КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Как построить реально работающую систему безопасности объекта КИИ?

Николай Домуховский
ООО «УЦСБ»

Как построить неработающую СБОКИИ?

Подскажите список средств, закрывающих требования 239-го приказа для ЗОКИИ 3-й категории значимости…

Как построить неработающую СБОКИИ?

Подскажите список средств, закрывающих требования 239-го приказа для ЗОКИИ 3-й категории значимости…

Вот, пожалуйста: список_СрЗИ.xlsx

Как построить неработающую СБОКИИ?

Подскажите список средств, закрывающих требования 239-го приказа для ЗОКИИ 3-й категории значимости…

Вот, пожалуйста: список_СрЗИ.xlsx

Как построить неработающую СБОКИИ?

Подскажите список средств, закрывающих требования 239-го приказа для ЗОКИИ 3-й категории значимости…

Вот, пожалуйста: список_СрЗИ.xlsx

СБОКИИ. Общая структура

Приказ №235

Система безопасности объекта КИИ

Силы

Подразделения, ответственные за безопасность
Подразделения, эксплуатирующие ЗОКИИ
Подразделения, обслуживающие ЗОКИИ

Организационно-распорядительные документы

Цели, задачи, правила и процедуры обеспечения безопасности значимого объекта

Средства

Программные и программно-аппаратные СрЗИ

Приказ №239

Жизненный цикл СБОКИИ

Категорирование ОКИИ

- Создание комиссии
- Проведение категорирования
- Оформление акта
- Направление результатов во ФСТЭК России

Создание СБОКИИ

- Создание сил СБОКИИ
- Создание средств СБОКИИ
- Разработка ОРД

Функционирование СБОКИИ

Совершенствование

- Анализ функционирования СБОКИИ
- Предложения по совершенствованию
- Оценка руководства

Планирование

- Мероприятия по обеспечению функционирования СБОКИИ
- Мероприятия по обеспечению безопасности ОКИИ

Мониторинг и контроль

- Внутренний контроль
- Государственный контроль

Реализация

- Реализация мероприятий по обеспечению функционирования СБОКИИ
- Реализация (внедрение) мероприятий по обеспечению безопасности ОКИИ

Установление требований

Разработка мер

Внедрение мер

Приказ 239 в числах

19 **мероприятий** по обеспечению безопасности объектов КИИ описывает приказ 239

17 **групп мер** по обеспечению безопасности объектов КИИ описывает приказ 239, из которых 15 должны быть реализованы в ОКИИ 3-й категории значимости

