ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лекция 10(Организационное обеспечение информационной безопасности):

«Организационные основы управления информационной безопасностью»

Вопросы:

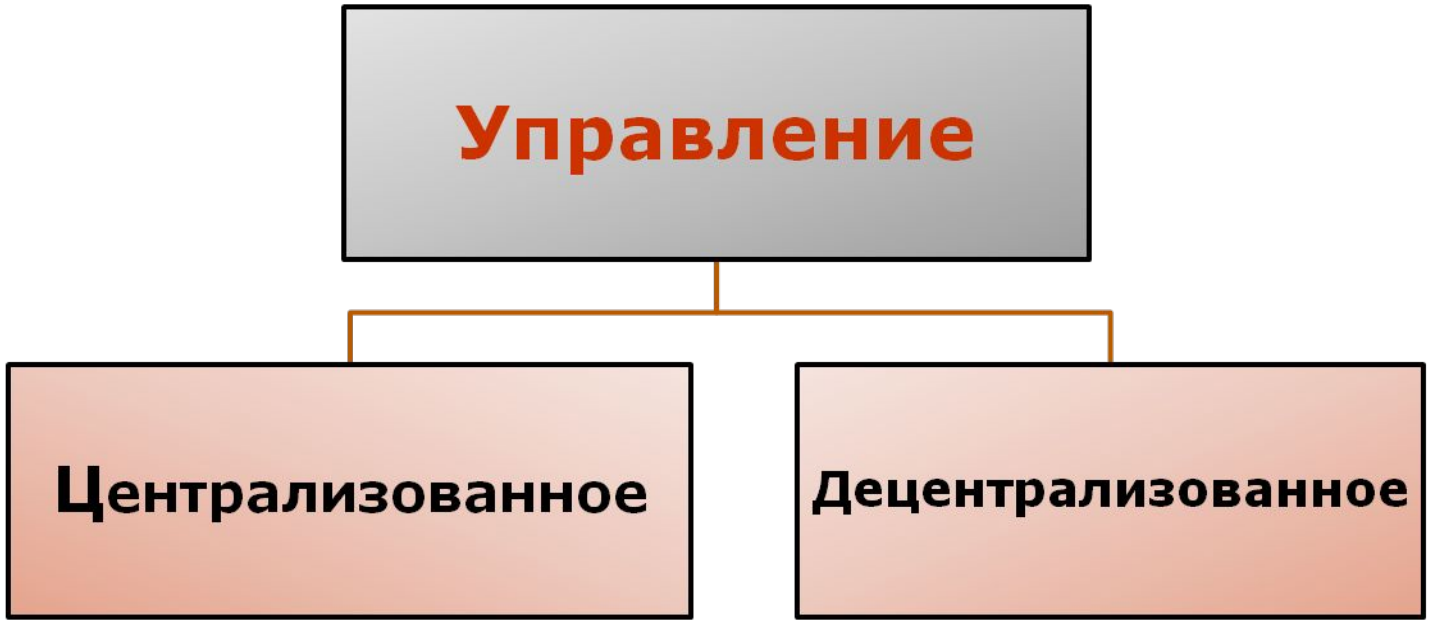
1. **Модели организационного управления ИБ.**
2. **Организационная инфраструктура управления ИБ.**
3. **Организационные мероприятия по управлению ИБ.**
4. **Основы организации службы защиты информации.**

Вопрос 1: «Модели организационного управления ИБ»

- **Главная цель организационного управления ИБ** - наиболее продуктивным способом объединить существующие в организации структуры и культуру с новой деятельностью по разработке и внедрению СОИБ.

