Централизация управления информационной безопасностью в условиях использования современных решений коллективной обработки данных и применения технологий виртуализации

Внедрение новых информационных технологий и в частности: систем централизованной обработки данных на базе ЦОД, систем виртуализации, применение технологий облачных сервисов, в настоящее время является объективной необходимостью.

При этом всегда имеют место риски невыполнения (срыва) стоящих перед организацией целевых задач.

Что необходимо для минимизации данных рисков?

Система управления и контроля

Внедрение процессов организации (менеджмента ИБ), должно обеспечивать эффективное управление и контроль состояния применяемых в ИС систем и средств защиты информации.

Выполнение каких требований должна обеспечить система управления?

1. СОИБ функционировала в соответствии установленными технологическими регламентами Политики ИБ;
2. Применяемые системы администрирования мер и средств защиты были унифицированы;
3. Процессы обеспечения ИБ были типизированы (регламентированы);
4. Управление системами/подсистемами СОИБ велось из единого центра управления и мониторинга;
5. Применение средств и систем защиты было комплексным (эшелонированным);
6. Процессы оценки и анализа защищенности обеспечивали эффективное управление рисками ИБ и выполнялись оперативно .

Стратегическая задача обеспечения ИБ в территориально-распределенной информационно-телекоммуникационной системе

Совершенствование СОИБ в условиях применения современных решений коллективной обработки данных и технологий виртуализации

