

2008

КОНЦЕПЦИЯ И МОДЕЛИ МЕНЕДЖМЕНТА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Студенты группы 4406

Кукарин Тимур,

Шамсутдинова Диляра

ГОСТ Р ИСО/МЭК 13335-1

- Идентичен международному стандарту ИСО/МЭК 13335-1:2004;
- Устанавливает концепцию и модели, лежащие в основе базового понимания безопасности ИТТ;
- Раскрывает общие вопросы управления, которые важны для успешного планирования, реализации и поддержки безопасности ИТТ

Термины

- Подотчетность (accountability)
- Аутентичность (authenticity)
- Инцидент информационной безопасности (information security incident)
- Неотказуемость (non-repudiation)
- Информационная безопасность (information security)
- Менеджмент риска (risk management)

Концепция безопасности и взаимосвязи: принципы

- Менеджмент риска;
- Обязательства;
- Служебные обязанности и ответственность ;
- Цели, стратегии и политика;
- Управление жизненным циклом

Концепция безопасности и взаимосвязи: активы

- Материальные активы;
- Информация;
- Программное обеспечение;
- Способность производить продукт или предоставлять услугу;
- Люди;
- Нематериальные ресурсы;

Концепция безопасности и взаимосвязи: угрозы

Т а б л и ц а 1 — Примеры угроз

Угрозы, обусловленные человеческим фактором		Угрозы среды
целенаправленные	случайные	
Подслушивание/перехват. Модификация информации. Атака хакера на систему. Злонамеренный код. Хищение	Ошибки и упущения. Удаление файла. Ошибка маршрутизации. Материальные несчастные случаи	Землетрясение. Молния. Наводнение. Пожар

Концепция безопасности и взаимосвязи: уязвимости

- **Уязвимость** - слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами.
- **Пример:** отсутствие контроля доступа, которое может обусловить возникновение угрозы несанкционированного доступа и привести к утрате активов.

Концепция безопасности и взаимосвязи: воздействие

- **Воздействие** – результат нежелательного инцидента информационной безопасности.
- **Воздействие:**
 - Разрушение актива;
 - Повреждение ИТТ;
 - Нарушение конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности

Концепция безопасности и взаимосвязи: риск

- Риск - потенциальная опасность нанесения ущерба организации в результате реализации некоторой угрозы с использованием уязвимостей актива или группы активов.
- Риск – это **вероятность инцидента и его воздействие.**
- Остаточный риск - риск, остающийся после его обработки.

Концепция безопасности и взаимосвязи: защитные меры

- **Защитная мера** - сложившаяся практика, процедура или механизм обработки риска.
- Понятие «**защитная мера**» может считаться синонимом понятию «**контроль**».
- **Функции:**
 - Предотвращение;
 - Обнаружение;
 - Исправление;
 - Восстановление;
 - и иное.

Взаимосвязь компонентов безопасности

- Модель безопасности:
- окружающую среду;
- активы организации;
- уязвимости;
- меры для защиты активов;
- приемлемые для организации остаточные риски.