Основы организационного управления

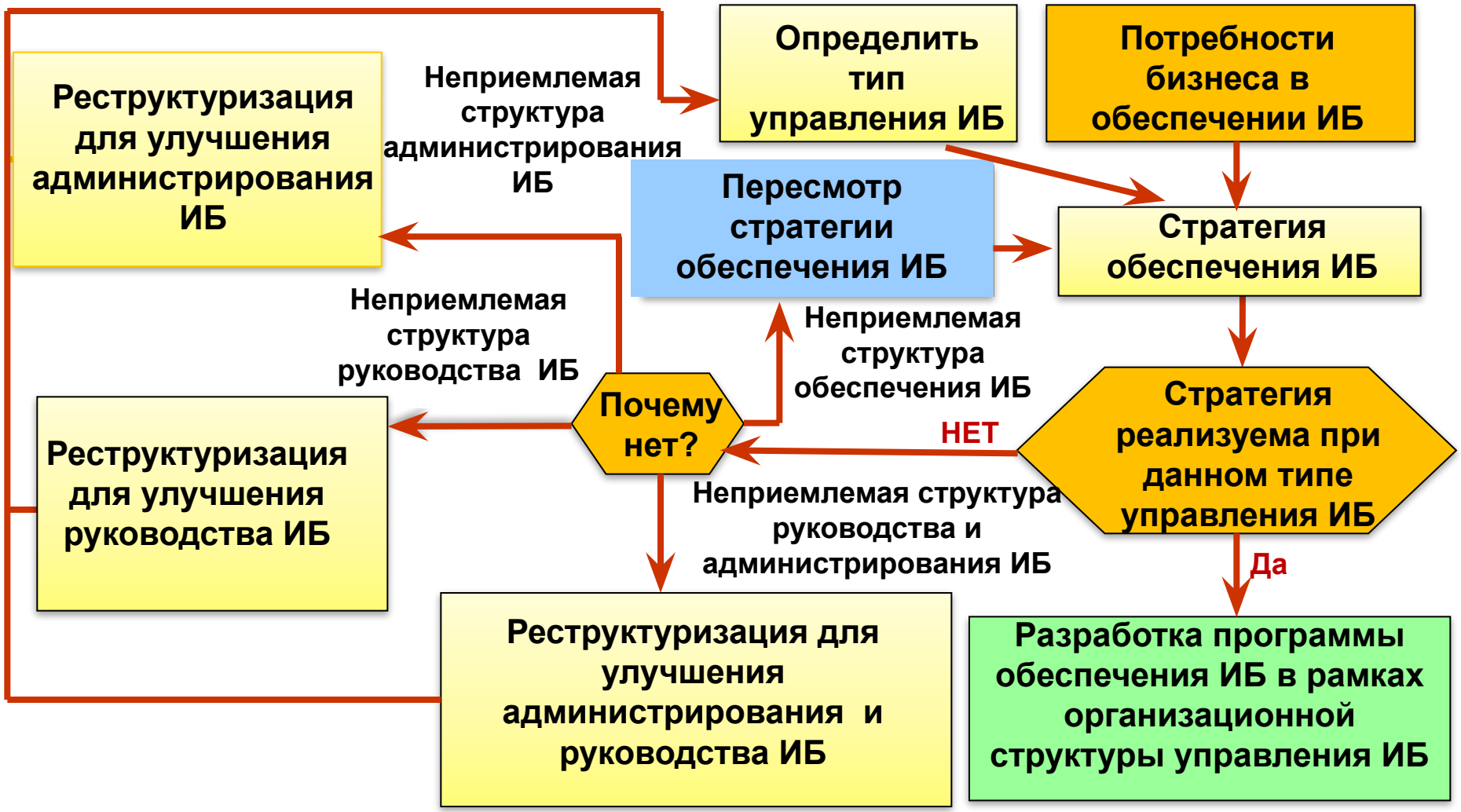
- Организационное управления ИБ **определяет** способ, которым ИБ передается под контроль, реализуется и управляется во всей организации.



