

# Учебный курс

## Информационная безопасность в инфокоммуникационных системах

**Раздел 1.** Введение в информационную безопасность.  
Организация работы администратора безопасности  
компьютерной сети.

# Информационная безопасность

Информационная безопасность – это бесперебойное предоставление доступа к информации уполномоченным потребителям.

# Работа администратора безопасности

- Представление
- Планирование
- Разработка
- Внедрение
- Переоценка

# Обзор общих принципов проектирования

- Принципы успешного проектирования
- Команда проекта
- Основы управления рисками
- Документирование



# Принципы успешного проектирования

## Успешный проект:

- Отвечает деловым потребностям организации
- Представляет четкий план достижения цели вовремя, в рамках бюджета и с заранее оговоренными функциональными возможностями

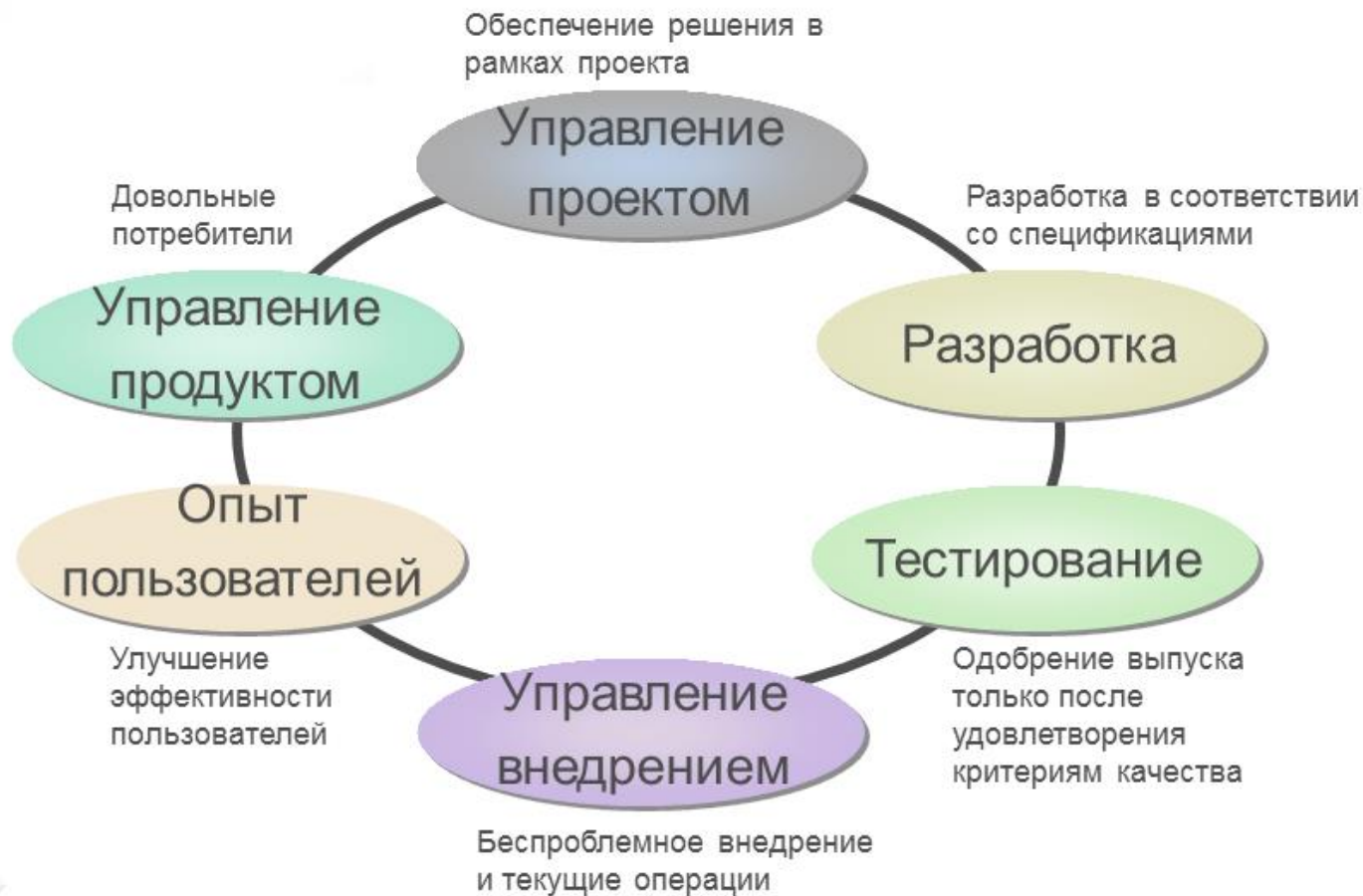
Есть несколько проверенных моделей проектирования