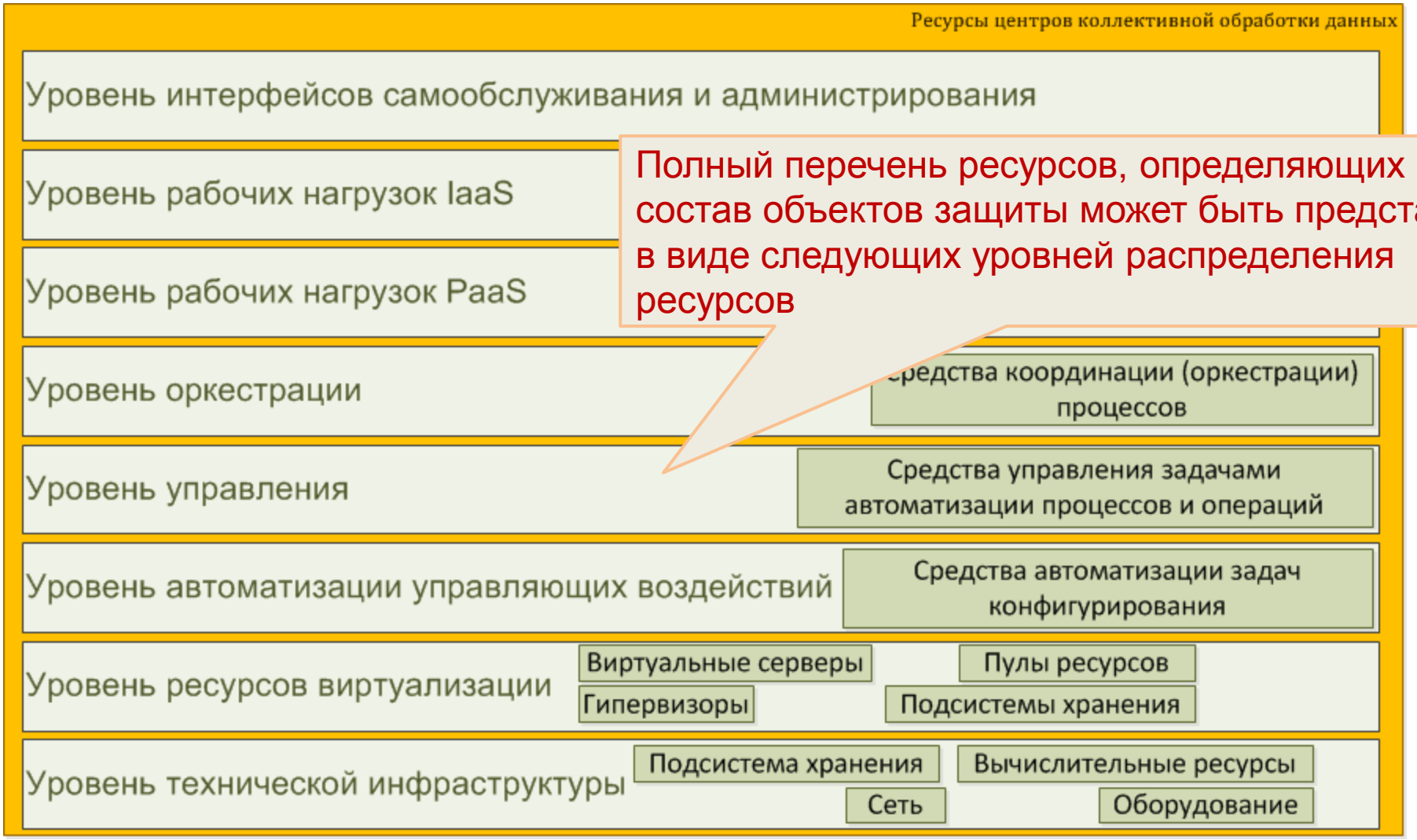
Объекты защиты

Построение любой системы управления ИБ непосредственно связано в информационными ресурсами, подлежащими защите.

В качестве типовых объектов защиты характерных для систем распределенной обработки данных, ЦОД, систем виртуализации должны рассматриваться:

- **многопроцессорные системы**, функционирующие как одна мощная компьютерная система;
- **RAID-массивы и средства управления томами**, обеспечивающих представление нескольких физических дисков как один логический;
- **объекты виртуальной среды и средства управления ими**. Такие как системы хранения, применяемые для создания сетей хранения данных SAN (Storage Area Network);
- **виртуальные частные сети (VPN) и сервисы трансляции сетевых адресов** (NAT), позволяющие создавать виртуальные пространства сетевых адресов и доменных имен.

Форма представления объектов защиты



Полный перечень ресурсов, определяющих состав объектов защиты может быть представл в виде следующих уровней распределения ресурсов

Особенности современных технологий обработки данных

1. Кластеризация компьютеров
2. Распределенные вычисления (grid computing)
3. Разделение ресурсов виртуальной среды
4. Инкапсуляция. Как сокрытие объектом внутри себя своей реализации
5. Динамическая миграция объектов среды виртуализации

Представленные технологии должны рассматриваться, как актуальные источники уязвимостей.

Новые риски, не характерных для традиционных АС

Определяются уязвимостями применяемых гипервизоров. Если гипервизор ненадежен, он станет первой целью злоумышленников

1. Риски компрометации гипервизора виртуальных машин.

Определяются уязвимостями процессов выделения и освобождения такие ресурсы, как локальные виртуальные хранилища