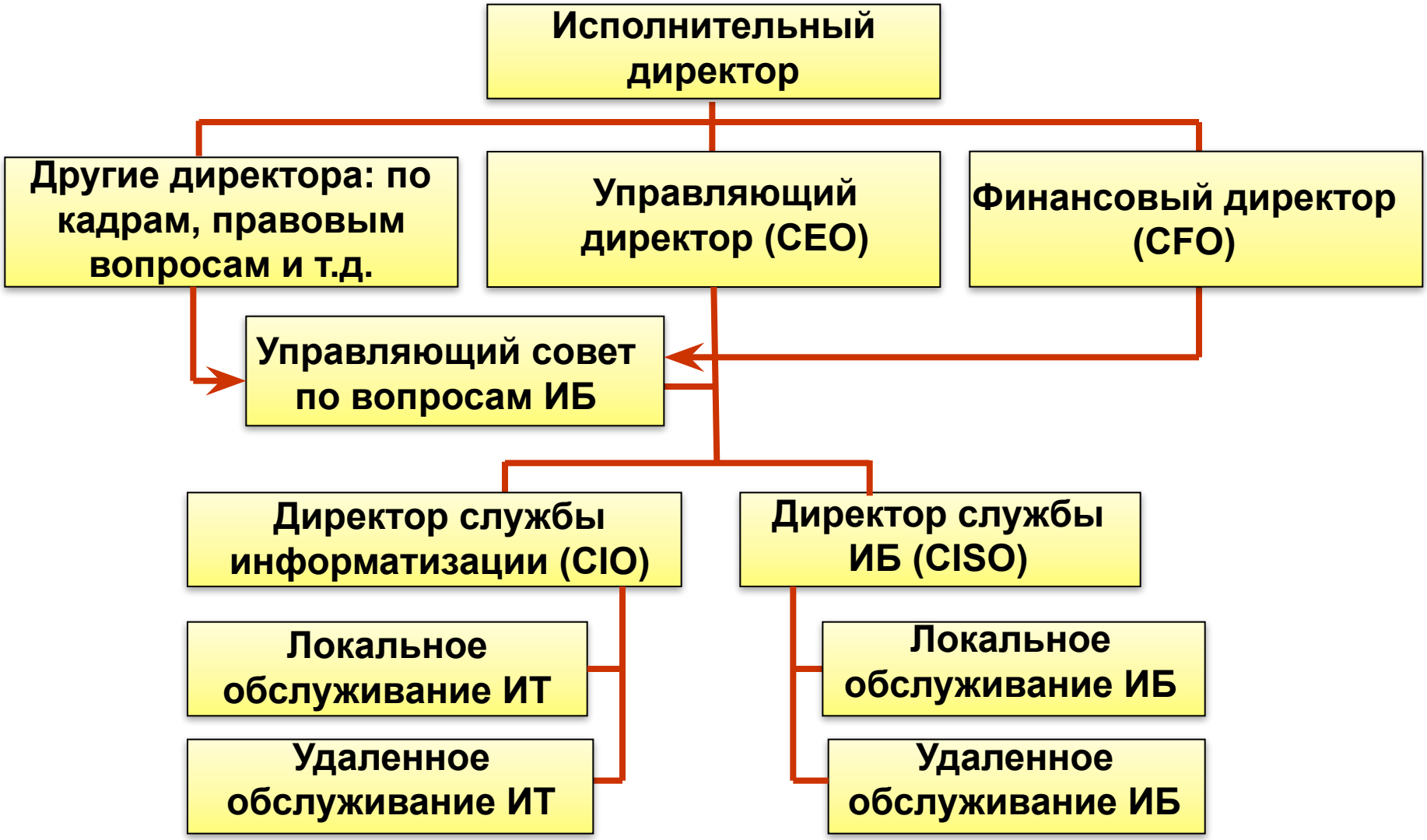
Различие вариантов управления

- Централизация указывает на **наличие единого органа**, который может быть **отдельным лицом, комитетом или другой структурной единицей**.
- Децентрализация подразумевает **наличие нескольких органов** с одинаковым уровнем полномочий.

