

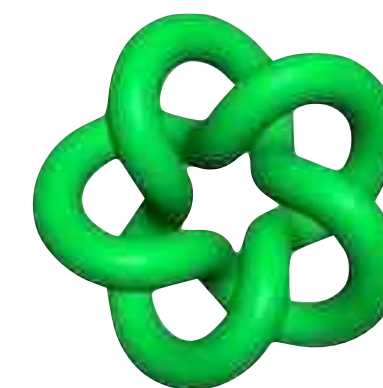
Чем пристальнее смотришь, тем меньше видишь

Мониторинг информационной безопасности
Промышленная кибербезопасность



30.09.2020

Код ИБ Онлайн - Безопасная среда



Алексей Комаров
<https://ZLONOV.ru>

Содержание

О чём будем говорить

Термины

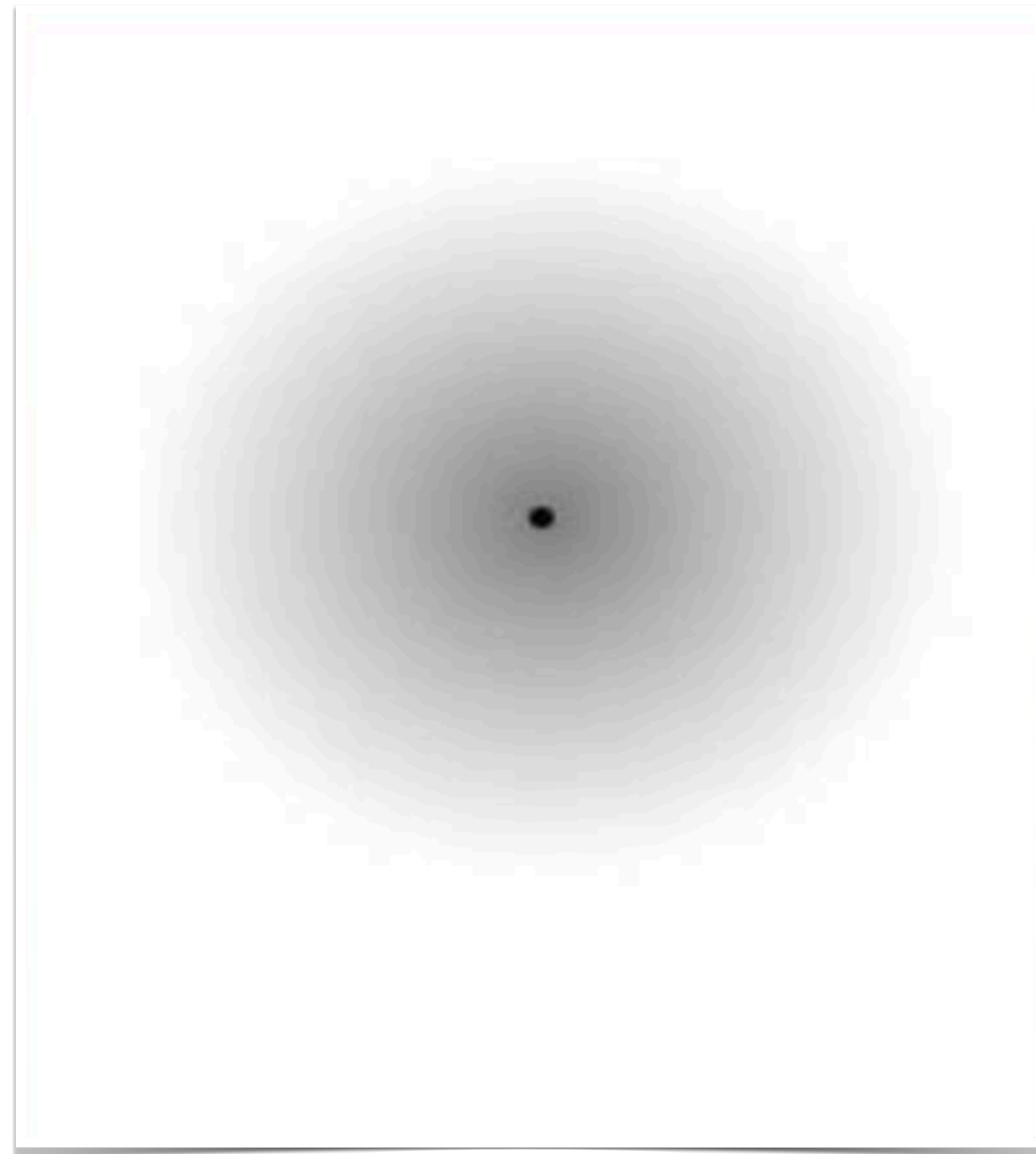
Новый ГОСТ по мониторингу ИБ

Влияние 187-ФЗ

Типовые ошибки

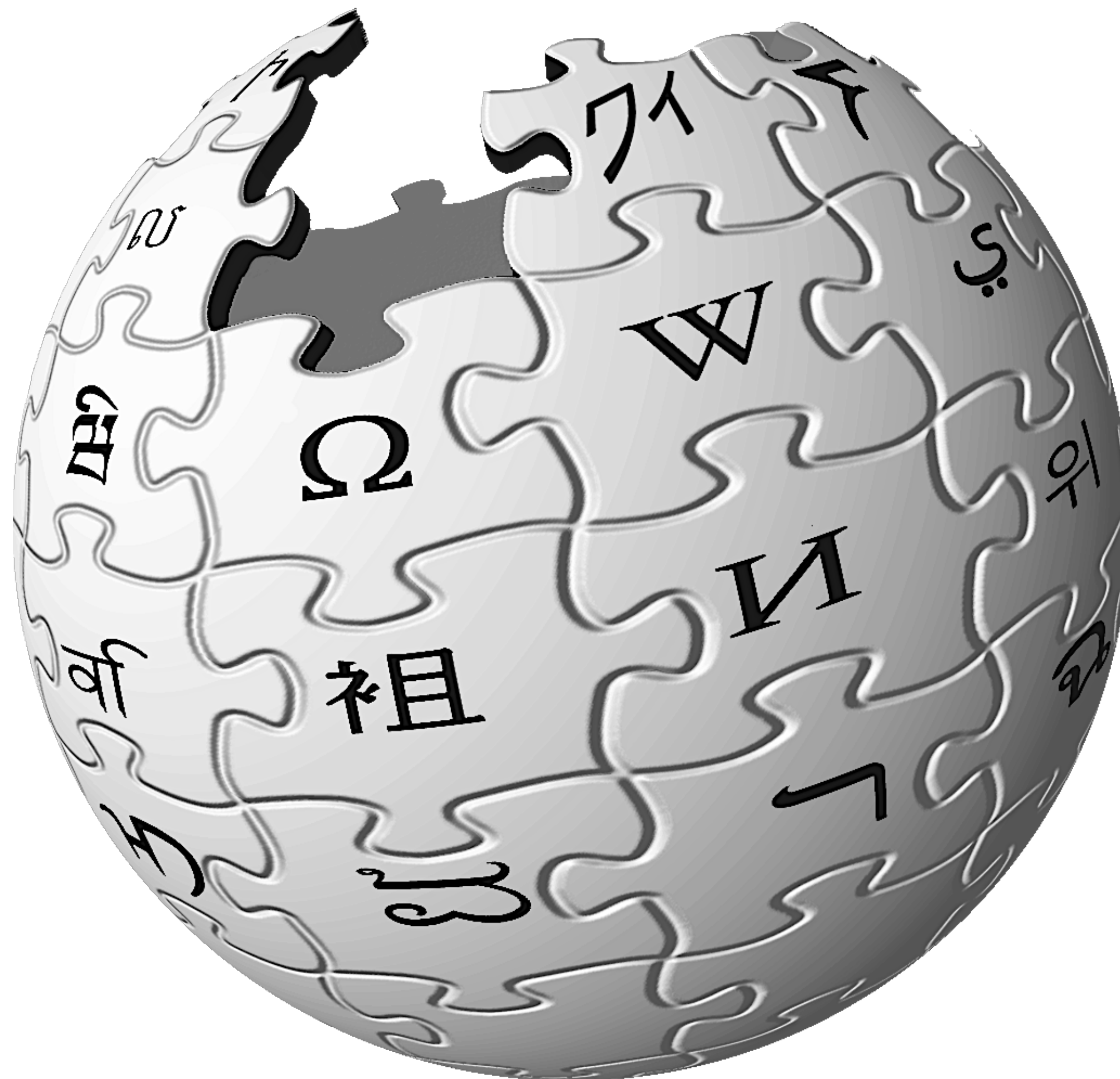
А может SOC?