2. Риски компрометации ресурсов виртуальных машин

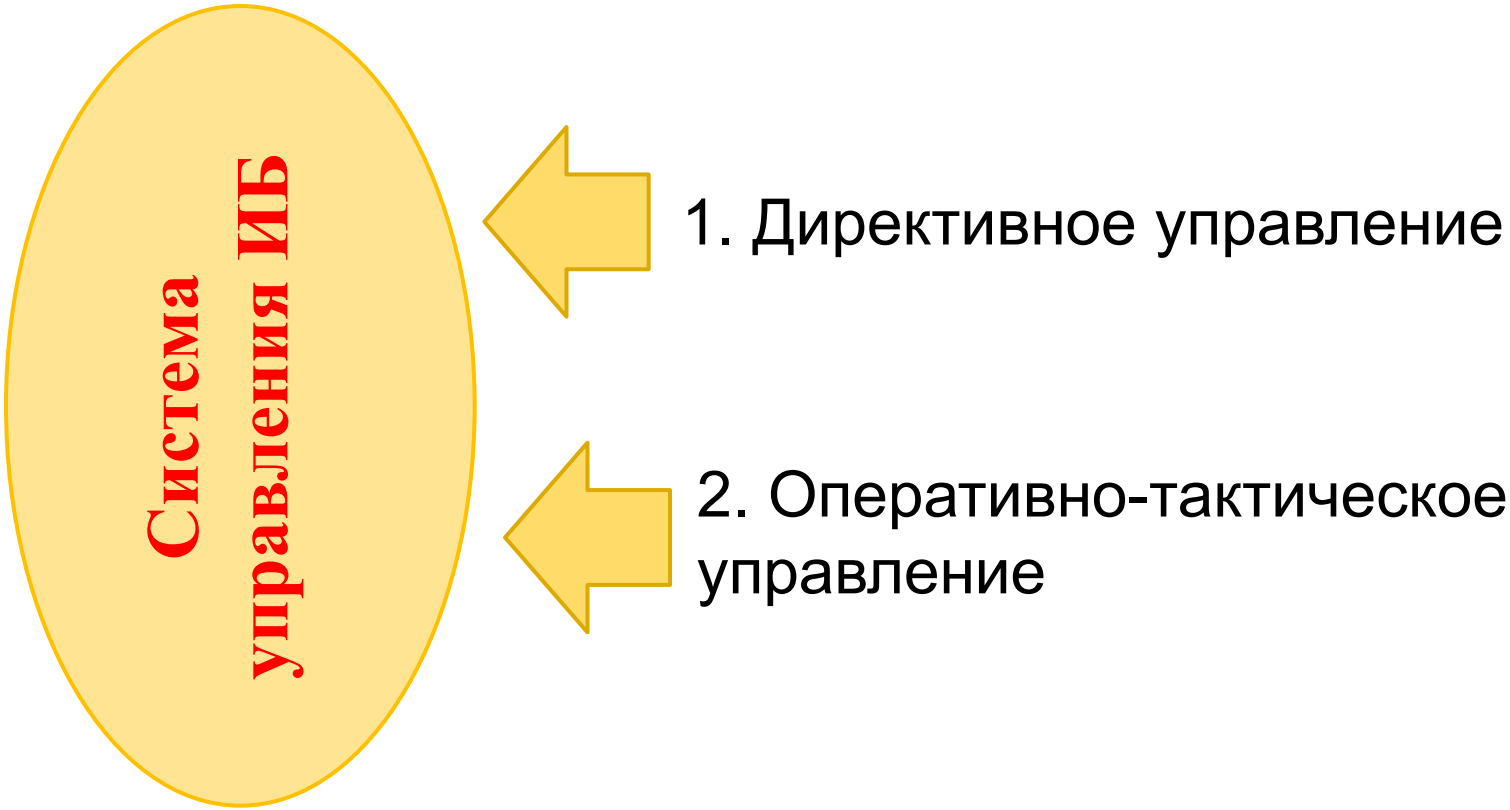
Определяются уязвимостями в мониторинге сетевого трафика виртуальные машины, которые динамически перемещаться в ходе выполнения балансировки рабочей нагрузки серверов виртуализации

3. Риски реализации сетевых атак между виртуальными машинами, расположенными на одном физическом сервере