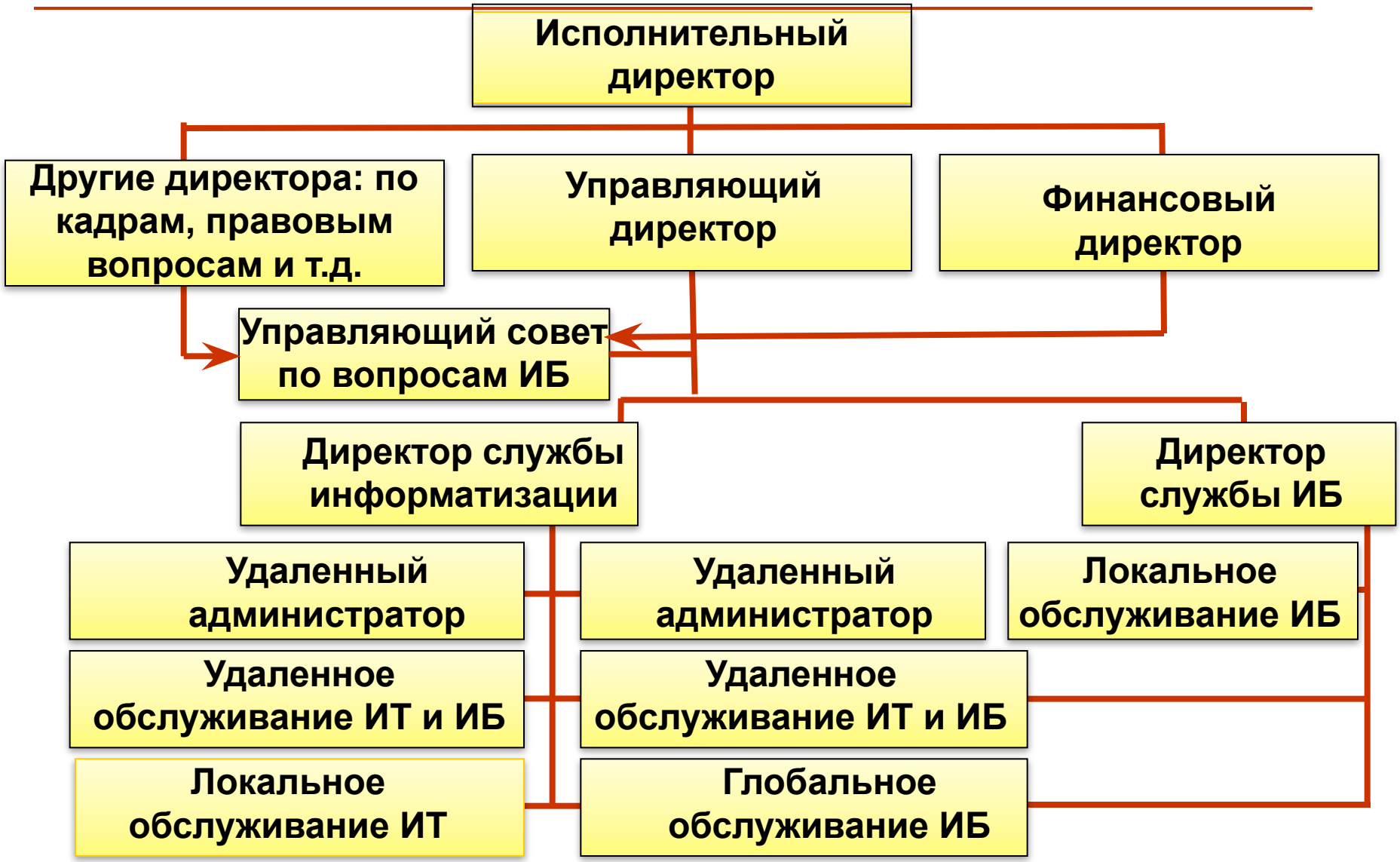
Модель организационного управления ИБ



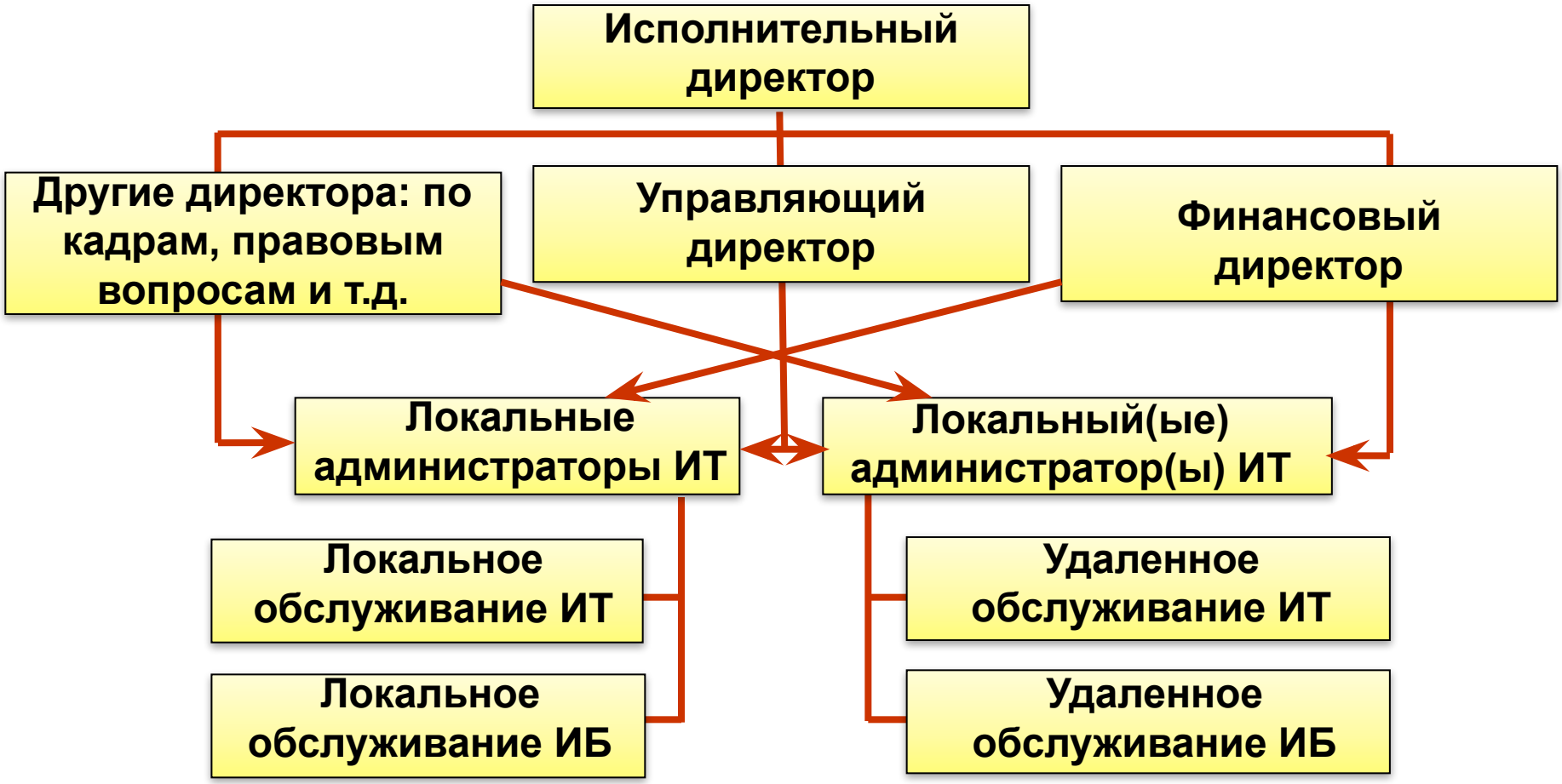
Централизованное руководство/ централизованное администрирование ИБ