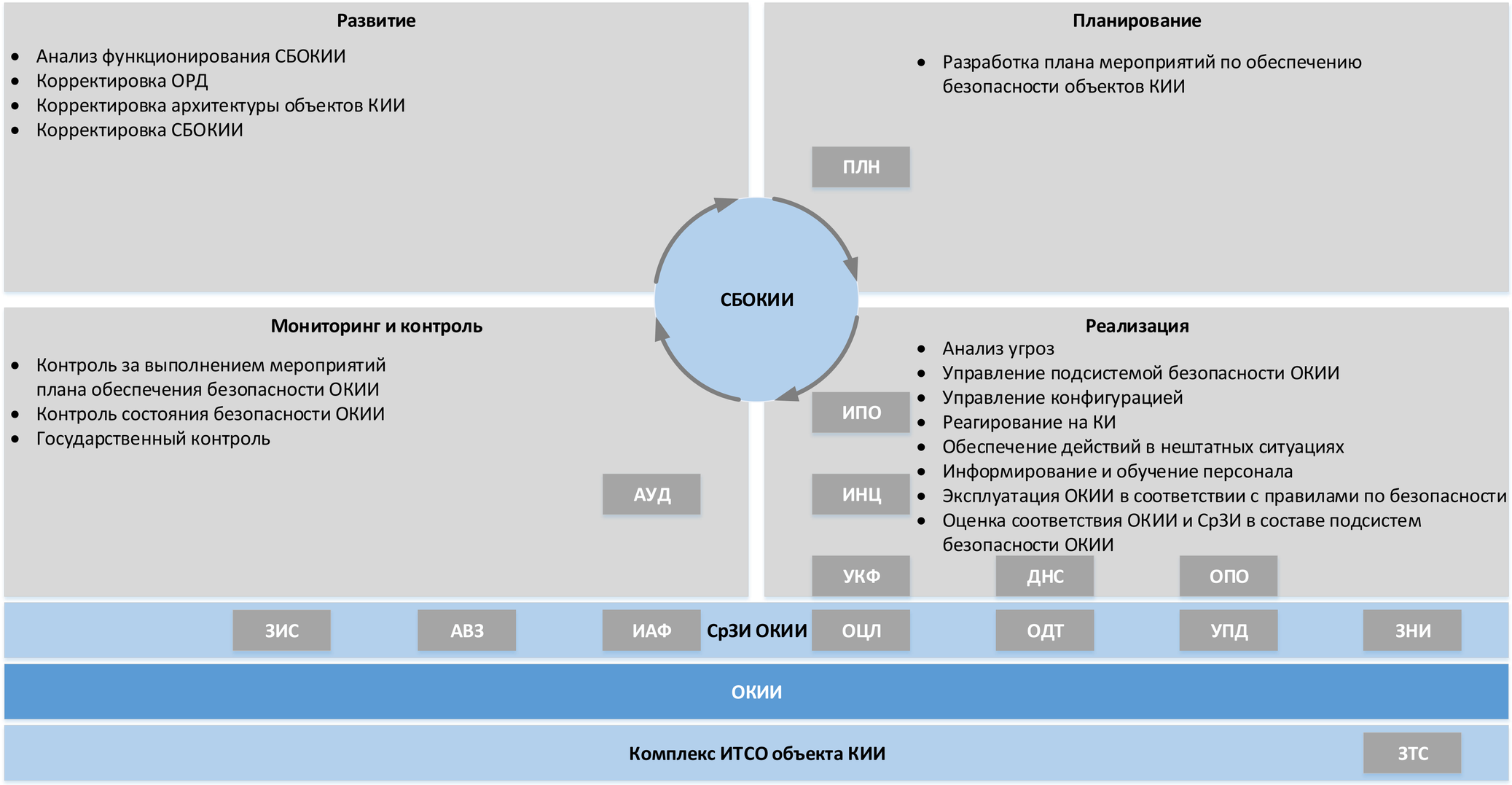
10 **мероприятий** относятся к разработке и внедрению мер защиты объектов КИИ и еще 4 к стадии вывода ОКИИ из эксплуатации

7 **групп мер** реализуются с применением технических средств защиты информации (направленных на нейтрализацию актуальных угроз ИБ) и еще одна – с применением инженерно-технических средств охраны

5 **мероприятий** относятся к обеспечению функционирования СБОКИИ (должны выполняться постоянно)

7 **групп мер** детализируют мероприятия, относящиеся к обеспечению функционирования СБОКИИ (фактически, содержат требования к организации работы сил СБОКИИ)

Функциональная структура СБОКИИ



Силы СБОКИИ. Один в поле не воин

Руководитель субъекта КИИ

- Создает СБОКИИ
- Определяет состав сил и функции участников
- Назначает подразделение по безопасности
- Утверждает планы и результаты контроля

Подразделение по безопасности

- Анализ угроз
- Реализация требований
- Реализация организационно-технических мер
- Реагирование на инциденты
- Оценка соответствия
- Совершенствование СБОКИИ