Взаимосвязь компонентов безопасности

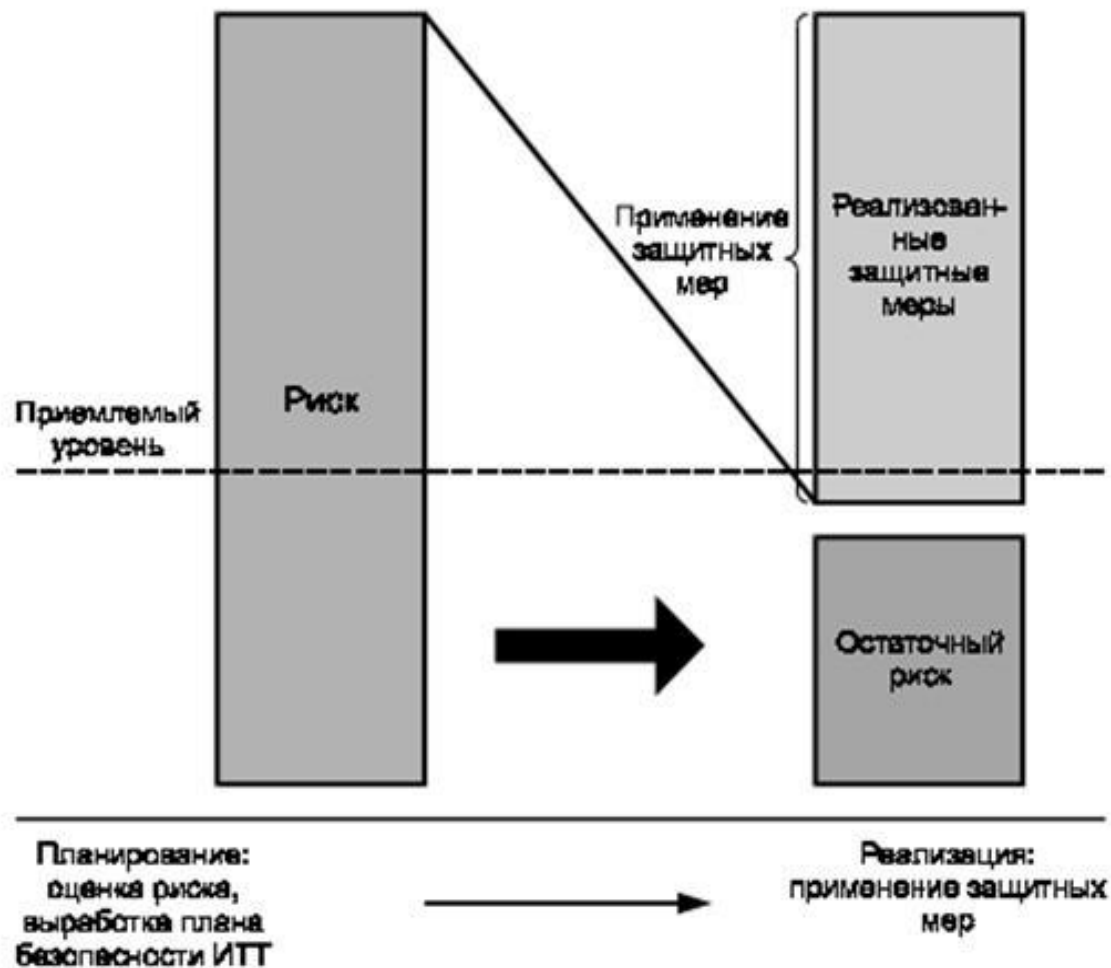


Рисунок 2 — Взаимосвязь защитных мер и риска

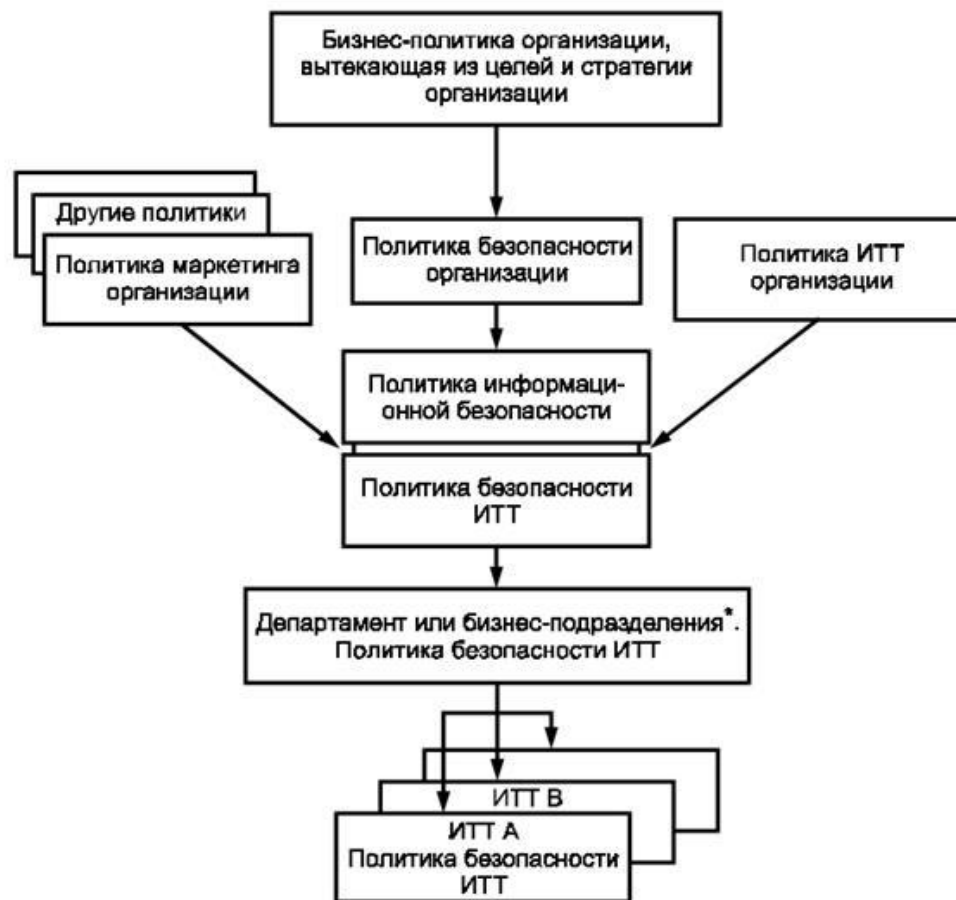
Цели, стратегия и политика

- Содействуют деятельности организации;
- Обеспечивают согласованность всех защитных мер;
- Определяют уровень безопасности для организации и порог приемлемого риска.

Цели, стратегия и политика

- Какие важные составляющие бизнеса не могут осуществляться без ИТТ?
- Какие задачи могут быть решены только при помощи ИТТ?
- Какие важные решения зависят от конфиденциальности, целостности, доступности, неотказуемости, подотчетности и аутентичности информации, хранимой или обрабатываемой ИТТ?
- Какая хранимая или обрабатываемая информация должна защищаться;

