НПП “Гамма”

Меры по защите значимых объектов КИИ и функции центра ГосСОПКА. Как избежать дублирования функционала СЗИ?

Холодов Артём Владимирович

Директор департамента информационных технологий

ФГУП «НПП «Гамма»

Тел.: +7 (903) 110-28-49

e-mail: holodov@nppgamma.ru

2019 г.

Система безопасности значимого объекта критической информационной инфраструктуры

НПП "Гамма"

РД ФСТЭК России

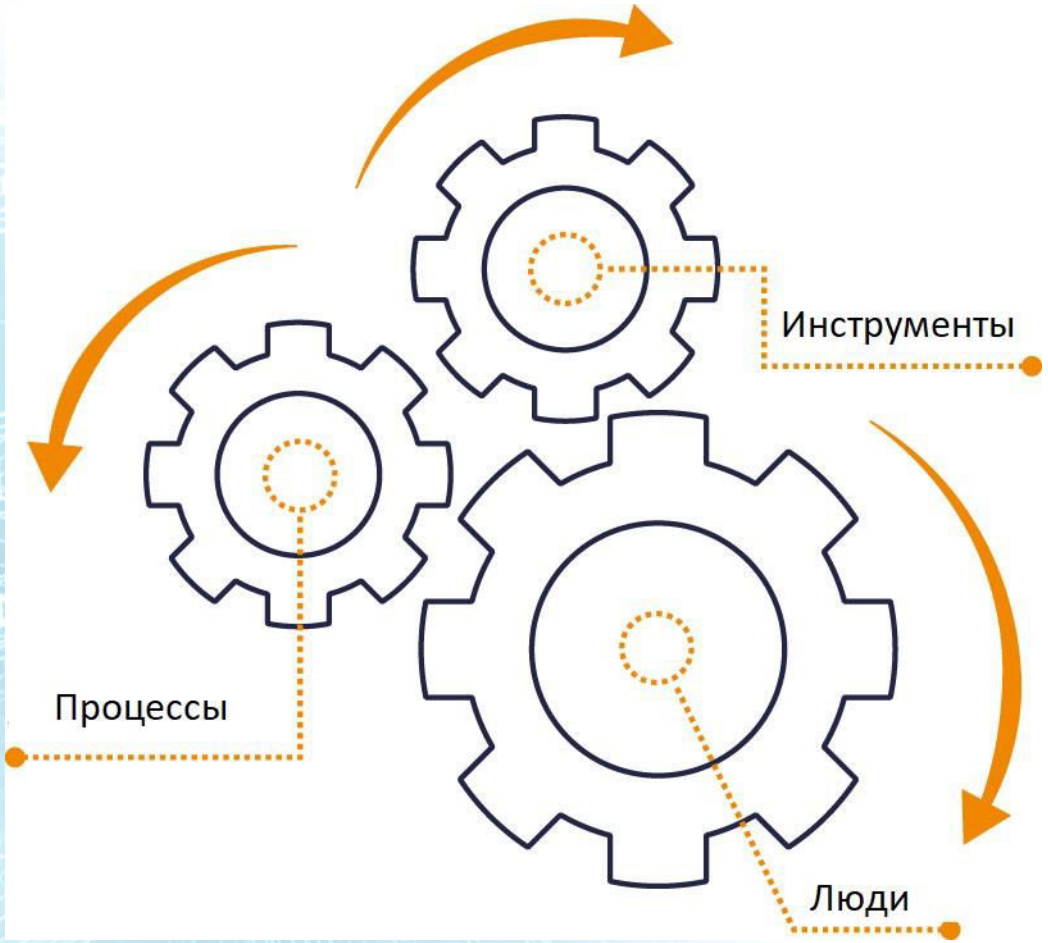
Требования по обеспечению безопасности значимых объектов КИИ Российской Федерации