Основные задачи проектирования выполняются в фазах представления и планирования





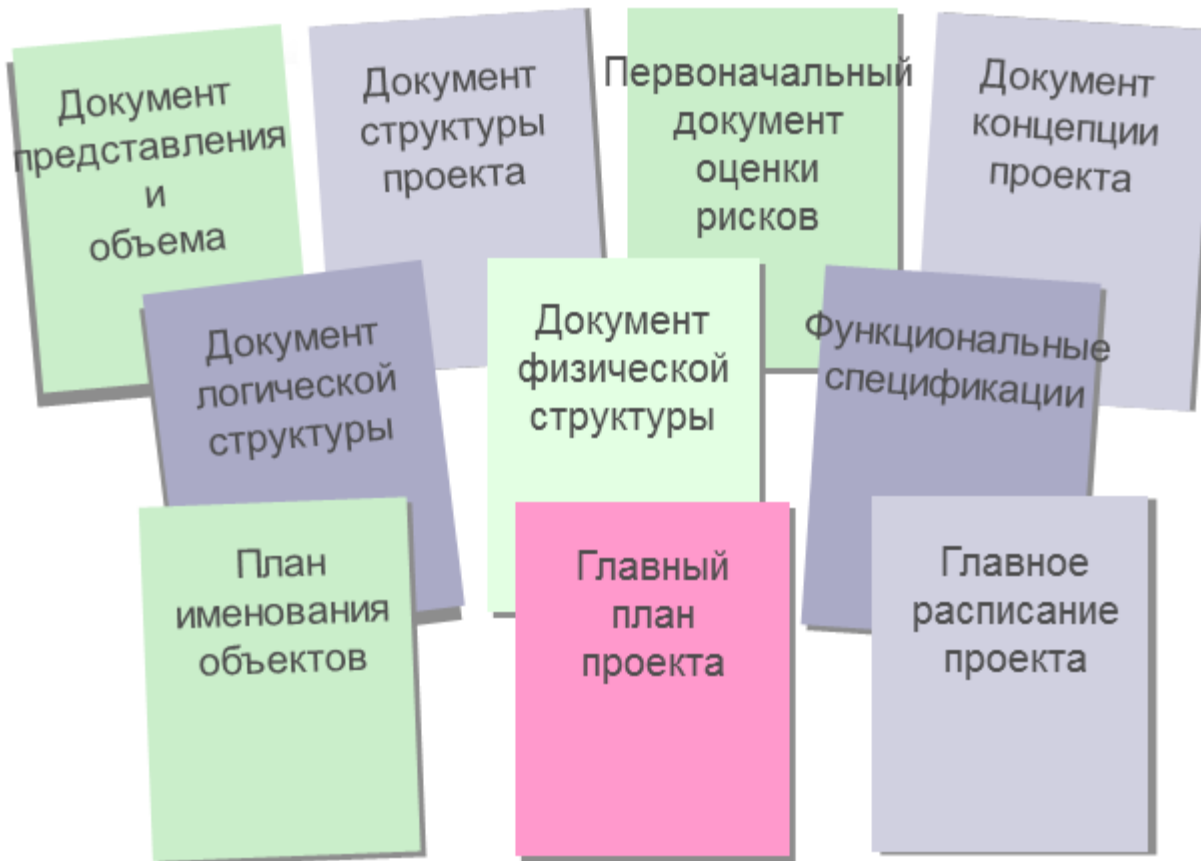
# Команда проекта



# Основы управления рисками



# Документирование







# Защита сети, серверов и сетевых сервисов

Внутренняя защита сети

Внешняя защита сети

A close-up photograph of a hand holding a golden key, positioned on the left side of the slide. The hand is holding the key by its handle, and the key is pointing towards the right. The background of the slide is a dark blue gradient.

# Внутренняя защита сети

- Разработайте действенную политику безопасности
- Ограничьте доступ к вашим серверам
- Ограничьте доступ к сетевым устройствам
- Защитите серверную файловую систему
- Защитите систему сетевой печати
- Ограничьте пользовательский доступ к сети
- Ограничьте административный доступ к сети
- Защитите серверы и рабочие станции от вирусов

# Что такое политика безопасности

Политика безопасности – это документ (комплект документов), который описывает условия, правила, процедуры и методы проверки безопасности, применяемые в компании, и составляет основу для обеспечения безопасной и защищенной среды.