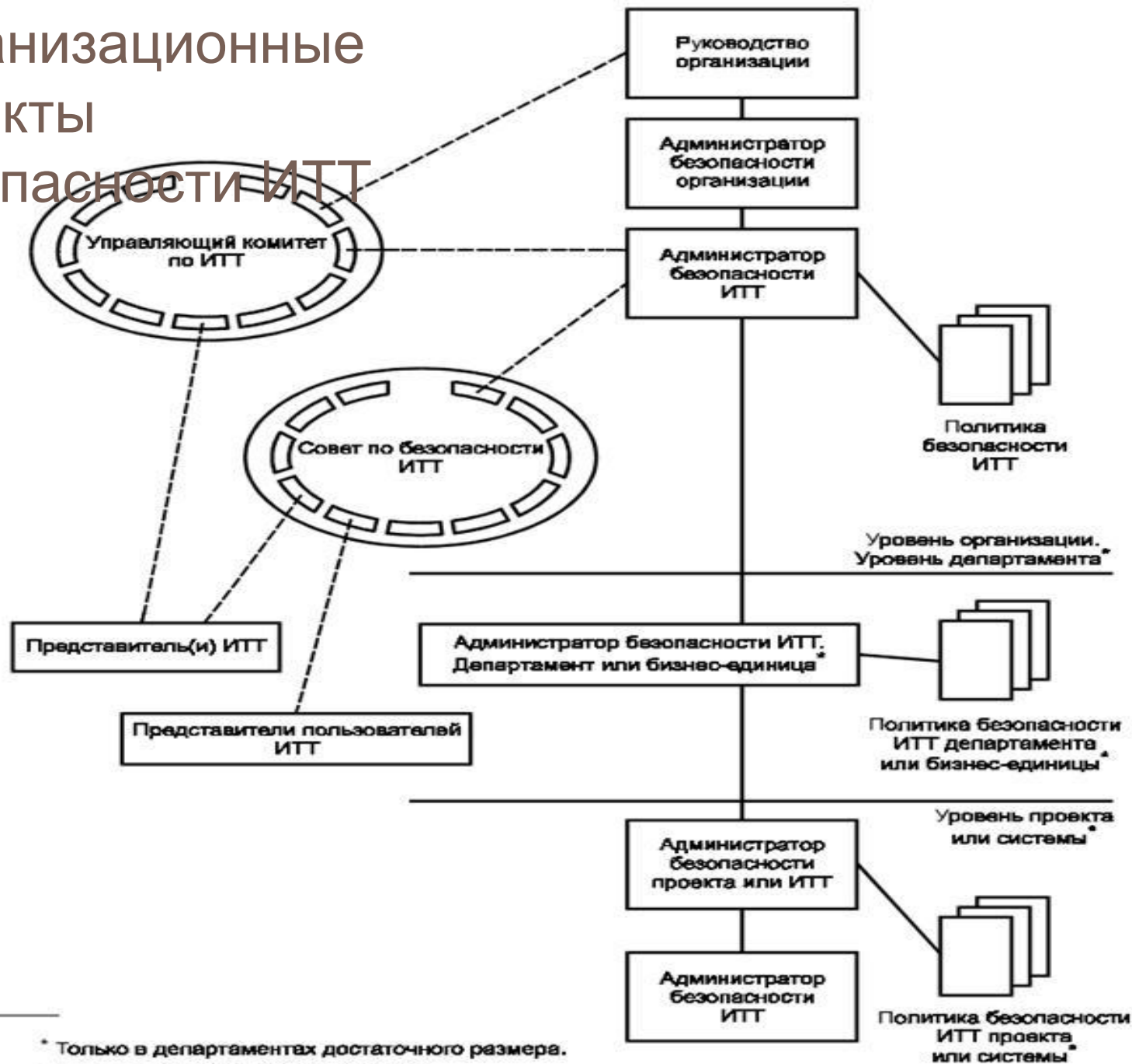
Иерархия политик



* Глубина иерархии (число слов) зависит от нескольких факторов (например размера организации).

Рисунок 3 — Иерархия политик

Организационные аспекты безопасности ИТТ



* Только в департаментах достаточного размера.

----- - служебные обязанности;

————— - организационный уровень

Совет по безопасности ИТ

- **Обязанности:**
- Консультирование по вопросам стратегического планирования в сфере безопасности;
- Формулирование политики безопасности;
- Транслирование политики безопасности в программу безопасности ИТТ;
- Мониторинг реализации программы безопасности ИТТ;
- Анализ эффективности политики безопасности ИТТ;
- Повышение осведомленности о вопросах безопасности ИТТ

Администратор безопасности ИТТ

- **Обязанности:**
- Наблюдение за реализацией программы безопасности ИТТ;
- Опубликование и поддержка политики безопасности ИТТ и директив;
- Координация расследования инцидентов;
- Анализ, аудит и мониторинг эффективности контроля безопасности;
- Анализ, аудит и мониторинг строгого соблюдения процедур безопасности ИТТ в организации

Функции управления безопасностью ИТТ

а) планирование:

- 1) определение организацией требований по безопасности ИТТ,
- 2) определение организацией целей, стратегий и политик безопасности ИТТ,
- 3) установление обязанностей и ответственности в рамках организации,
- 4) разработка плана по безопасности ИТТ,
- 5) оценка рисков,
- 6) решение об обработке риска и выборе защитных мер,
- 7) планирование непрерывности бизнеса;

б) реализация:

- 1) создание защитных мер,
- 2) одобрение ИТТ,
- 3) разработка и выполнение программы осведомленности персонала о безопасности,
- 4) аудит-функционирование защитных мер;

в) эксплуатация и поддержка:

- 1) контроль конфигурации и управление изменениями,
- 2) управление непрерывностью бизнеса,
- 3) анализ, аудит и мониторинг, а также проверка соответствия безопасности заявленным требованиям,
- 4) управление инцидентами безопасности информации.