Подразделение, эксплуатирующее ОКИИ

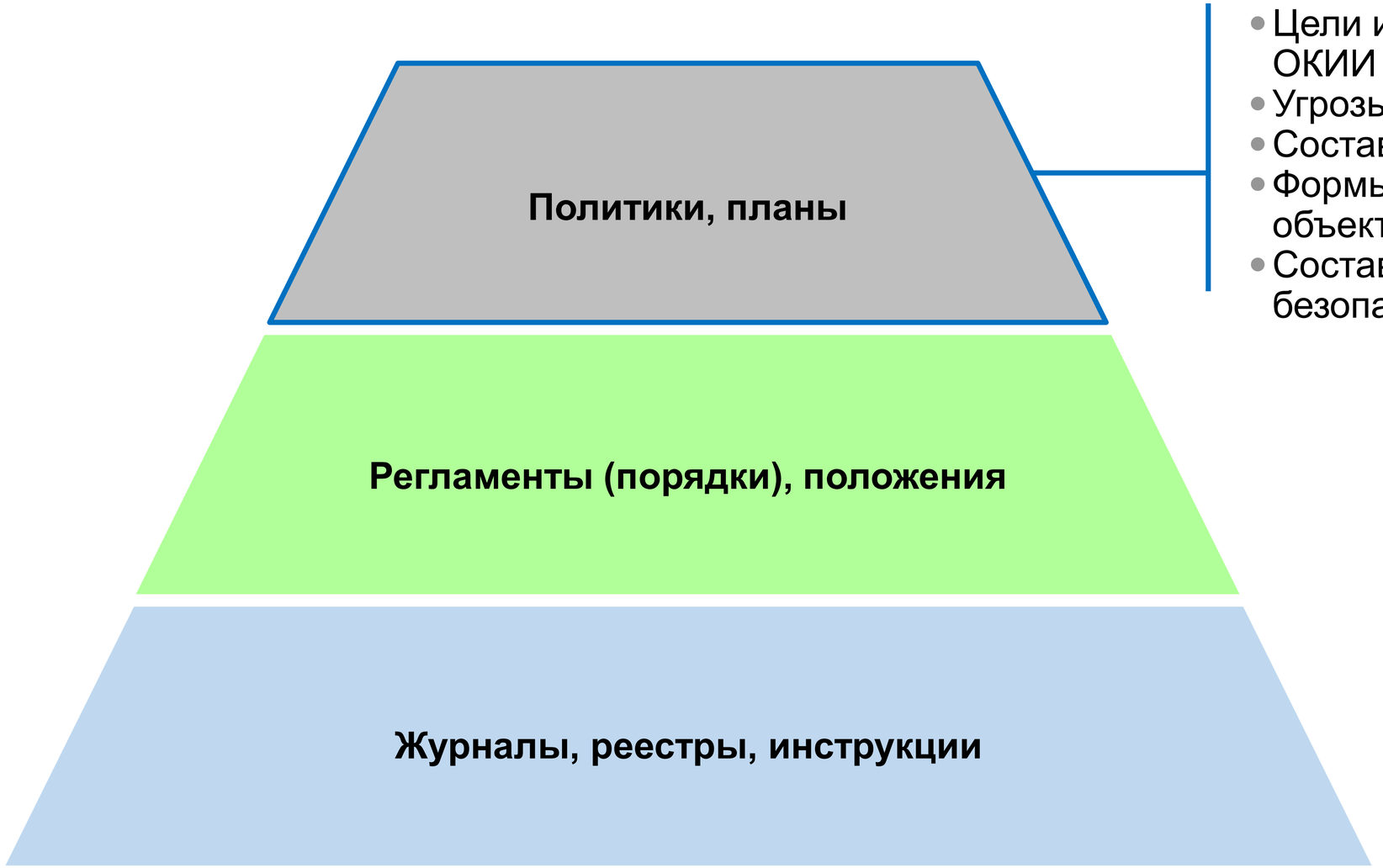
- Эксплуатация ОКИИ в соответствии с правилами по безопасности
- Участие в мероприятиях по: категорированию ОКИИ, планированию мероприятий, контролю за исполнением, подготовке предложений по совершенствованию

Подразделение, обеспечивающее функционирование

- Сопровождение ОКИИ в соответствии с правилами по безопасности
- Участие в мероприятиях по: категорированию ОКИИ, планированию мероприятий, контролю за исполнением, подготовке предложений по совершенствованию