- V. Аудит безопасности (АУД)
- XII. Реагирование на компьютерные инциденты (ИНЦ)
- XIV. Управление обновлениями программного обеспечения (ОПО)
- VII. Предотвращение вторжений (компьютерных атак) (СОВ)
- XIII. Управление конфигурацией (УКФ)
- XVII. Информирование и обучение персонала (ИПО)

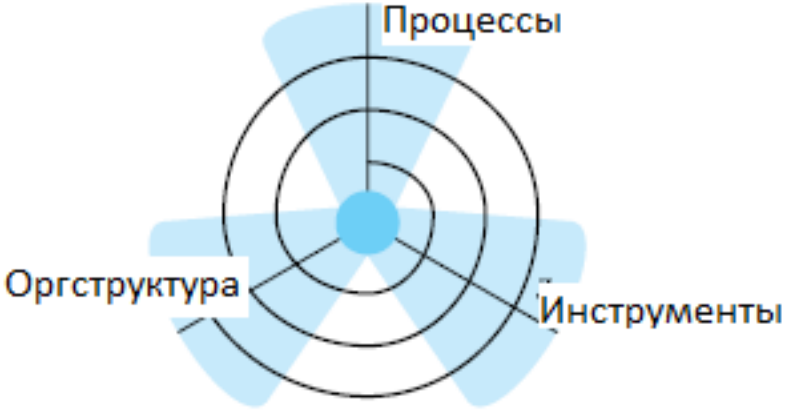
РД ФСБ России

Функции центра ГосСОПКА

Центр ГосСОПКА



!



Проектировать необходимо всё в комплексе.

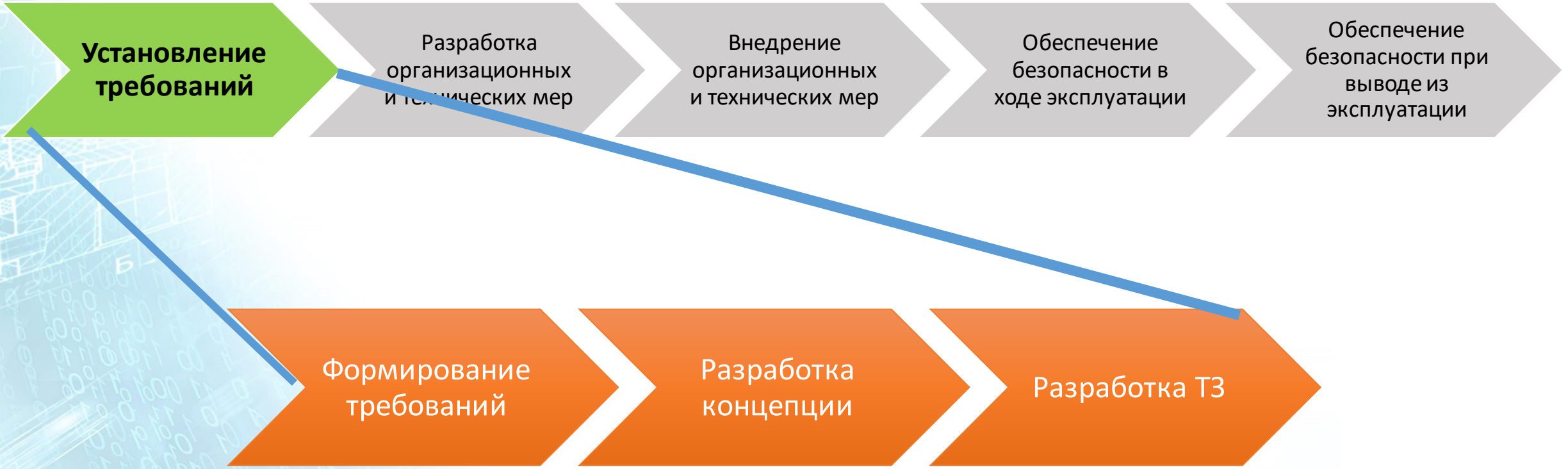
Итеративно.

С учетом особенностей объектов КИИ и системы защиты информации.

Когда ошибка стоит дороже всего?