Не забудьте про ГосСОПКА



В широком смысле слова

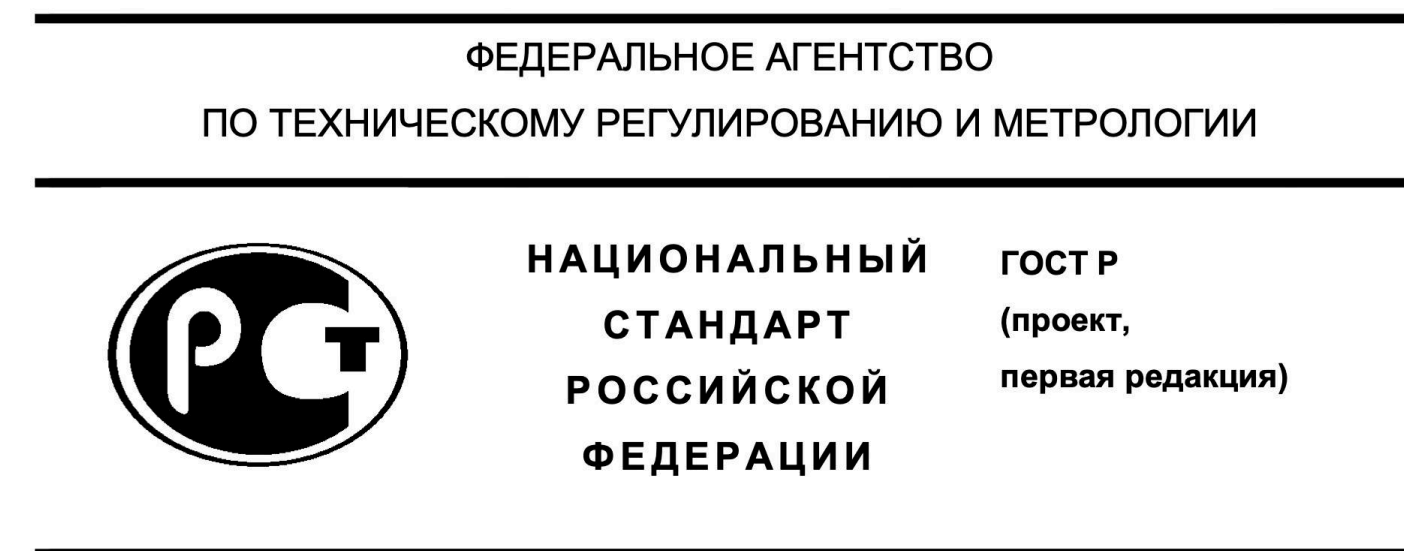
- Мониторинг — система **постоянного наблюдения** за явлениями и процессами, проходящими в окружающей среде и обществе, **результаты которого служат для обоснования управленческих решений** по обеспечению безопасности людей и объектов экономики. **В рамках системы наблюдения происходит оценка, контроль объекта, управление** состоянием объекта в зависимости от воздействия определённых факторов.