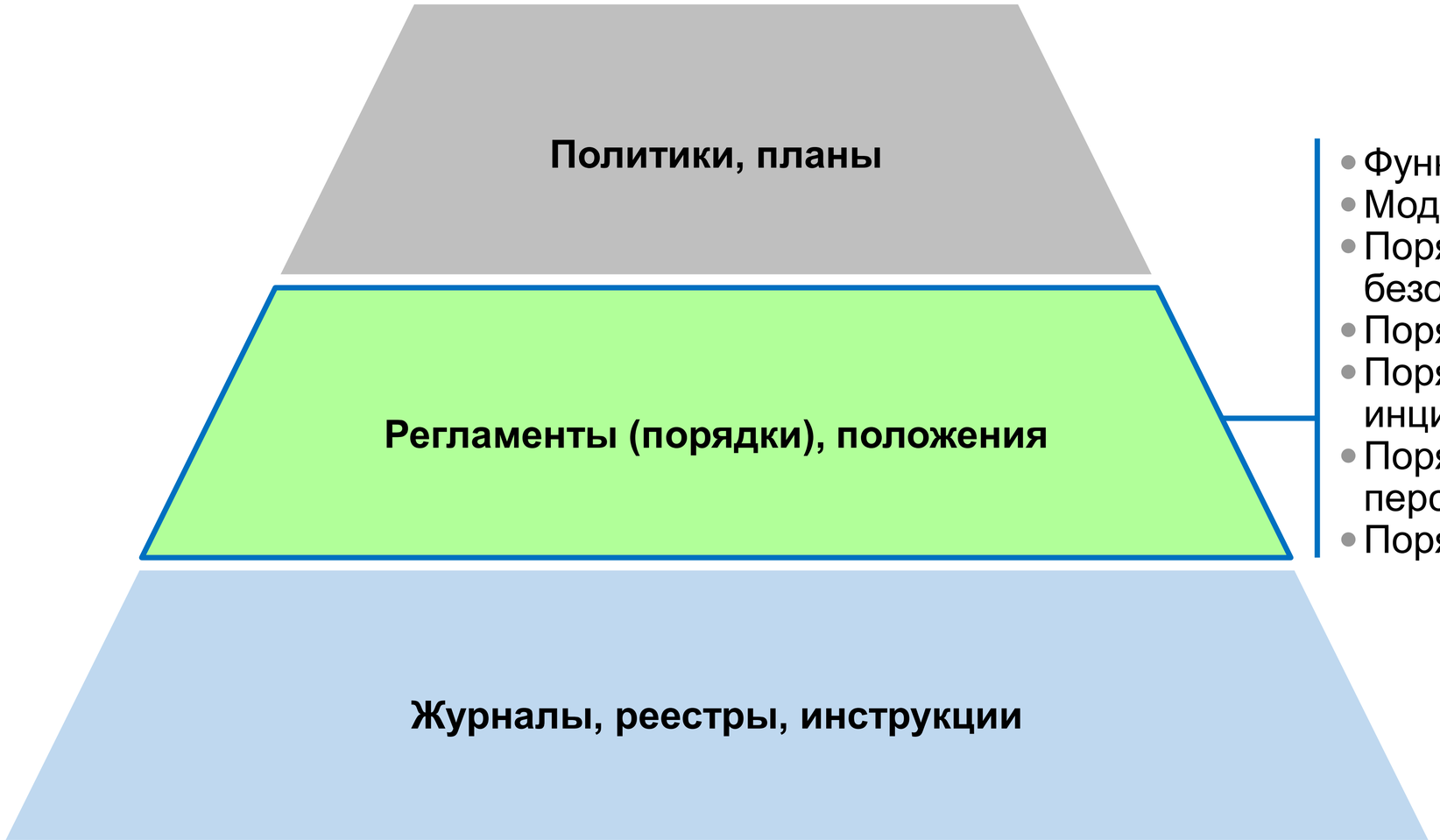
Приказ 235 не определяет явно ответственных за мероприятия: управление СрЗИ, управление конфигурацией ОКИИ и действия в нештатных ситуациях. Конкретное распределение функций должно определяться в ОРД