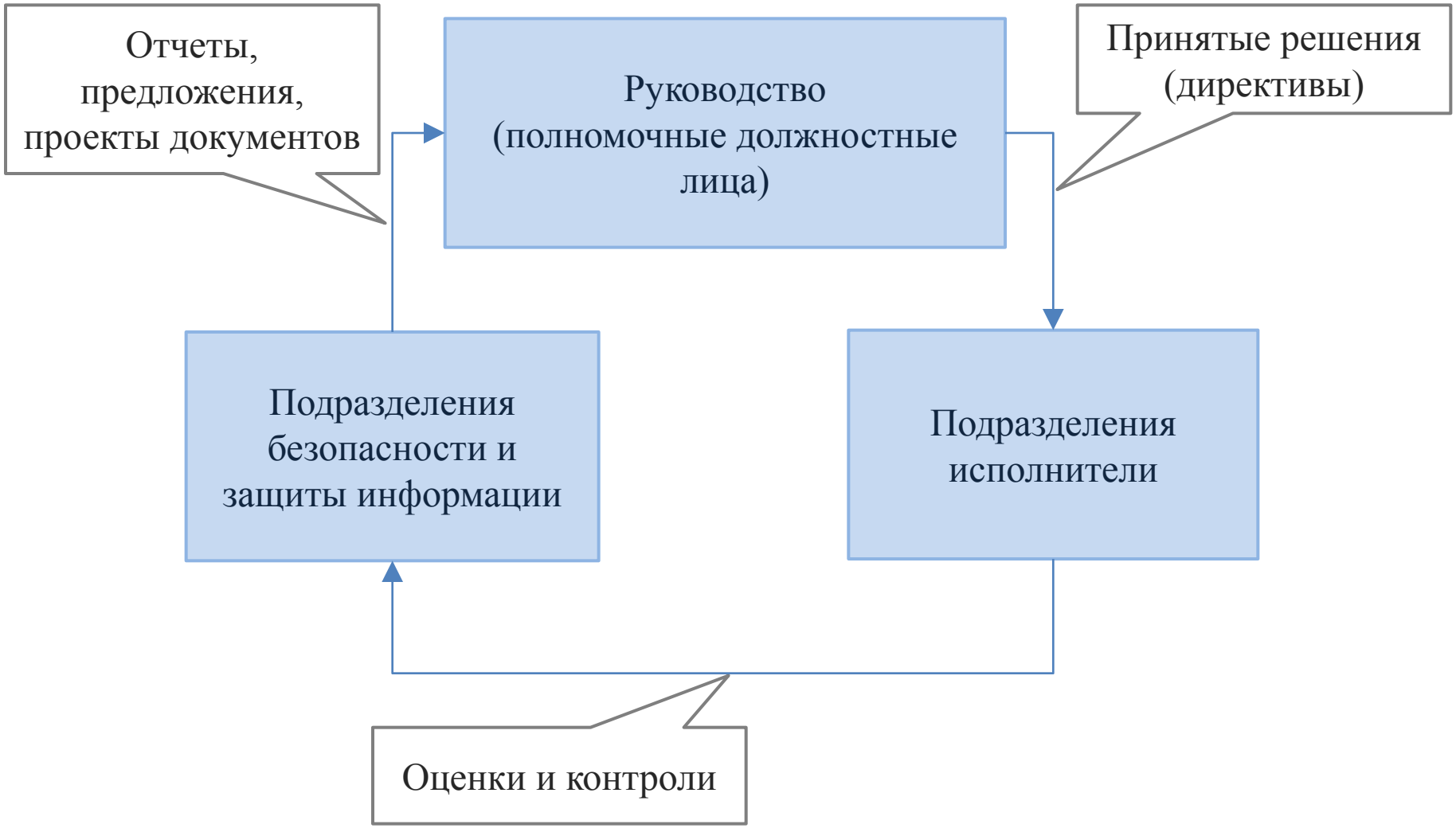
Стороны – участники процессов функционирования систем КОД или групповые роли, применяемые в современной СОИБ

Участники процессов управления	Определение
1. Потребитель услуг	Сторона (подразделения), использующая услуги системы КОД
2. Провайдер услуг	Сторона (подразделение), отвечающая за доступность предоставляемых услуг системы КОД
3. Контролер	Сторона (подразделение), ответственная за проведение оценки качества предоставляемых услуг
4. Распорядитель услуг	Сторона (подразделение), определяющая порядок и правила предоставления услуг системы КОД, а также регламентирующая отношения между *Провайдером* и *Потребителями*
5. Оператор связи	Сторона, предоставляющая услуги подключения и транспорт доставки услуг от *Провайдера услуг* к *Потребителям*

Способы управления процессами обеспечения ИБ или что влияет на организацию процессов управления ИБ?



Директивное управление



Оперативно-тактическое управление

Правила оперативно-тактического управления

Правило №1

Все участники информационных процессов должны рассматриваться как часть СОИБ.

В качестве примера можно привести ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ в которой состав организационной основы (компоненты) СОИБ РФ определяется участниками (сторонами), начиная от Президента РФ и заканчивая гражданами РФ.