НПП "Гамма"

Для значимых объектов, находящихся в эксплуатации , требования подлежат реализации в рамках модернизации или дооснащения подсистем безопасности с учетом имеющихся программ и планов



НПП "Гамма"

1. Сформулируйте цель

ЦЕЛЬ («зачем?»)

НПП "Гамма"

«… обеспечить выполнение требований регуляторов….»

НЕТ!!!

Целью обеспечения безопасности значимого объекта является

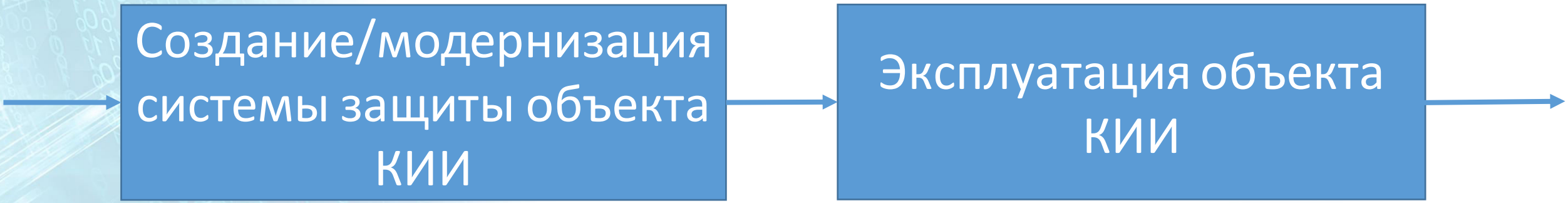
обеспечение его устойчивого функционирования

в проектных режимах работы в условиях реализации в отношении значимого объекта угроз безопасности информации.

(приказ ФСТЭК от 25.12.2017 № 239)

Устойчивость объекта (системы)

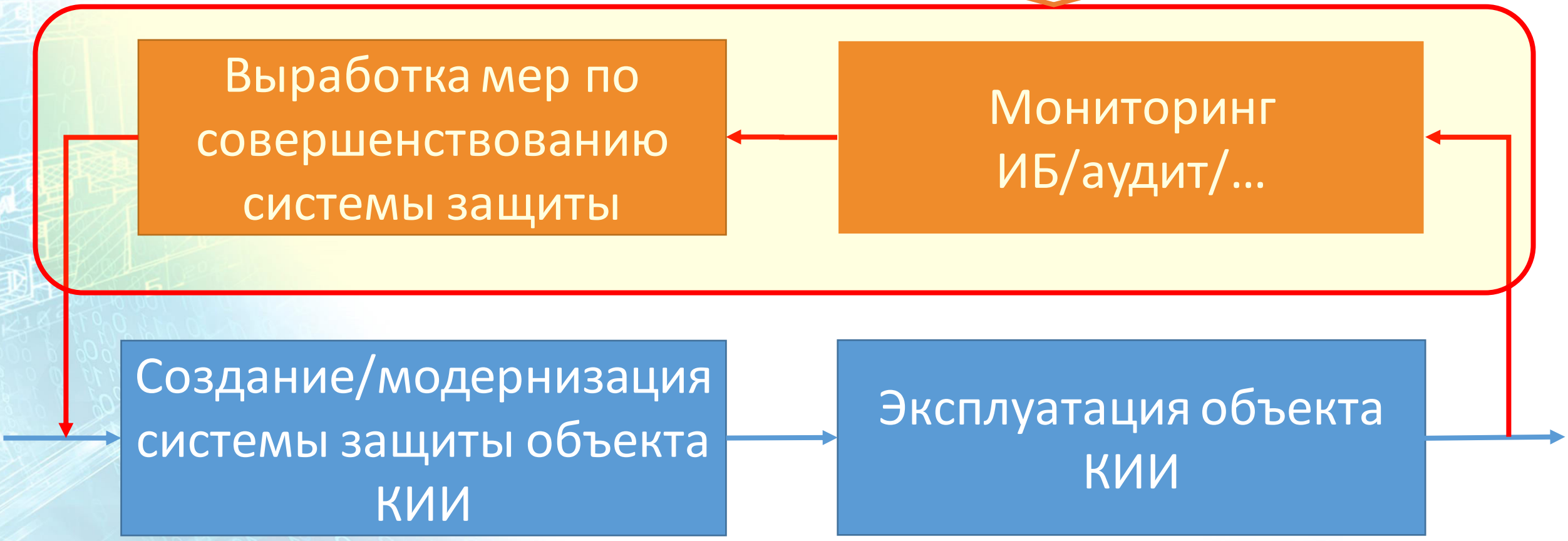
НПП "Гамма"