Состав ОРД СБОКИИ



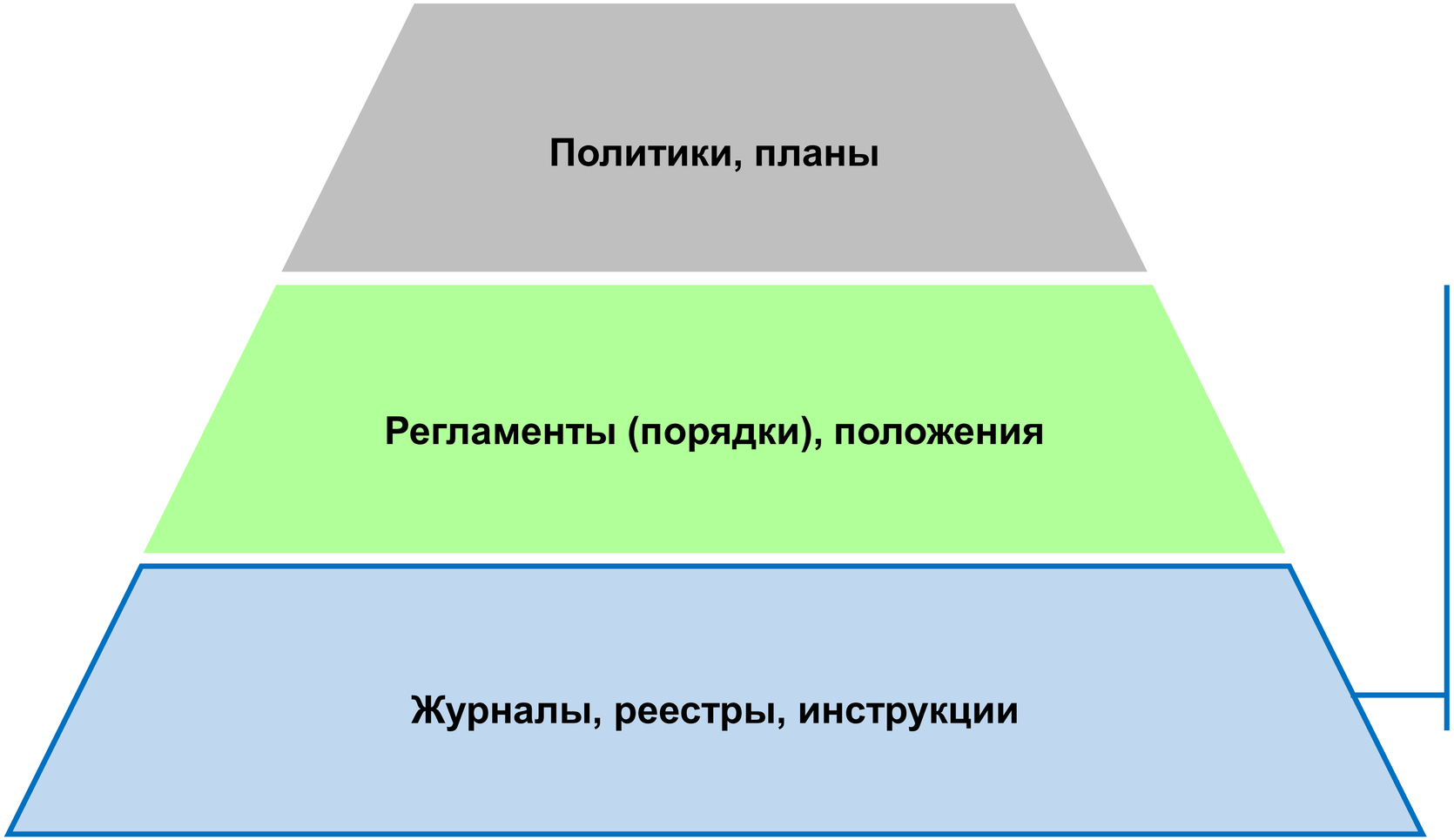
- Цели и задачи обеспечения безопасности ОКИИ
- Угрозы и нарушители (базовая модель)
- Состав и структура СБОКИИ
- Формы оценки соответствия значимых объектов
- Состав мероприятий по обеспечению безопасности ОКИИ

Состав ОРД СБОКИИ



- Функции участников СБОКИИ
- Модели угроз безопасности ОКИИ
- Порядок реализации мер по обеспечению безопасности ОКИИ
- Порядок проведения испытаний/приемки
- Порядок реагирования на компьютерные инциденты
- Порядок информирования и обучения персонала
- Порядок взаимодействия

Состав ОРД СБОКИИ



- Правила и процедуры безопасной работы в ОКИИ
- Действия при компьютерных инцидентах и иных нештатных ситуациях
- Документы, подтверждающие выполнение мероприятий по обеспечению безопасности ОКИИ (записи)

ОРД – цена нарушения

Работники, эксплуатирующие значимые объекты критической информационной инфраструктуры (пользователи), а также работники, обеспечивающие функционирование значимых объектов критической информационной инфраструктуры, должны выполнять свои обязанности на значимых объектах критической информационной инфраструктуры **в соответствии с правилами безопасности**, установленными организационно-распорядительными документами по безопасности значимых объектов (инструкциями, руководствами).

