определения
2. Виды угроз безопасности информации
3. Обеспечение информационной безопасности
4. Базовые технологии защиты информации
5. Технологии защиты от вирусов

1. Основные понятия и определения

Информационная безопасность – защищенность информации от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб субъектам информационных отношений (владельцам и пользователям информации)

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Угроза – это потенциальная возможность нарушить информационную безопасность
Попытка реализации угрозы называется атакой

Составляющие информационной безопасности

Доступность – это возможность за приемлемое время получить требуемую информационную услугу

Информационная безопасность — это процесс обеспечения конфиденциальности, целостности и доступности информации

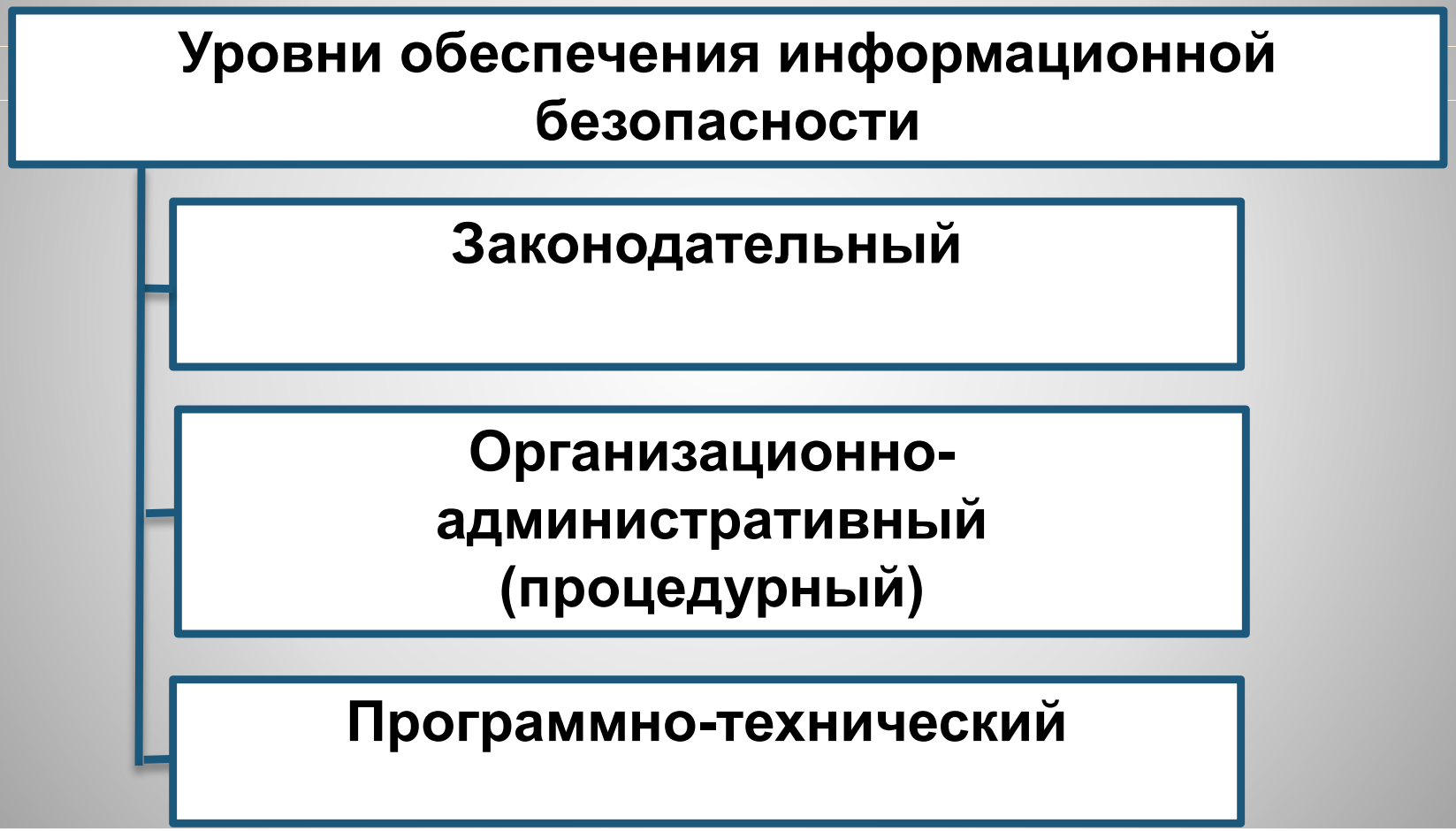
Конфиденциальность – это защита от несанкционированного доступа к информации. Конфиденциальную информацию можно разделить на предметную и служебную.