Устойчивость за счет обратной связи

НПП "Гамма"

Основные отличия в подходе к защите ОКИИ – в этом



НПП "Гамма"

2. Постройте функциональную модель

Как учесть все требования? Построение функциональной модели

НПП "Гамма"

Требования по обеспечению безопасности

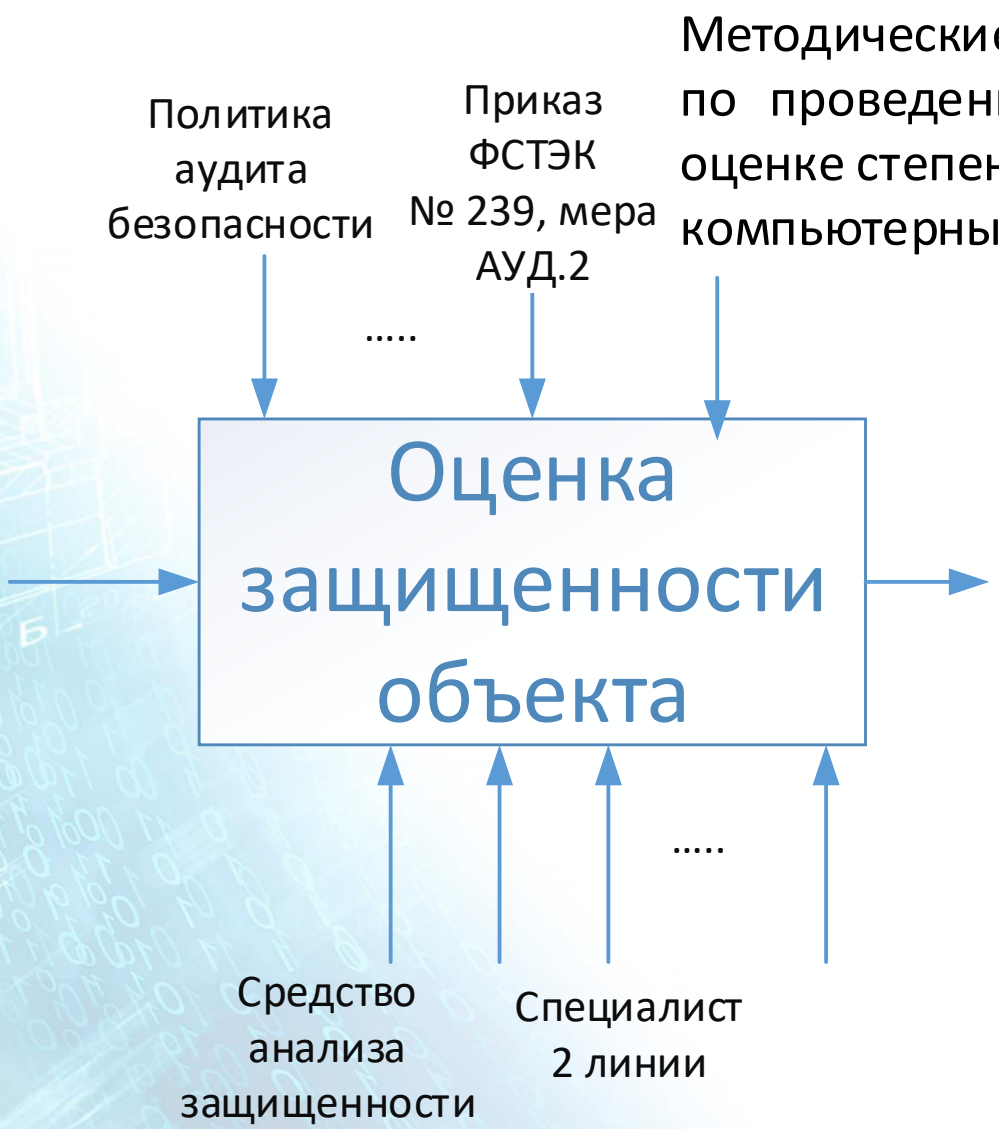
≠

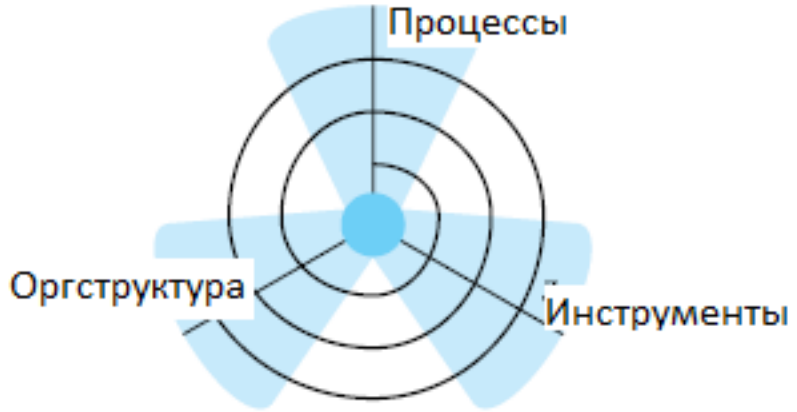
Требования к системе

(«что» ≠ «как»)

Построение функциональной модели

НПП "Гамма"





НПП "Гамма"

3. Проанализируйте взаимодействие подсистем

Структурный анализ

НПП "Гамма"

