



Курс: **основы информационной безопасности**

Тема: **Политика безопасности,
регламентирующие документы**

Преподаватель: Пятков
Антон Геннадьевич

Красноярск

Принципы организационной ЗИ

Организационная **защита** информации на предприятии – регламентация производственной деятельности и взаимоотношений субъектов (сотрудников предприятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию.

Организационные **меры** информационной безопасности – меры, предусматривающие установление временных, территориальных, пространственных, правовых, методических и иных **ограничений** на условия использования и режимы работы объекта информатизации.

Основные принципы организационной защиты информации:

- ✓ принцип комплексного подхода (эффективное использование сил, средств, способов и методов защиты информации для решения поставленных задач в зависимости от конкретной складывающейся ситуации и наличия факторов, ослабляющих или усиливающих угрозу защищаемой инф.);
- ✓ принцип оперативности принятия управленческих решений (отражает нацеленность руководства и персонала предприятия на решение задач защиты информации, определяет гибкость и эффективность системы);
- ✓ принцип персональной ответственности (распределение задач по защите информации между руководством и персоналом предприятия и определение ответственности за полноту и качество их выполнения).

Нормативно-правовое обеспечение ИБ

На уровне предприятия разрабатываются/используются следующие документы:

- ✓ устав;
- ✓ концепция системы защиты информации на предприятии;
- ✓ политика ИБ;
- ✓ положение о подразделении по защите информации;
- ✓ коллективный трудовой договор;
- ✓ трудовые договоры с сотрудниками предприятия;
- ✓ правила внутреннего распорядка служащих предприятия;
- ✓ должностные обязанности руководителя, специалистов, служащих предприятия;
- ✓ инструкции пользователям АС и БД;
- ✓ инструкции администраторов АС и БД;
- ✓ инструкции сотрудников, допущенных к защищаемой информации;
- ✓ инструкции сотрудников, ответственных за защиту информации;
- ✓ памятка сотрудника о сохранении коммерческой тайны;
- ✓ договорные обязательства персонала.

Эталонная структура нормативного обеспечения системы ИБ



Политика ИБ

Согласованность, целенаправленность и планомерность деятельности по обеспечению ИБ может быть достигнута только при нормативном закреплении ожиданий руководства и правил осуществления деятельности в организации.

Документы позволяют отразить и формализовать нормы.

Политика ИБ – документация, определяющая высокоуровневые цели, содержание и основные направления деятельности по обеспечению ИБ, предназначенная для организации в целом.

Частная политика ИБ - документация, детализирующая положения политики ИБ применительно к одной или нескольким областям ИБ, видам и технологиям деятельности

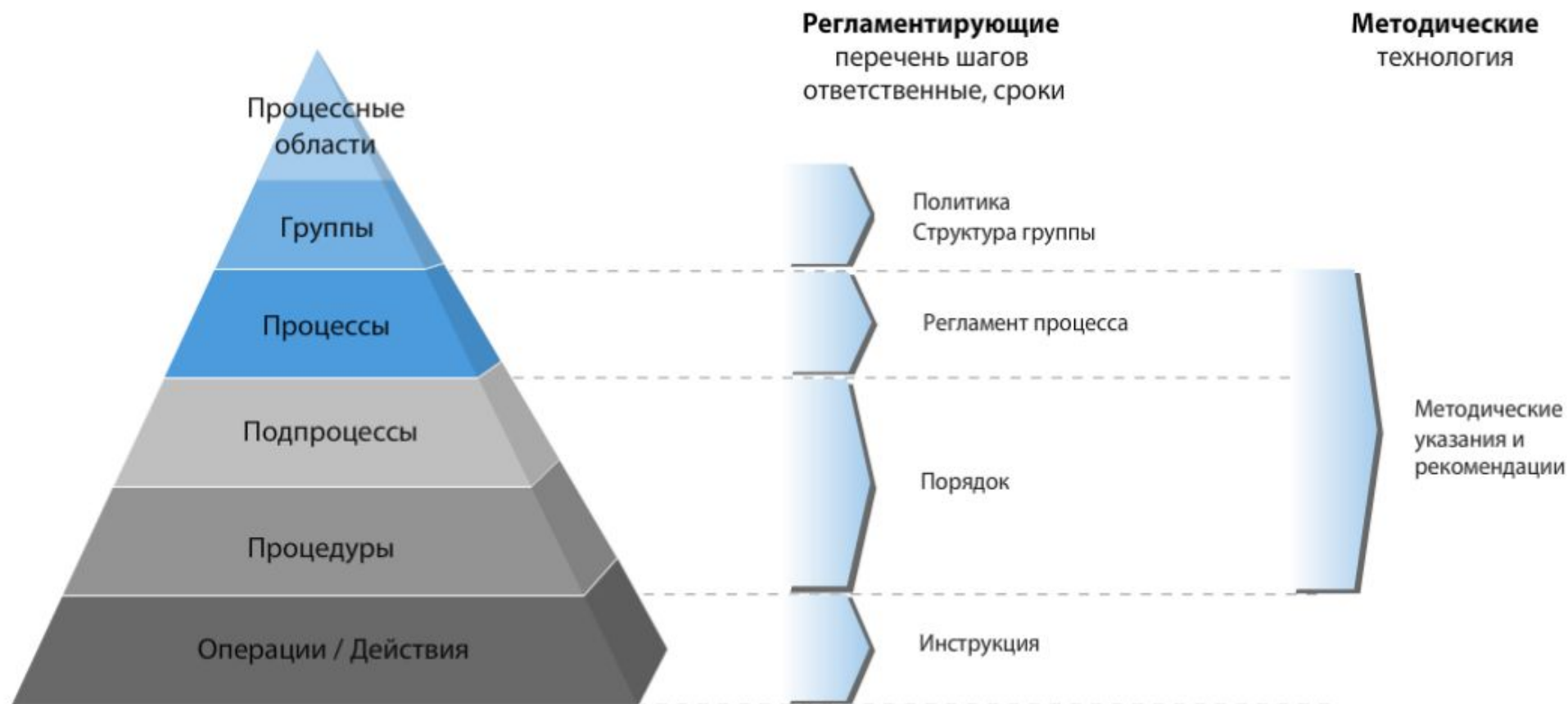
В политике (в частных политиках) ИБ должны определяться:

- ✓ цели и задачи обеспечения ИБ;
- ✓ основные области обеспечения ИБ;
- ✓ типы основных защищаемых информационных активов;
- ✓ модели угроз и нарушителей;
- ✓ совокупность правил, требований и руководящих принципов в области ИБ;
- ✓ основные требования по обеспечению ИБ;
- ✓ принципы противодействия угрозам ИБ защищаемых активов;
- ✓ принципы повышения уровня осознания и осведомленности в области ИБ;
- ✓ принципы реализации и контроля выполнения требований политики ИБ.

Процессная модель

Структура процессной модели

Документы



Безопасность – это постоянный процесс

Цикл Деминга для ИБ