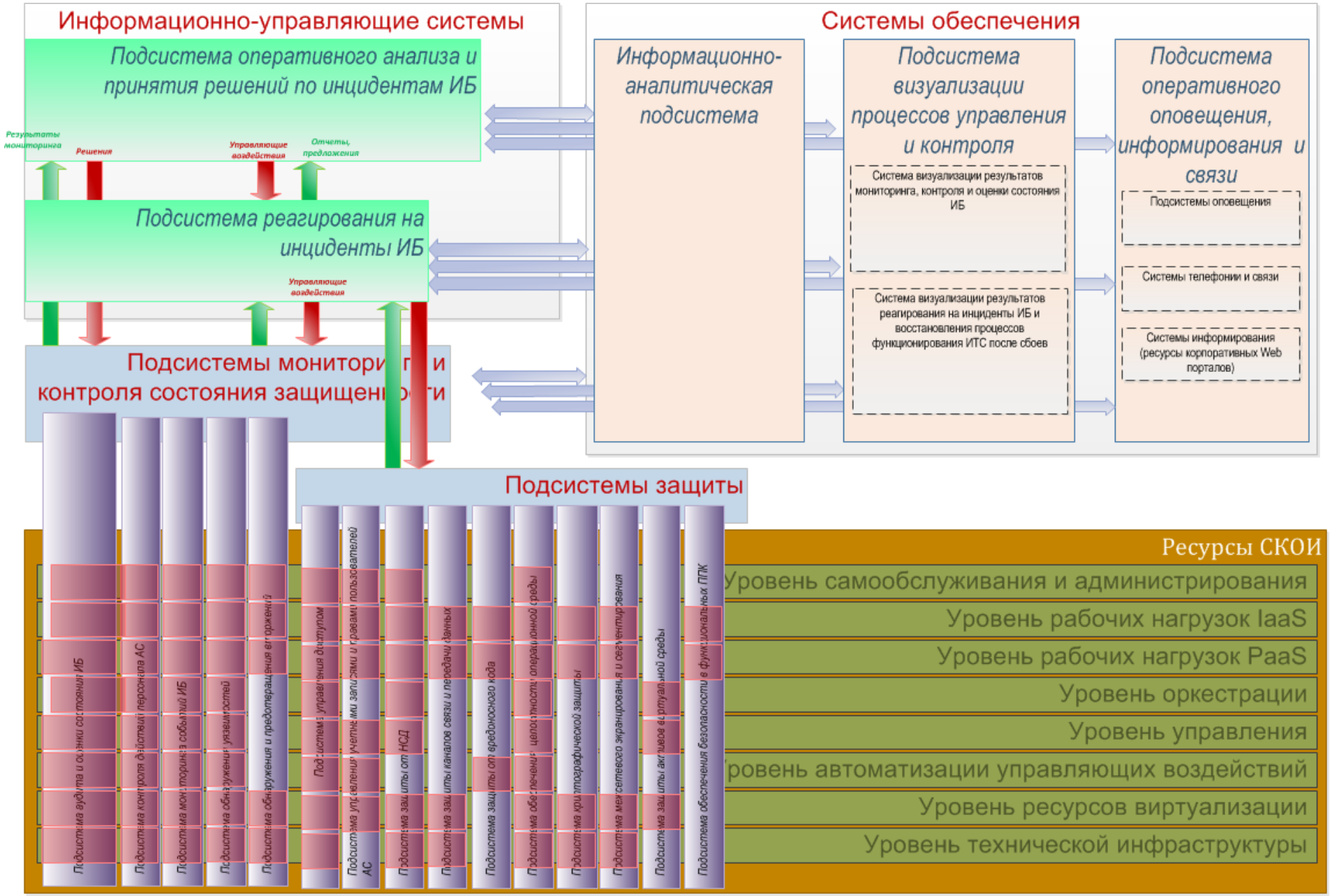
Правило №2

Должна быть четко управляющая роль подразделений безопасности и защиты информации.

При этом - важным аспектом является тот факт, что в случае наделения подразделений безопасности и защиты информации полномочиями оперативного управления, должно быть определено и подразделение контроля за деятельностью сотрудников подразделений безопасности и защиты информации. При этом данное подразделение должно быть независимо от руководства контролируемых им подразделений безопасности.