## Как начать разрабатывать политику безопасности

- Узнайте, что у вас есть
- Выясните, что нужно защищать
- Оцените то, что нужно защищать
- Каковы возможные угрозы
- Оцените вероятность осуществления (проявления) угрозы
- Отранжируйте угрозы
- Возможные способы защиты от наиболее вероятных угроз
- Оцените способы защиты
- Примите экономически обоснованные меры, которые защитят ваши ценности
- Постоянно пересматривайте процесс и улучшайте его по мере обнаружения слабых мест и появления новых угроз

## Основные вопросы, рассматриваемые в политике безопасности

- Кому разрешено использовать ресурс?
- Как правильно использовать ресурс?
- Кто уполномочен предоставлять доступ и подтверждать использование?
- Кто может иметь административные полномочия?
- Каковы права пользователей и их ответственность?
- Чем отличаются права и ответственность администратора и пользователей?
- Что делать с конфиденциальной информацией?

# Эталонная модель МОС/ВОС

## Уровни

**7** Приложения

**6** Представления

**5** Сеансовый

**4** Транспортный

**3** Сетевой

**2** Канальный

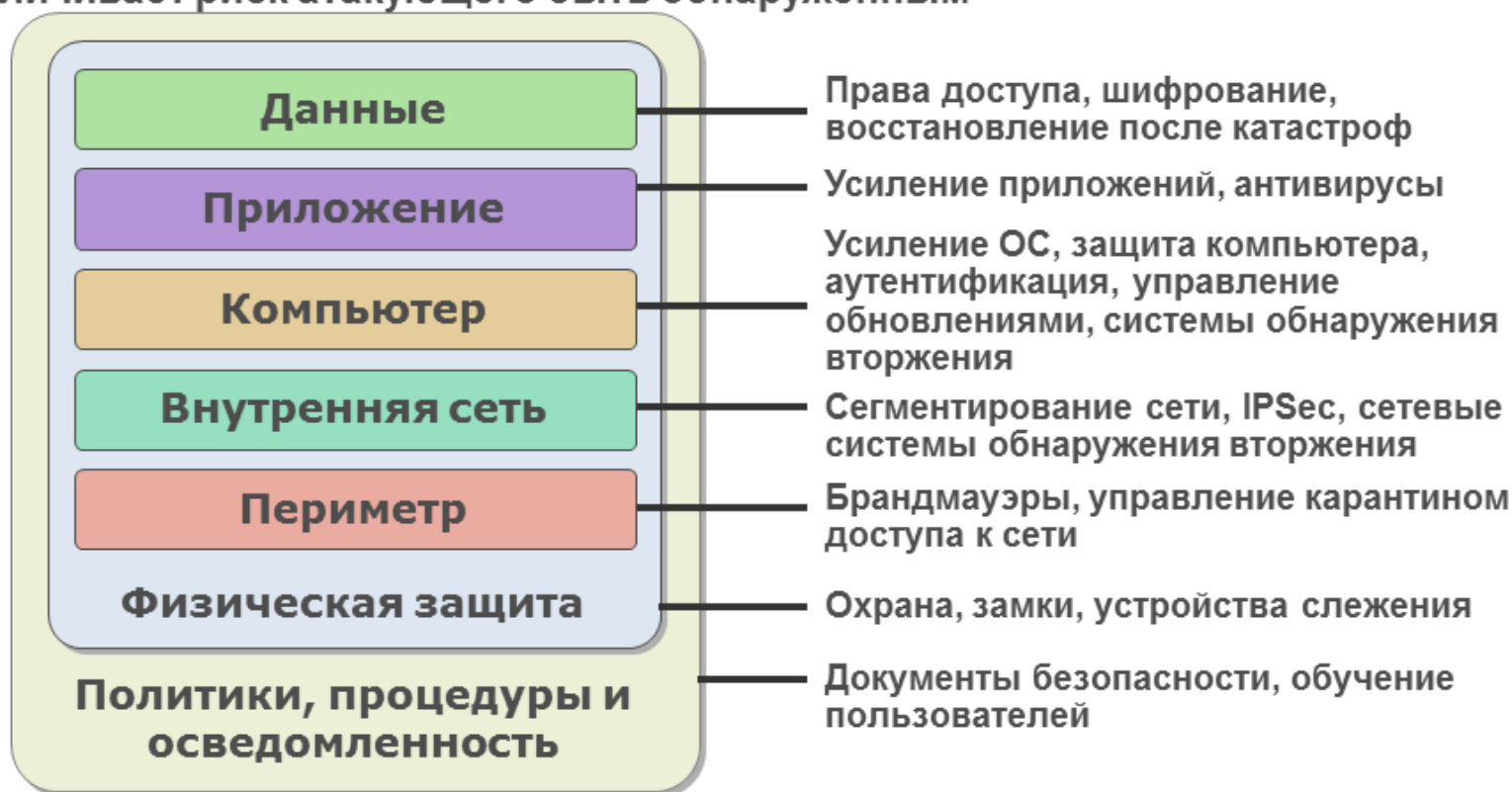
**1** Физический

- Каждый уровень описывает сетевые задачи
- Каждый уровень взаимодействует с выше- и нижележащим уровнем
- 7-й уровень предоставляет сетевые сервисы для программ
- 1-й и 2-й уровни описывают физическую сетевую среду и соответствующие задачи


# Эшелонированная защита

Эшелонированная защита применяет многослойный подход, который:

- Уменьшает шансы атакующего на успех
- Увеличивает риск атакующего быть обнаруженным







# Управление изменениями

Административные процедуры внесения изменений

Кто и при каких условиях может подавать заявку на изменения

Согласование и утверждение изменений

Тестирование

Внедрение изменений

Документирование



# Политики, процедуры и осведомленность

Политики, процедуры и осведомленность относятся к правилам, действиям и знаниям, направленным на избежание проблем с безопасностью

Источники проблем включают:

- Незнание пользователями установленных правил
- Пользователи считают правила ненужными
- Социальная инженерия



# Уровень физической безопасности

**Уровень физической безопасности помогает предотвратить физический доступ к сетевой инфраструктуре и нанесение ей вреда**

Физический доступ к системам позволяет осуществить:

- Физическое уничтожение, порчу
- Установку программ
- Изменение данных
- Кражу

# Безопасность периметра

Безопасность периметра относится к соединениям вашей сети с другими сетями

Проблемы с безопасностью периметра могут привести к:

- Атакам на ресурсы в сети периметра