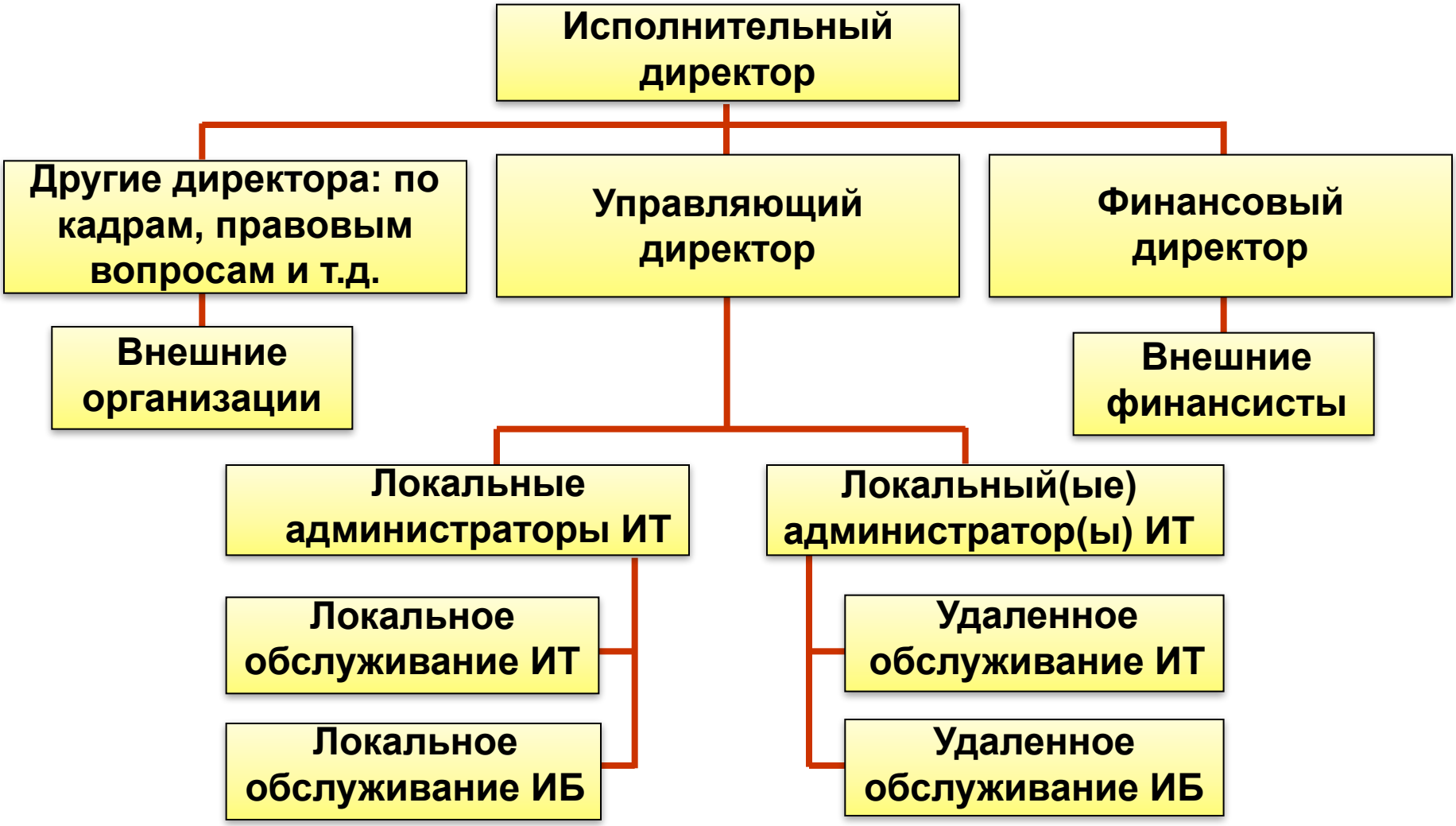
Централизованное руководство/ децентрализованное администрирование ИБ