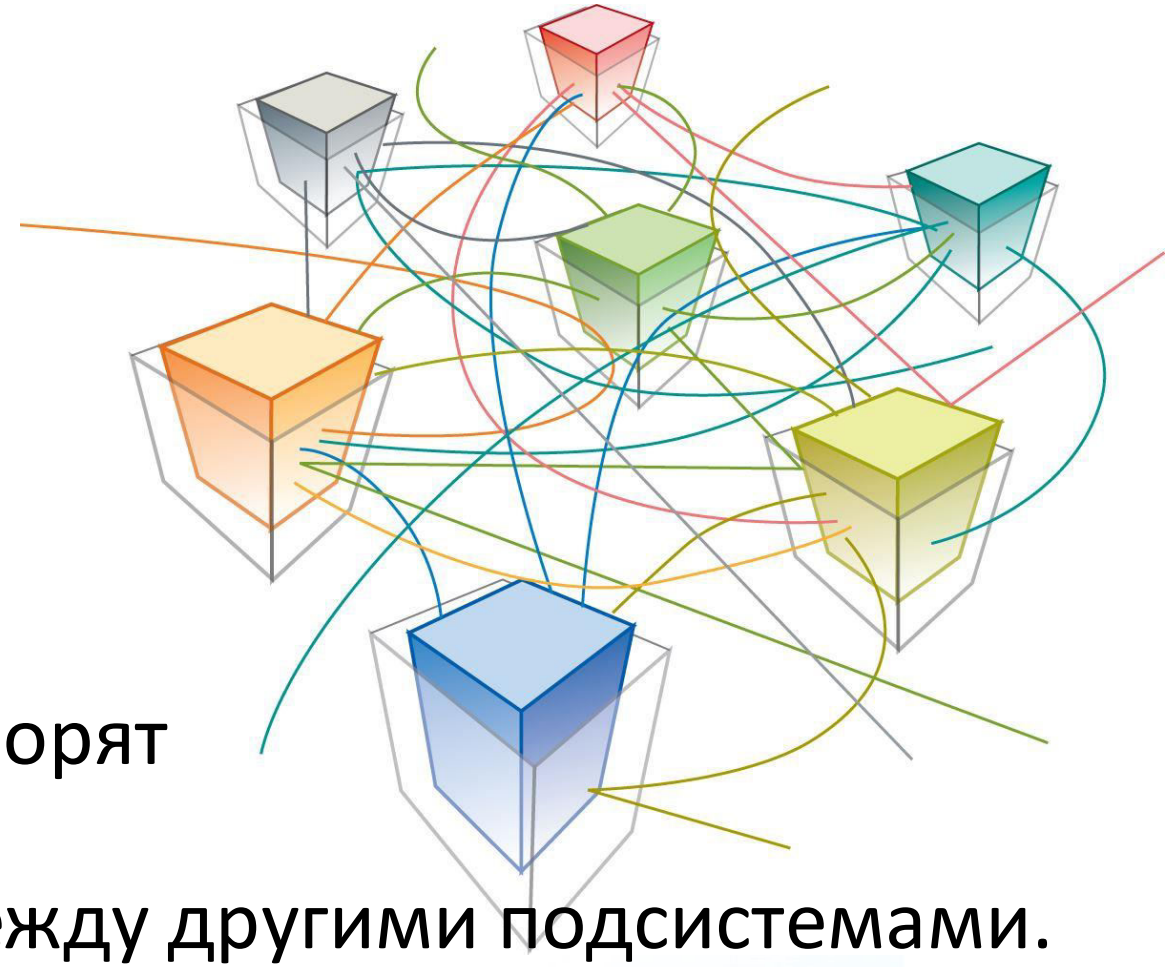
Матрица взаимодействий подсистем

	SIEM	Подсистема анализа защищенности	ITSM-система	СОВ	Подсистема инвентаризации
SIEM	+	+	+	+	+
Подсистема анализа защищенности	+	+			+