2. Виды угроз безопасности информации

УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ (по способу осуществления)

Случайные угрозы:	Преднамеренные угрозы:
Непреднамеренные ошибки обслуживающего персонала и пользователей (до 65% потерь)	Кражи и подлоги, шпионаж и диверсии
Стихийные бедствия и аварии (до 13% потерь)	Несанкционированный доступ к информации и аппаратуре
Сбои и отказы аппаратного и программного обеспечения	Вредоносные программы

3. Обеспечение информационной безопасности



Законодательный уровень

Меры законодательного уровня

Направленные на создание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности

Способствующие повышению образованности общества в области информационной безопасности

Закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации"

Система ГАРАНТ:
http://base.garant.ru/12148555/#ixzz3b4oxaDQ9

Статья 16. Защита информации
Статья 17. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации

Преступления в сфере компьютерной информации

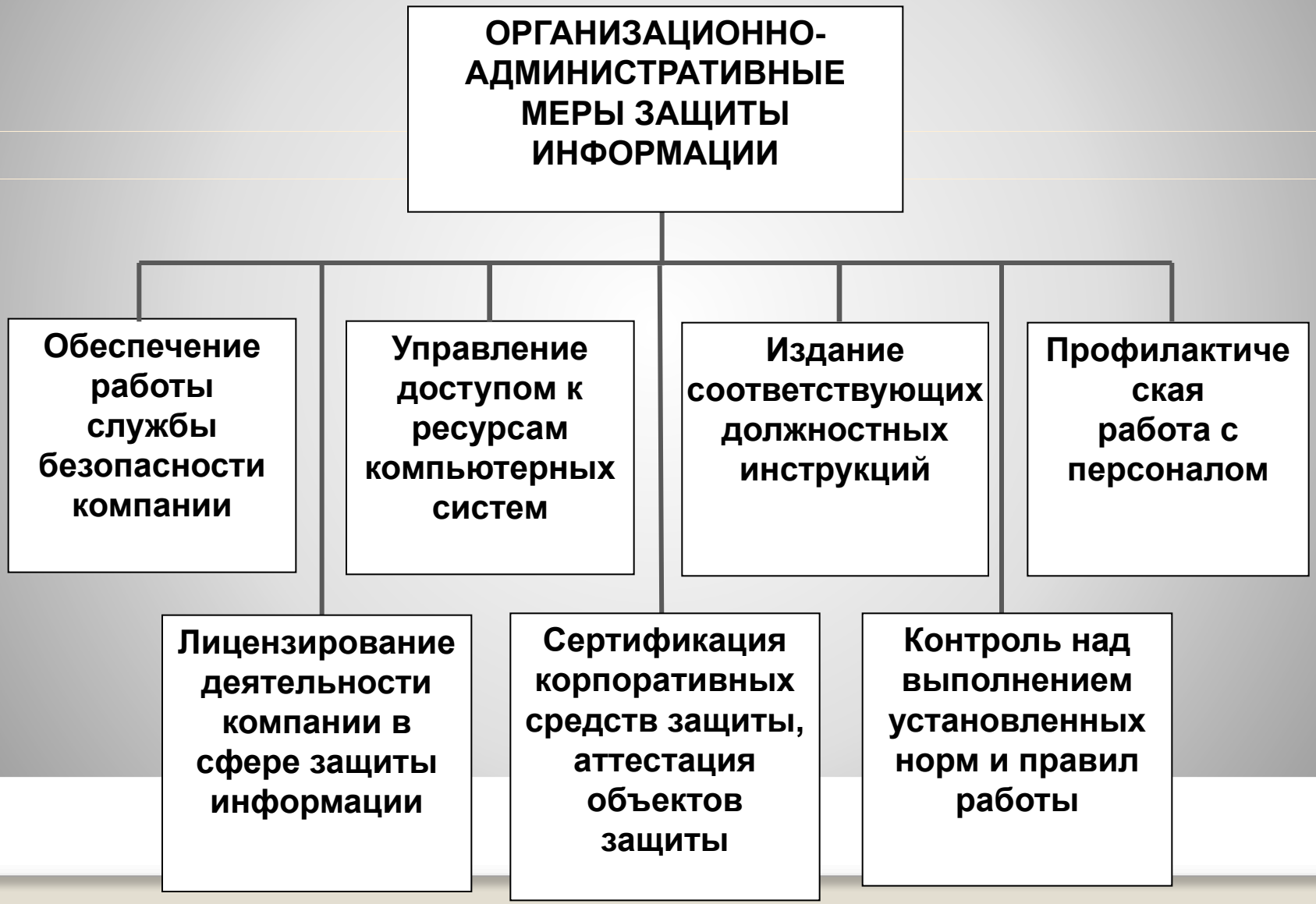
Уголовный кодекс РФ
(с 1 января 1997 года):

