

# **Построение политики безопасности организации**

**УЦ «Вигоне»  
2007 год**

## Основной руководящий документ и стандарт Обеспечения ИБ. ИСО МЭК 17799

Политика безопасности – это набор правил и механизмов разграничения доступа регламентирующих функционирование информационных и организационных ресурсов компании

Политика безопасности должна устанавливать ответственность руководства, а также излагать подход организации к управлению информационной безопасностью.

## Составляющие политики безопасности

- Организационные вопросы безопасности
- Классификация и управление активами
- Вопросы безопасности, связанные с персоналом
- Физическая защита и защита от воздействия окружающей среды
- Управление передачей данных и операционной деятельностью
- Контроль доступа
- Разработка и обслуживание систем
- Управление непрерывностью бизнеса
- Механизмы управления рисками безопасности и расследования инцидентов

## Организационные вопросы обеспечения безопасности

- **Обеспечение безопасности при наличии доступа к информационным системам сторонних организаций**
- **Привлечение сторонних организаций к обработке информации (аутсорсинг)**
- **Организационная инфраструктура информационной безопасности**

# Классификация и управление активами

- **Учет активов**
- **Классификация информации**

## Вопросы безопасности связанные с персоналом

- **Учет вопросов безопасности в должностных обязанностях и при найме персонала**
- **Обучение пользователей**
- **Реагирование на инциденты нарушения информационной безопасности и сбои**

# Физическая защита и защита от воздействию окружающей среды

- **Охраняемые зоны**
- **Безопасность оборудования**
- **Общие мероприятия по управлению информационной безопасностью**

## Управление передачей данных и операционной деятельности

- **Операционные процедуры и обязанности**
- **Планирование нагрузки и приемка систем**
- **Защита от вредоносного программного обеспечения**
- **Вспомогательные операции**
- **Управление сетевыми ресурсами**
- **Безопасность носителей информации**
- **Обмен информацией и программным обеспечением**



## Контроль доступа

- **Требование бизнеса по обеспечению контроля в отношении логического доступа**
- **Контроль в отношении доступа пользователей**
- **Обязанности пользователей**
- **Контроль сетевого доступа**
- **Контроль доступа к операционной системе**
- **Контроль доступа к приложениям**
- **Мониторинг доступа и использования системы**
- **Работа с переносными устройствами и работа в дистанционном режиме**

## Разработка и обслуживание систем

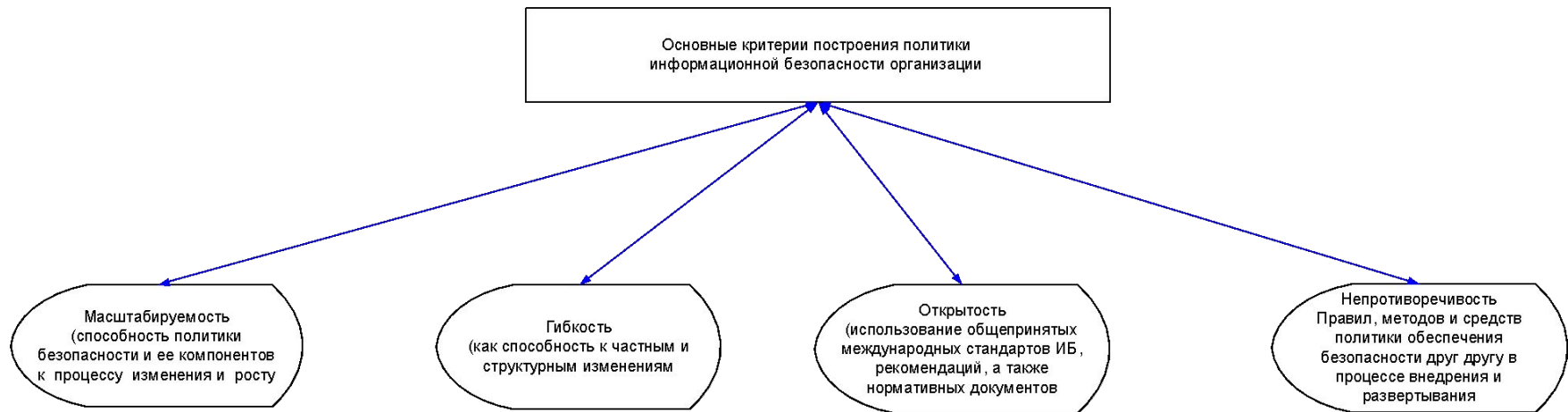
- **Требования к безопасности систем**
- **Безопасность в прикладных системах**
- **Меры защиты информации, связанные с использованием криптографии**
- **Безопасность системных файлов**
- **Безопасность в процессах разработки и поддержки**

## Управление непрерывностью бизнеса

- **Введение механизмов оценки рисков безопасности**
- **Введение механизмов расследования инцидентов безопасности**

# Основные принципы разработки политики безопасности

## Критерии политики безопасности



# Схема полного жизненного цикла обеспечения политики безопасности