ITSM-система	+		+		+
СОВ	+		+	+	
Подсистема инвентаризации	+	+	+		+

Взаимодействие подсистем

НПП "Гамма"

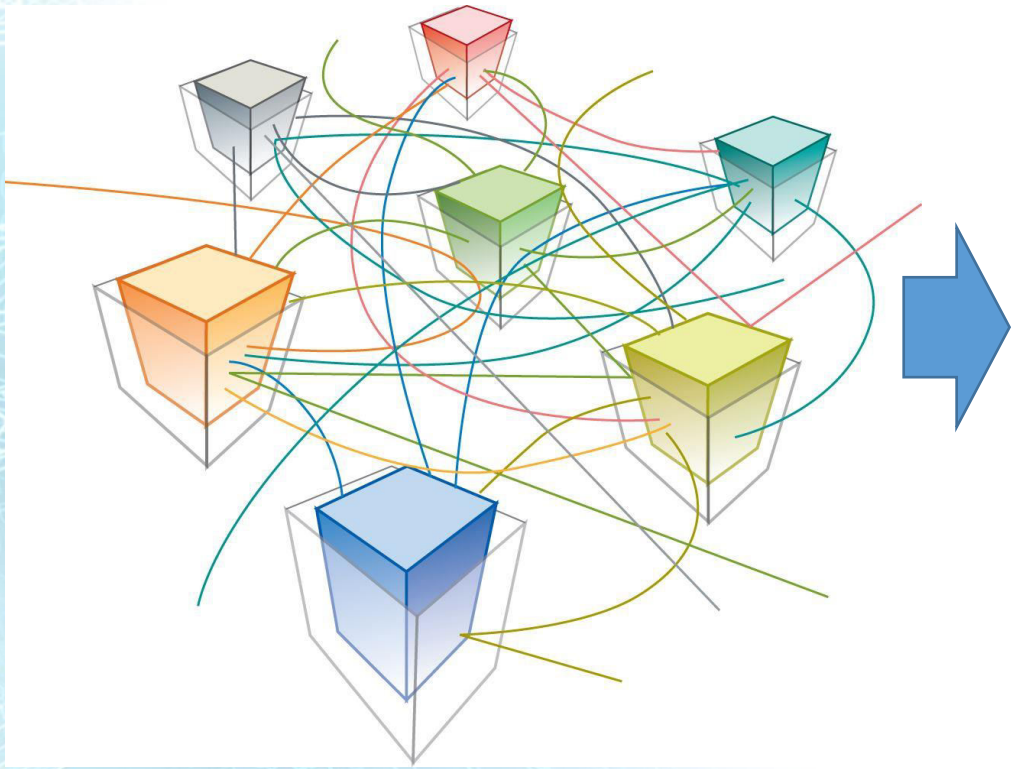
SIEM
ITSM
МСЭ
СОВ
АВЗ
НСД
САЗ
LM
….