(Это подразделения внутреннего контроля в части ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ).

Обобщенная модель СОИБ (оперативно-тактический уровень)



Характеристика информационно-управляющих систем

Информационно-управляющая система определяется как формальная система предназначенная для принятия управленческих решений.

В СОИБ выделяются три вида информационно-управляющих систем:

- **ИУС стратегического планирования.**

Обеспечивают процессы принятия решений в области ИБ, ориентированные на достижение бизнес целей организации в целом.

- **ИУС управленческого контроля.**

Данный вид систем предназначен для организации процессов управления конфигурациями, обновления, изменениями, обеспечения непрерывности функционирования систем защиты.

- **ИУС оперативный контроль.**

Данный вид управляющих систем относиться системам реального времени, обеспечивающих непрерывность процессов функционирования программных и аппаратных и программно-аппаратных систем и средств защиты информации.

Состав информационно-управляющих систем

В состав системы управления и мониторинга ИБ входят следующие информационно – управляющие системы:

– **Подсистема оперативного анализа и принятия решений по инцидентам ИБ** (ИУС управленческого контроля)

– **Подсистема реагирования на инциденты ИБ** (ИУС оперативный контроль)

Характеристика системы мониторинга ИБ

Система мониторинга ИБ предназначена для контроля функционирования информационных систем (ИС), систем передачи данных, средств и механизмов защиты.

Система мониторинга ИБ обеспечивает автоматизацию процессов оперативного контроля, первичного анализа и оценки состояния ИБ, что в свою очередь необходимо для решения задач своевременного реагирования на угрозы ИБ.

Состав системы, определяется следующими подсистемами:

- Подсистема аудита ИБ;
- Подсистема контроля действий персонала ИС;
- Подсистема мониторинга событий ИБ;
- Подсистема обнаружения уязвимостей;
- Подсистема обнаружения и предотвращения вторжений.

Характеристика системы защиты информации

Состав система защиты информации, определяется следующими подсистемами:

- Подсистема управления доступом;
- Подсистема управления учетными записями и правами пользователей АС;
- Подсистема защиты от НСД;
- Подсистема защиты каналов связи и передачи данных;
- Подсистема защиты от вредоносного кода;
- Подсистема обеспечения целостности операционной среды;
- Подсистема криптографической защиты;
- Подсистема межсетевого экранирования и сегментирования ;
- Подсистема защиты активов виртуальной среды;
- Подсистема обеспечения безопасности в функциональных ППК.