Децентрализованное руководство/ централизованное администрирование ИБ



Децентрализованное руководство/ децентрализованное администрирование ИБ



Вопрос 2: «Организационная инфраструктура управления ИБ»

- **Организационная инфраструктура управления ИБ** строится так, чтобы она способствовала контроля за внедрением организации ИБ.
- **Для этого:**
- Назначается **ответственный** за все вопросы, связанные с ИБ.
- Создаются **комитеты по управлению** вопросами ИБ с участием высшего руководства.

Ключевые участники процесса управления ИБ

Комитет по управлению вопросами ИБ

РУКОВОДСТВО

Служба ИТ

Служба управления рисками ИБ

Служба внутреннего аудита

Служба ИБ

Функции участников процесса управления ИБ

- **Руководство**: поддержка и анализ СУИБ, утверждение Политики ИБ, распределение ключевых ролей и ответственности, общий контроль за управлением ИБ;
- **Комитет по управлению вопросами ИБ**: стратегическое управление, утверждение ключевых документов и бюджета ИБ;
- **Служба ИБ**: оперативное управление, реализация мероприятий по обеспечению ИБ и уменьшению соответствующих рисков;

Функции участников процесса управления ИБ

- **Служба управления рисками ИБ**: оценка рисков ИБ, подготовка и контроль реализации решений руководства по обработке рисков ИБ;
- **Служба внутреннего аудита**: независимый контроль и оценка эффективности деятельности всех подразделений (риск-менеджмент);
- **Служба ИТ**: реализация ПТС управления ИБ в зоне ответственности совместно или под контролем службы ИБ.

Все участники процессов управления и обеспечения ИБ должны иметь:

- **механизмы взаимодействия с другими лицами;**
- **обязанности,** одобренные надлежащими лицами и в надлежащем порядке;
- **определенные и достаточные полномочия** для обеспечения выполнения **Политики ИБ** организации.

Вопрос 3: «Организационные мероприятия по управлению ИБ»

- Организационные мероприятия по управлению ИБ создают **основу, объединяющую различные защитные меры в единую СОИБ.**

Разовые мероприятия

- **Однократно проводимые** и повторяемые только при полном пересмотре принятых решений в области управления ИБ:
  - Создание организационной инфраструктуры управления ИБ;
  - Построение моделей нарушителей ИБ для всех активов организации;
  - Разработка требований по основным направлениям ОИБ в организации;
  - Разработка правил разграничения доступа к активам, организация охраны и режима.

Постоянно проводимые мероприятия

- Мероприятия, проводимые **непрерывно или дискретно в случайные моменты времени**:
  - обеспечение достаточного уровня физической защиты всех активов;
  - постоянный мониторинг функционирования всех активов для выявления проблем с ИБ;
  - организацию явного и скрытого контроля за работой пользователей и персонала систем, сетей и сервисов;
  - анализ состояния, осуществляемый службы ИБ и т. д.

Проводимые периодически

- Мероприятия, проводимые **через определенные промежутки времени:**
  - распределение реквизитов разграничения доступа (паролей, ключей шифрования и т. п.);
  - пересмотр моделей угроз ИБ и нарушителей ИБ;
  - анализ состояния и оценки эффективности мер ЗИ, совершенствование СОИБ, проведение учений и обучения в области ИБ и т. д.

Проводимые по мере необходимости

- Мероприятия, проводимые при осуществлении или **возникновении определенных изменений** в защищаемых активах организации или ее внешней среде:
  - кадровые изменения в составе сотрудников организации, вовлеченных в процесс управления ИБ;
  - ремонт и модификация АО и ПО;
  - расследование инцидентов ИБ;
  - восстановление работы активов после инцидентов ИБ;
  - Консультации специалистов в области ИБ и т. д.

Сотрудничество между организациями и консультации со специалистами в области ИБ

- Организации могут получать **консультации специалистов по вопросам ИБ**.
- **Консультанты/администраторы** по ИБ должны иметь возможность сами **получать консультации** по всем аспектам ИБ, в том числе и с привлечением внешних специалистов.
- При обменах информацией по вопросам ИБ между организациями должна **обеспечиваться ЗИ от НСД.**

Вопрос 4: «Основы организации службы защиты информации»

Основные цели службы ИБ:

- **предотвращение возможности завладения** злоумышленником правами на чужой актив или самим активом;
- **предотвращение возможности нанесения** ущерба организации за счет получения злоумышленником дохода от неправомерного использования им чужого актива;
- **минимизация рисков** ИБ.