п. 15 Приказа 235

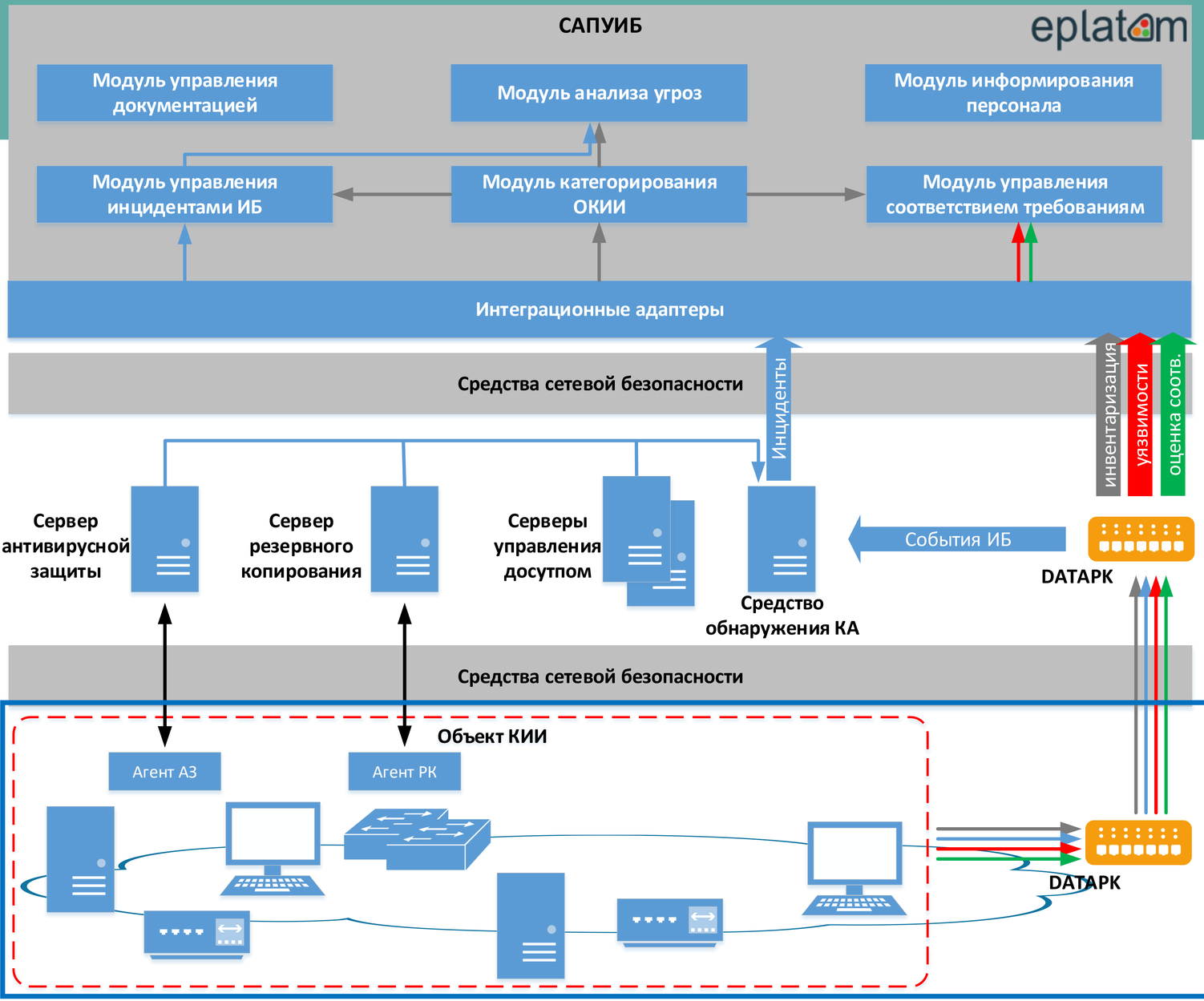
Рабочая (эксплуатационная) документация на значимый объект должна содержать:
…
правила эксплуатации программных и программно-аппаратных средств, в том числе средств защиты информации (**правила безопасной эксплуатации**).