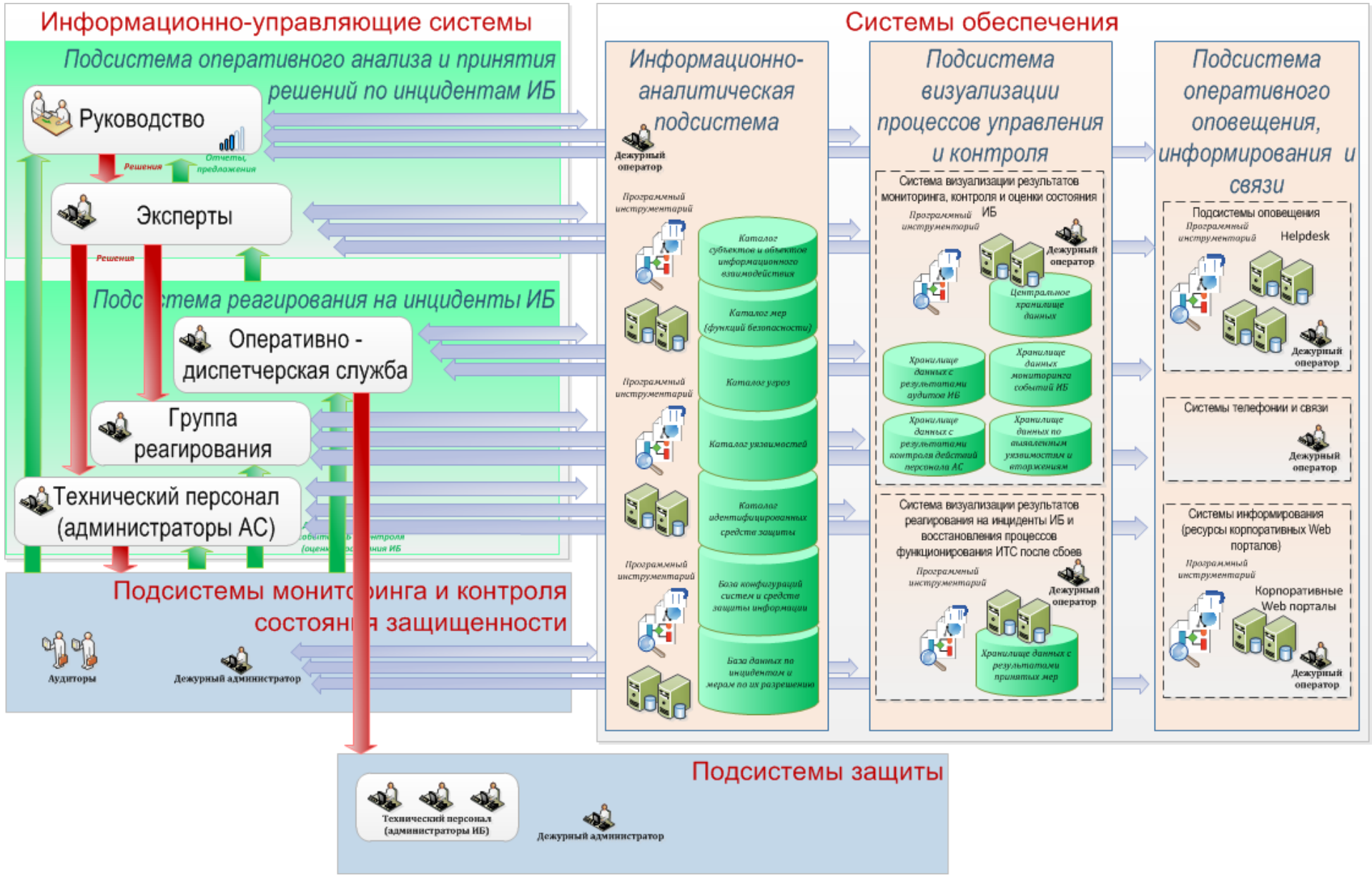
Система обеспечения

Система обеспечения как необходимый компонент автоматизации РЕШЕНИЯ ЦЕЛЕВЫХ ЗАДАЧ И ОБЕСПЕЧЕНИЯ ОПЕРАТИВНОСТИ ВЗАИМОДЕЙСТВИЯ.

Состав системы:

- Информационно-аналитическая подсистема
  - Подсистема визуализации
    - Подсистема оповещения, информирования и связи

Архитектура основных систем центра управления и мониторинга ИБ



Иерархия центров управления и мониторинга ИБ

ЧТО МЫ ИМЕЕТ КАК РЕЗУЛЬТАТ СОЗДАНИЯ ЦЕНТРАЛИЗОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ИБ?

1. *ИНФОРМАЦИОННО-УПРАВЛЯЮЩУЮ СИСТЕМУ. ОБЕСПЕЧИВАЮЩУЮ УПРАВЛЕНИЯ РИСКАМИ, ПРОБЛЕМАМИ, ИНЦИДЕНТАМИ ИБ;*

2. *ЕДИНУЮ СИСТЕМУ МОНИРИНГА И КОНТРОЛЯ СОСТОЯНИЯ ЗАЩИЩЕННОСТИ АКТИВОВ ОРГАНИЗАЦИИ;*

3. *ЭФФЕКТИВНУЮ СИСТЕМУ УПРАВЛЕНИЯ КОНФИГУРАЦИЯМИ СРЕДСТВ (СИСТЕМ) ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ ФУНКЦИОНИРОВАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ, В ЧАСТИ ЗАЩИТЫ ОТ УГРОЗ ИБ.*

Спасибо за внимание !