ст. 272. Неправомерный доступ к компьютерной информации (срок до 5-ти лет).

ст. 273. Создание, использование и распространение вредоносных программ для ЭВМ (срок до 7-ми лет).

ст. 274. Нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети (срок до 4-х лет).

Организационно-административный уровень

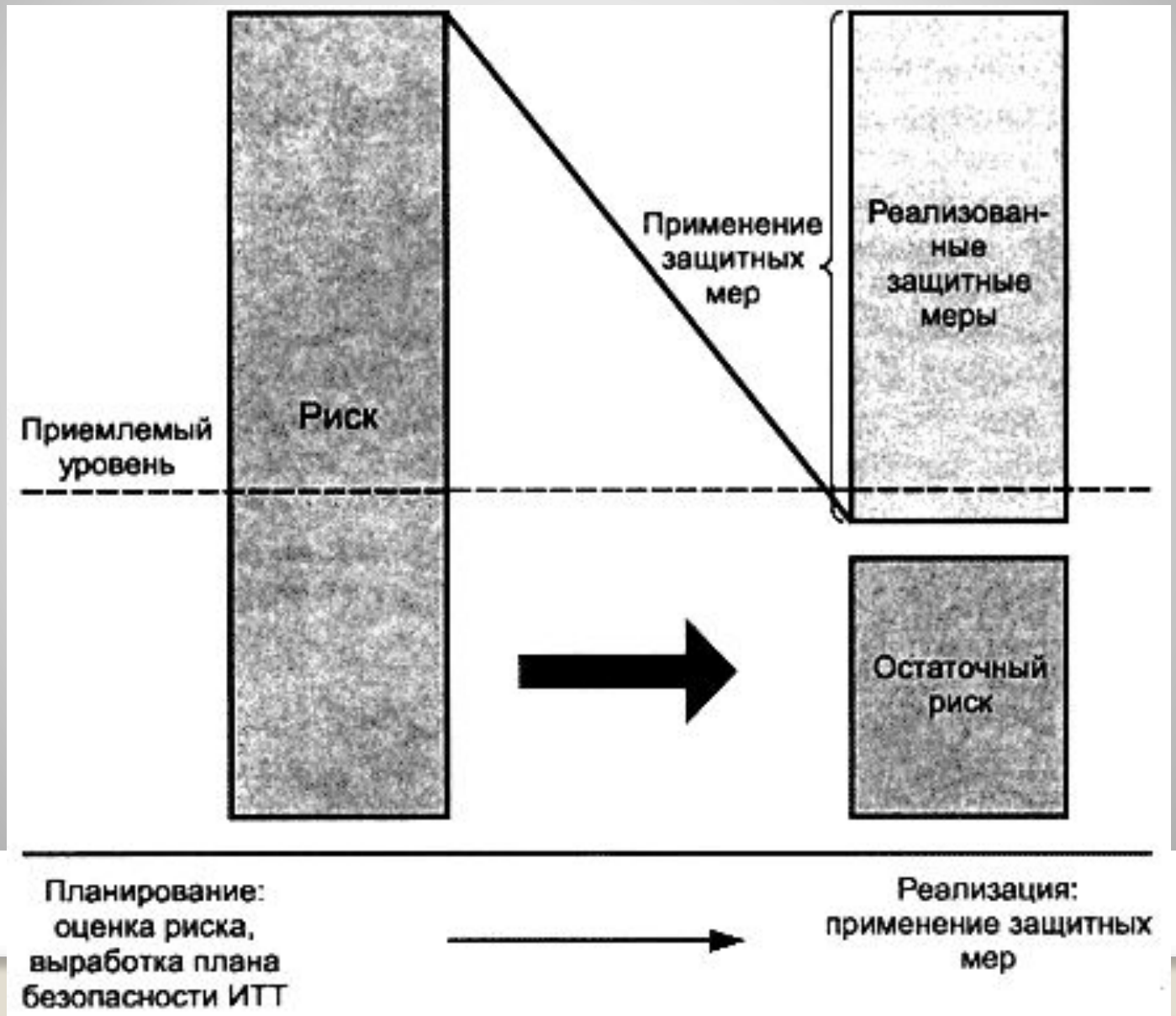


Программно-технические меры безопасности

Виды программно-технических мер информационной безопасности:

- **Превентивные, препятствующие нарушениям**
- **Меры обнаружения нарушений**
- **Локализующие, сужающие зону воздействия нарушений**
- **Меры по выявлению нарушителя**
- **Меры восстановления режима безопасности**

Взаимосвязь защитных мер и рисков, связанных с различными угрозами



4. Базовые технологии защиты информации

Аутентификация – это процедура доказательства

Авторизация – это процедура наделения легального пользователя системы правами выполнять определенные действия над ресурсами системы

Ау связанных с доступом к защищаемым ресурсам

Шифрование информационных данных – способ преобразования открытой информации в закрытую, и обратно (симметричное и асимметричное шифрование)

Межсетевое экранирование (Brandmauer, Firewall) – комплекс аппаратных или программных средств, ос

Тунеллирование – в комбинации с шифрованием и экранированием используется для реализации виртуальных частных сетей (VPN)

Признак классификации	Класс вирусов
По среде обитания	• загрузочные • файловые • файлово-загрузрчные • сетевые • системные
По степени воздействия	• безвредные • неопасные • опасные • разрушительные
По способам заражения среды обитания	• резидентные • нерезидентные
По алгоритмической особенности построения	• репликаторные • «троянский конь» • логическая бомба • мутанты • невидимки • макровирусы

5. Технологии защиты от вирусов

Методы и средства защиты от компьютерных вирусов:

- **общие методы и средства защиты информации**
- **специализированные программы для защиты от вирусов**
- **профилактические меры, позволяющие уменьшить вероятность заражения вирусами**

Антивирусные программы

Виды антивирусных программ:

- **программы-фаги (антивирусные сканеры)**
- **программы-ревизоры**
- **программы-блокировщики**
- **программы-иммунизаторы**