Нормативно-правовая база деятельности службы ИБ

- **законы и подзаконные акты**, действующие на территории РФ;
- **«Положение о службе безопасности организации**;
- **должностные инструкции**.

Основные функции службы ИБ

Функции разработки методологии и проведения анализа ИБ

Функции развития и взаимодействия

Функции аудита и контроля

Функции эксплуатации СЗИ

Функции, выходящие за рамки службы ИБ

Варианты создания службы ИБ

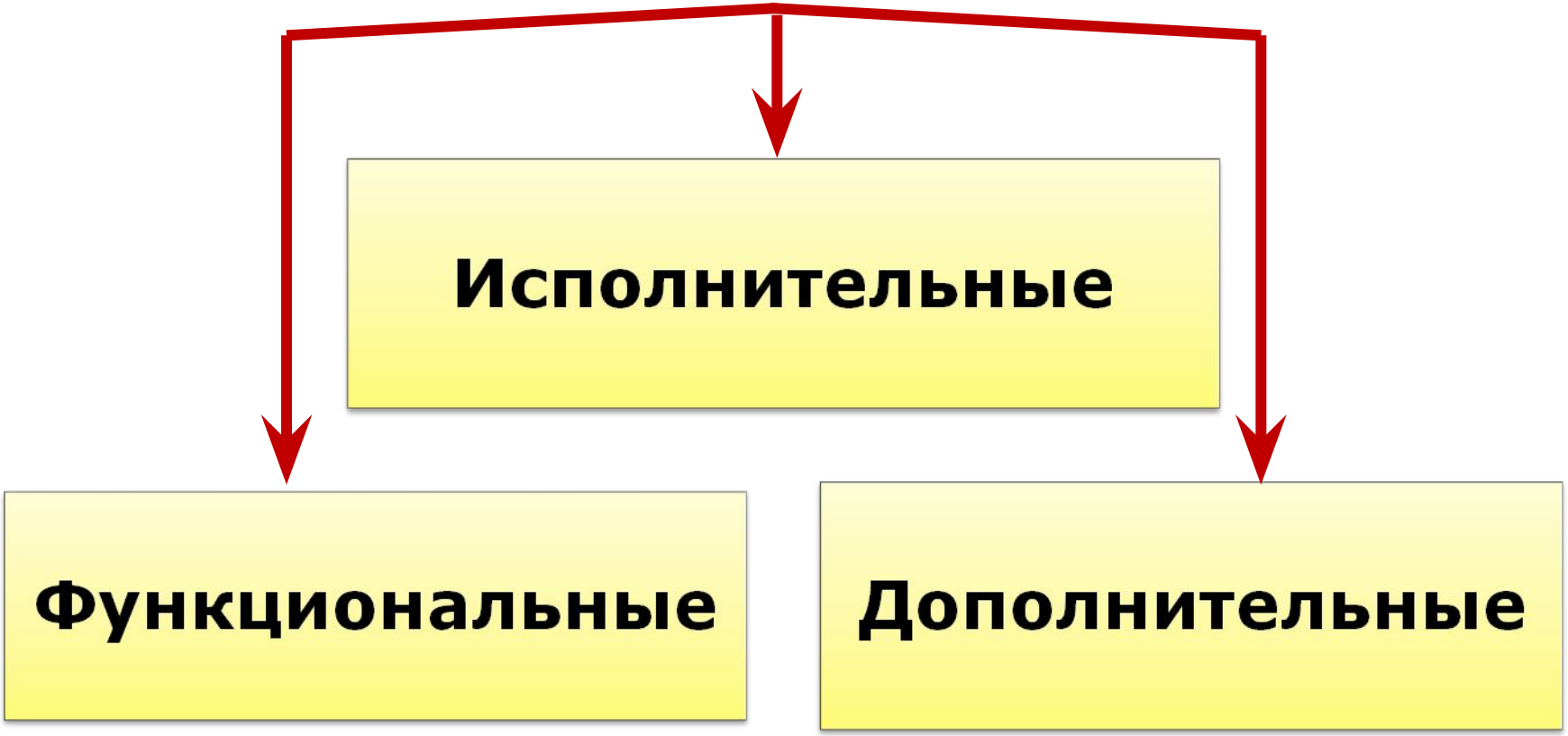
Системные администраторы и администраторы прикладных систем, фактически выполняющие функции ИБ

Выделенные в организации работники или отдельное подразделение, основной задачей которого является организация обеспечения ИБ