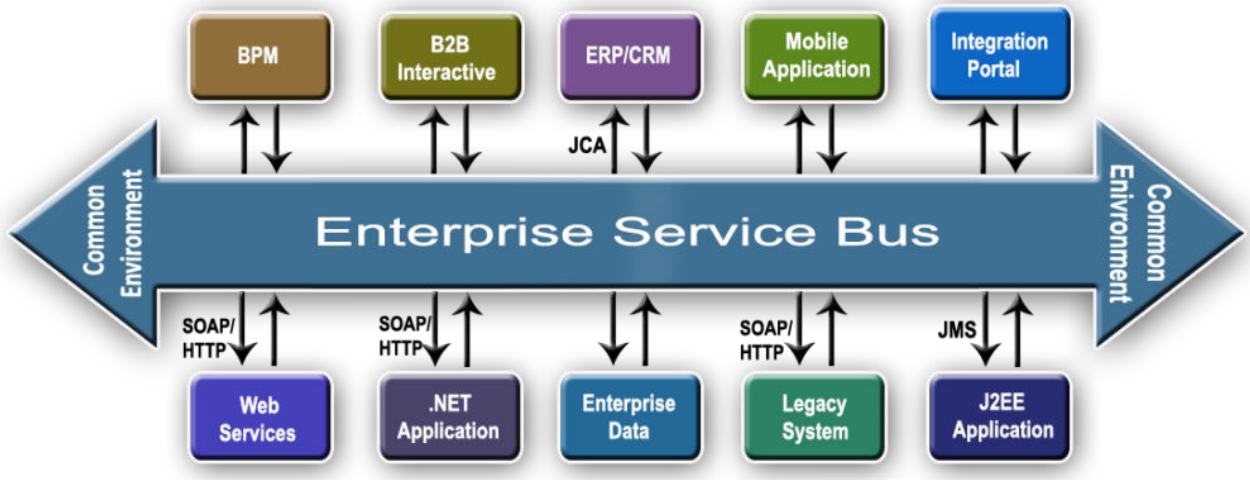
Про нормализацию событий говорят только применительно к SIEM…
Хотя актуально и при обмене между другими подсистемами.

Унифицированный формат обмена данными

НПП "Гамма"



Сервисная шина предприятия



В настоящее время идет работа над ГОСТ Р «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».
Это шаг к унификации обмена данными.

Рекомендации

НПП "Гамма"

Сформулируйте цель с которой создаете систему

Усильте внимание на этапе формирования концепции и требований к системе, подойдите системно

Центр ГосСОПКА – часть системы обеспечения безопасности ОКИИ, а не отдельная сущность

Проектируйте функции, а не только средства для их выполнения

Учитывайте взаимосвязи систем

Заключение

НПП "Гамма"

Эффект от хорошо спроектированной системы обеспечения безопасности с обратной связью – длительный.

С каждым днем польза от такой системы будет расти, а затраты – оптимизироваться.

НПП "Гамма"

Спасибо за внимание!

Холодов Артём Владимирович

Директор департамента информационных технологий

ФГУП «НПП «Гамма»

Тел.: +7 (903) 110-28-49

E-mail: holodov@nppgamma.ru