- Атакам на удаленных клиентов
- Атакам на деловых партнеров и клиентов



# Безопасность внутренней сети

**Безопасность внутренней сети относится к внутренним соединениям вашей сети, включая глобальные каналы связи**

Проблемы безопасности внутренней сети включают:

- Неразрешенные сетевые соединения, взаимодействия
- Неразрешенные сетевые подключения устройств
- Неразрешенный захват пакетов

# **Безопасность уровня данных**

**Безопасность уровня данных относится к данным, хранящимся (обрабатываемых) на компьютере**

**Проблемы безопасности данных включают:**

- Неразрешенный доступ и изменение файлов данных**
- Неразрешенный доступ к службам каталога**
- Изменение файлов приложений**
- Порча, кража данных**



# Варианты защиты компьютерных систем

- Четкие правила, исключая социальную инженерию
- Запираемые двери
- Брандмауэры
- Шифрование каналов связи
- Обновления операционных систем
- Использование минимально необходимых программ
- Шифрование данных, управление доступом

# Политики

Должны быть разные политики для разных групп пользователей:

- 3-5 страниц «курс молодого бойца» только что принятого на работу
- Документ, описывающий правила работы в сети для всех пользователей. Совершенно четко описать что можно делать в сети.
- Документ для администраторов
- Документ для службы информационной безопасности





# Физический уровень

Запираемая серверная комната

Убрать лишние устройства ввода/вывода

Источники бесперебойного питания и генераторы

Если есть компьютеры открытого доступа, то лучше в отдельной сети

Если пользователь покидает компьютер – **разрегистриваться или выключить!**

Актуальный план кабельной разводки.

Неиспользуемые розетки на местах не должны быть подключены к коммуникационному оборудованию.

Отслеживать появление беспроводных устройств, модемов.





# Физический уровень

Замена кабельной проводки:

Коаксиальный кабель -> витая пара -> оптоволокно.

Резервные каналы.

Аппаратное шифрование

Тревожные кнопки

Разграничение доступа в помещения

«Виртуальные» рабочие места

# Физический уровень

Надежность

Отказоустойчивость

Масштабируемость

Архивирование

Резервное копирование



## Сетевой уровень: периметр – препятствие на пути внешних угроз

Международные соединения (внутри компании)

Резервные пути

Соединение с Интернетом

Два последовательных брандмауэра лучше одного  
трехпортового

Пограничные сервисы: DNS, POP/SMTP, Time...



# Сетевой уровень

Сегментирование

Разные протоколы: NetBIOS, IPX/SPX, TCP/IP...

Связность сетей

Резервные пути

Доступ пользователей:

- Локально
- Удаленно
- Через Интернет