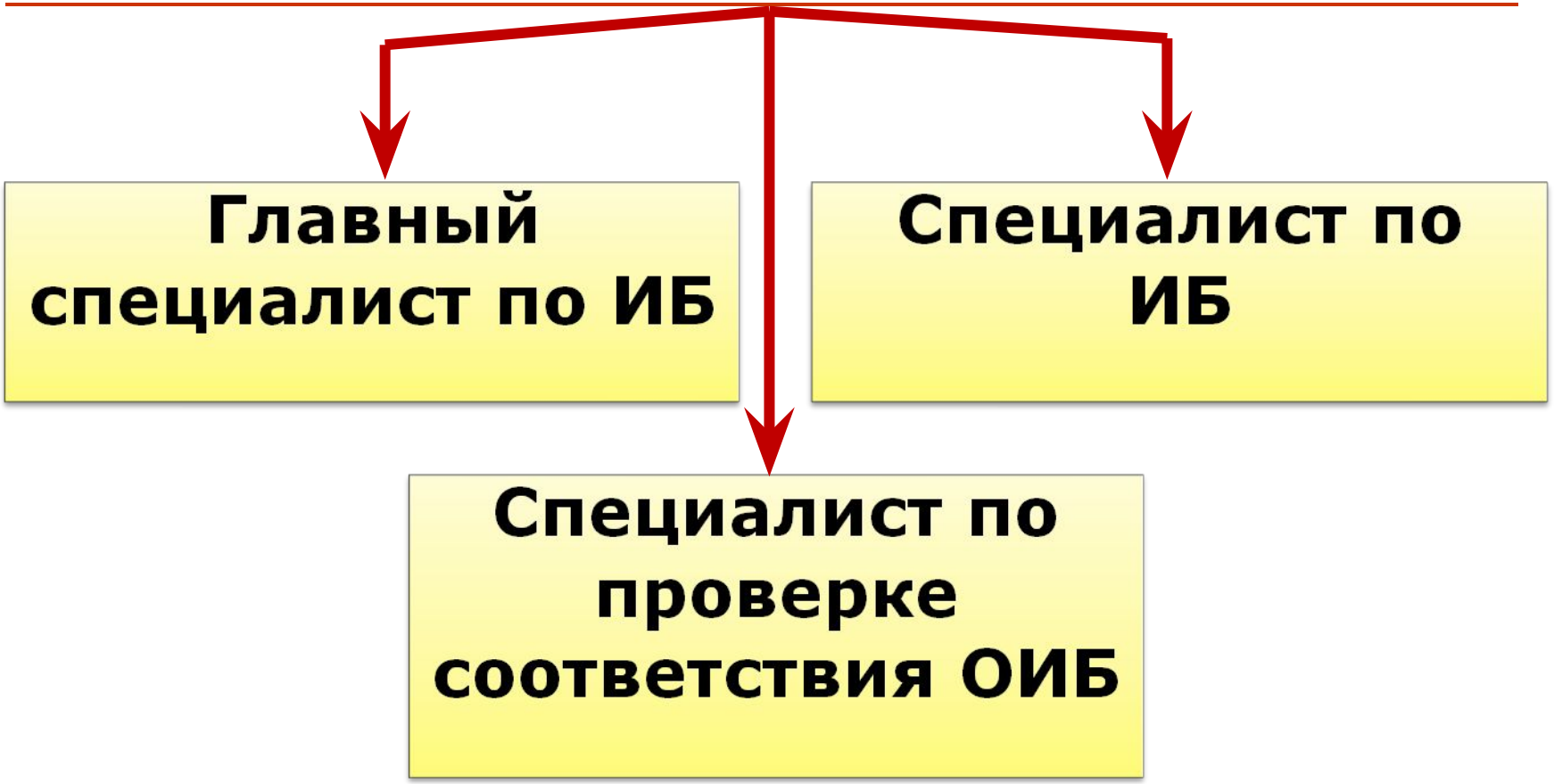
Состав службы ИБ

- руководитель/начальник или директор;
- заместитель начальника службы ИБ;
- аналитики по вопросам ИБ;
- риск-менеджер;
- криптоаналитик;
- ответственные за работу с ПДн;
- администраторы СКЗИ;
- администратор ИБ;
- Сотрудник по расследованию инцидентов.

Должности по обеспечению ИБ



Исполнительные должности



Функциональные должности

Дополнительные должности

Замещение должностей по ЗИ может подразумевать следующие виды профессиональной деятельности:

- организационно-управленческая (управление);
- проектная (разработка);
- эксплуатационная (реализация, внедрение);
- контрольно-аналитическая (оценка);
- научно-исследовательская (теория и методология, проведение научных исследований, защита диссертации);
- педагогическая (преподавательская деятельность).