П. 11.3 Приказа 239

Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации, - **наказывается …**

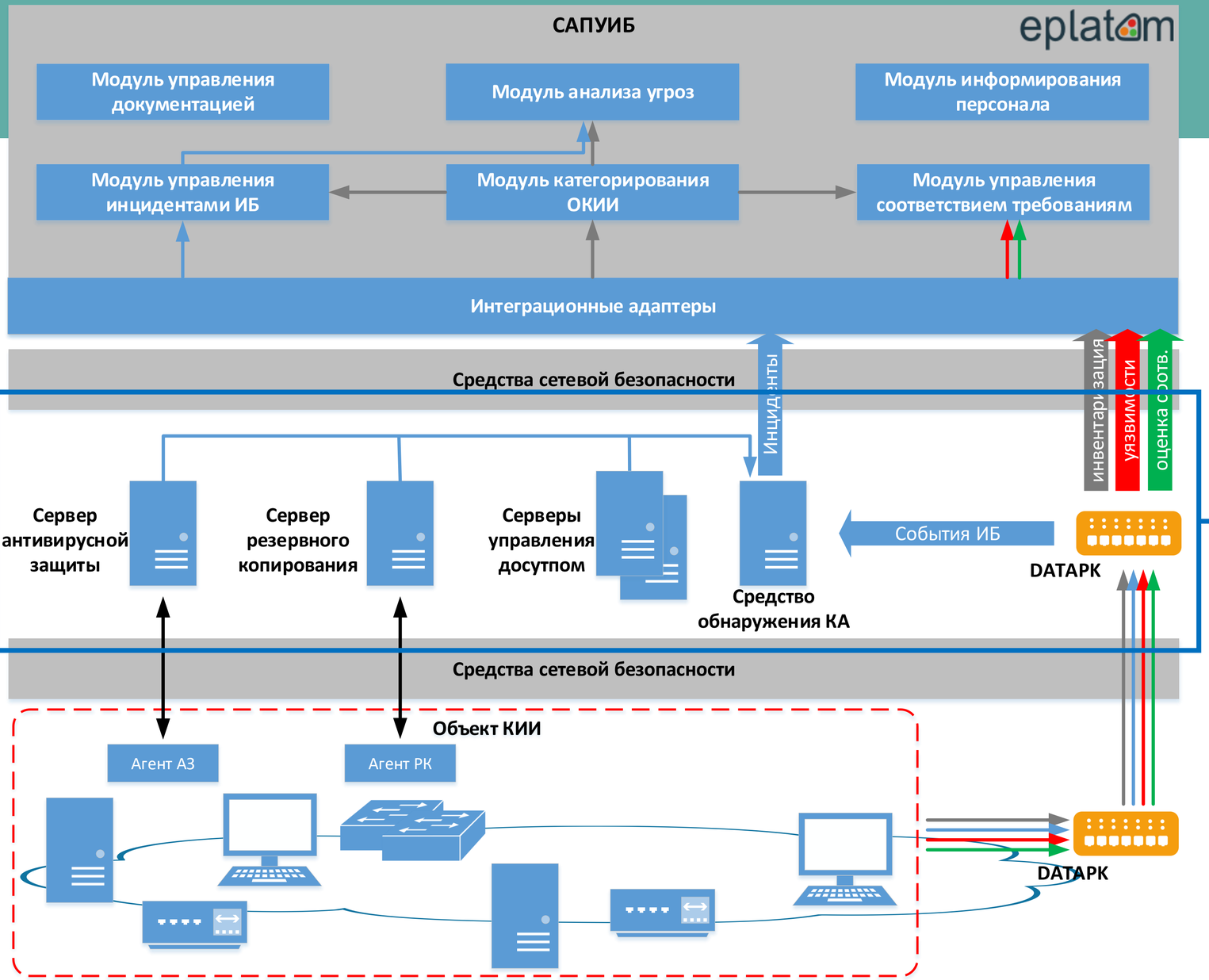
Ст. 273.1 п.3 УК РФ

СБОКИИ – техническая архитектура



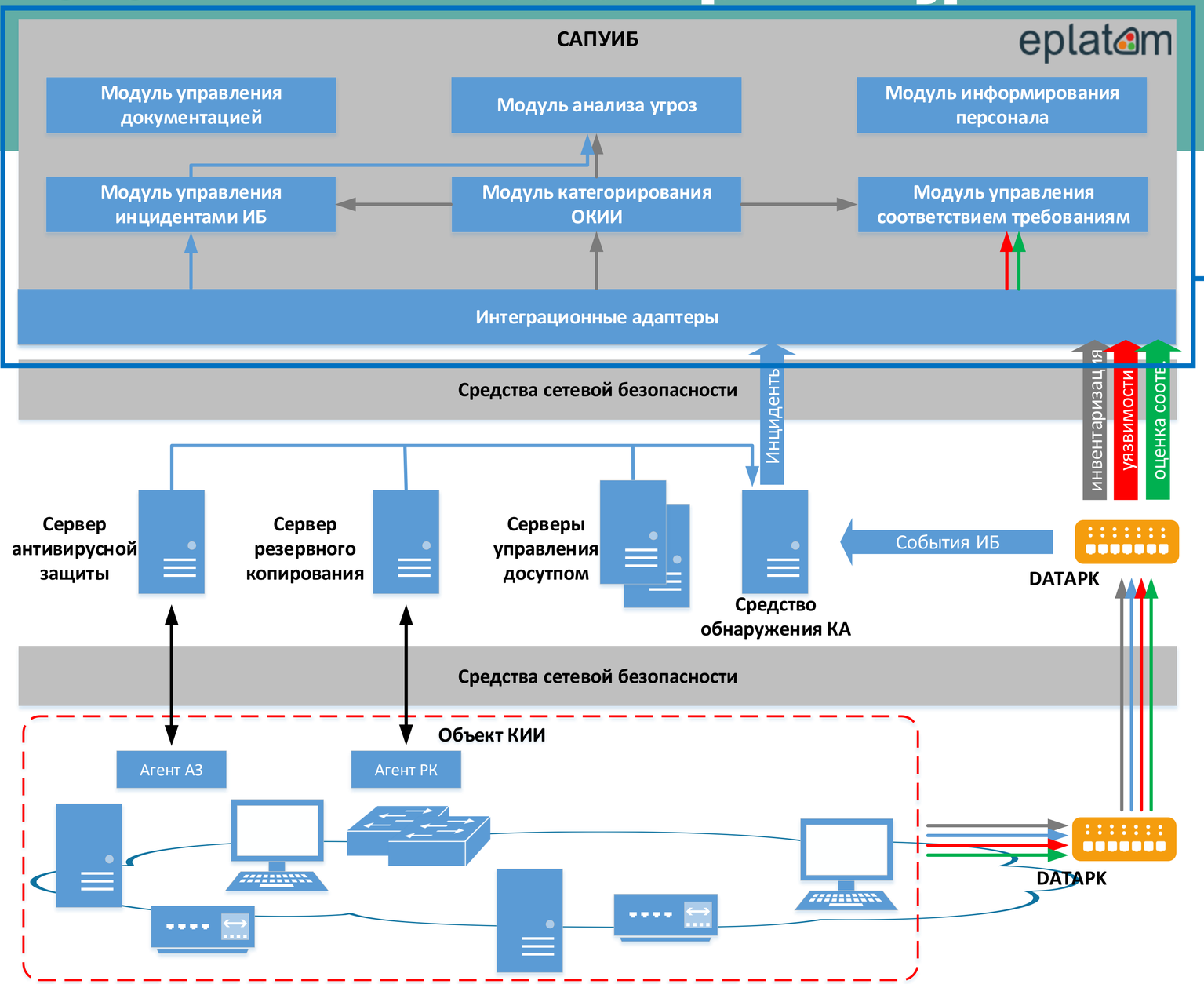
- ОКИИ выделяется в изолированный сегмент, в том числе от СБОКИИ
- Внутри изолированного сегмента преимущественно используются встроенные СрЗИ
- ПАК DATAPK обеспечивает безопасный сбор инвентаризационной информации, событий ИБ, сведений об уязвимостях и соответствию требованиям

СБОКИИ – техническая архитектура



- Основные технические средства СБОКИИ располагаются в выделенном сегменте ДМЗ ОКИИ
- В состав средств входят средства антивирусной защиты, резервного копирования, управления доступом (к СВТ, АСО и пр.), обнаружения компьютерных атак
- Для всех средств реализуется централизованное управление (мероприятие управление СрЗИ)

СБОКИИ – техническая архитектура



- САПУИБ на базе ПО ePlat4m реализует основные мероприятия СБОКИИ
- Слой интеграционных адаптеров обеспечивает получение данных от СрЗИ СБОКИИ: инвентаризационная информация, сведения об уязвимостях, соответствии требованиям и инцидентах ИБ

Как построить реально работающую систему безопасности объекта КИИ?

1

СБОКИИ – это не только технические средства
При создании СБОКИИ должны быть созданы все 3 компонента системы: силы, средства и ОРД

2

СБОКИИ – это не продукт, а процесс
Завершение внедрения мер СБОКИИ – только начало работы

3

СБОКИИ – общее дело
Помимо подразделения по безопасности в создании и функционировании СБОКИИ активное участие принимают: руководитель, подразделения, эксплуатирующие или сопровождающие ОК ИИ

4

ОРД СБОКИИ должны быть «живыми»
Если документы не выполняются надлежащим образом – это создает риски вплоть до уголовного преследования

5

Основные СрЗИ СБОКИИ – встроенные СрЗИ компонентов ОКИИ
Основные технические меры обеспечения безопасности ОКИИ наиболее эффективно реализуются встроенными СрЗИ

6

Мероприятия обеспечения безопасности ОКИИ рекомендуется автоматизировать
Использование решений DATAPK и ePlat4m с модулями автоматизации процессов СБОКИИ позволяет более эффективно реализовывать основные мероприятия СБОКИИ

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ

ndomukhovsky@ussc.ru
+7 343 379-98-34
www.ussc.ru