Мониторинг ИБ

Проект национального стандарта

- мониторинг информационной безопасности: **Процесс** постоянного **наблюдения** и **анализа** результатов **регистрации событий безопасности с целью** выявления **нарушений** безопасности информации, **угроз** безопасности информации и **уязвимостей** в информационных (автоматизированных) системах.
- *Проект ГОСТ Р «Защита информации. Мониторинг информационной безопасности. Общие положения»*

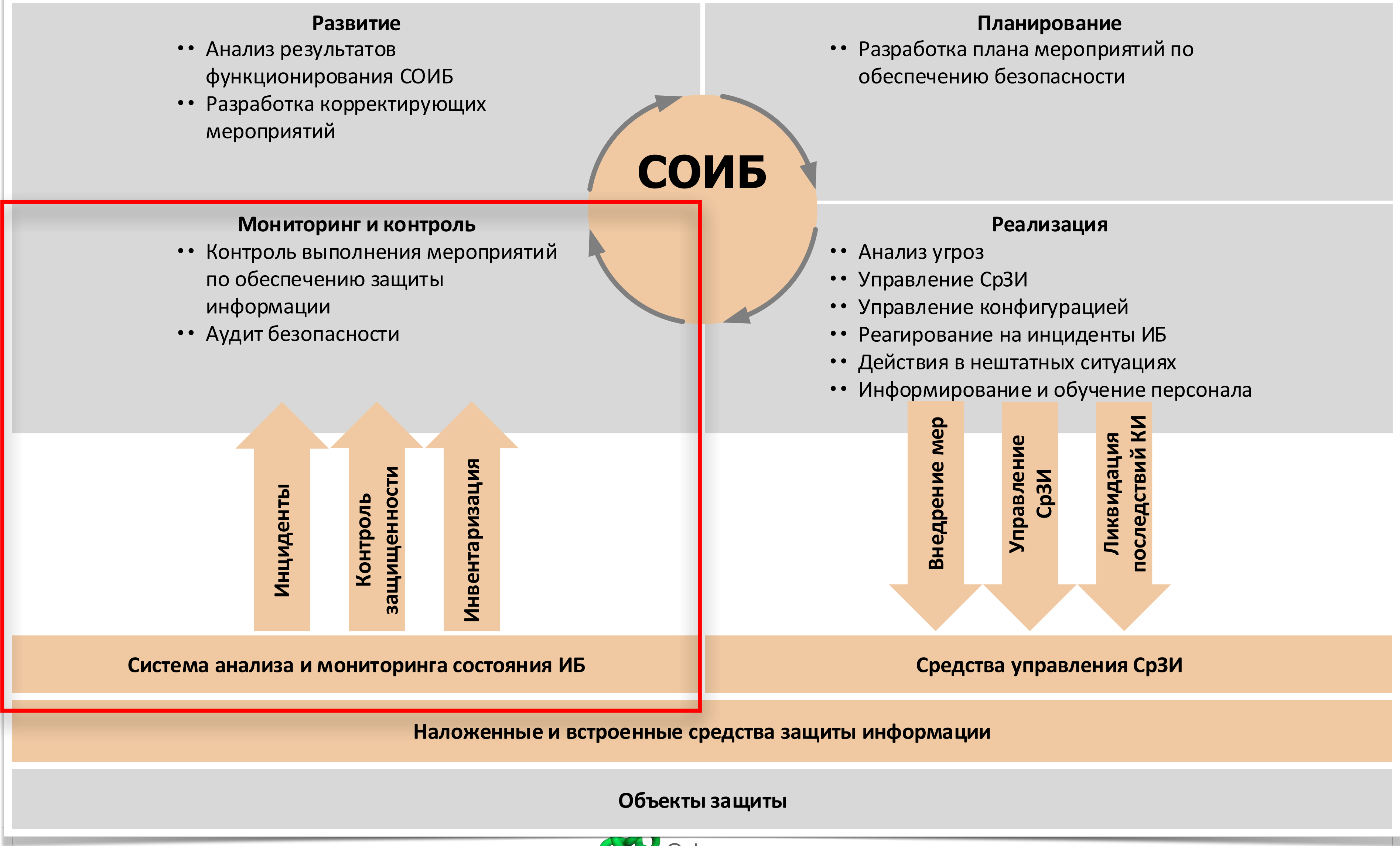


Защита информации
МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Общие положения

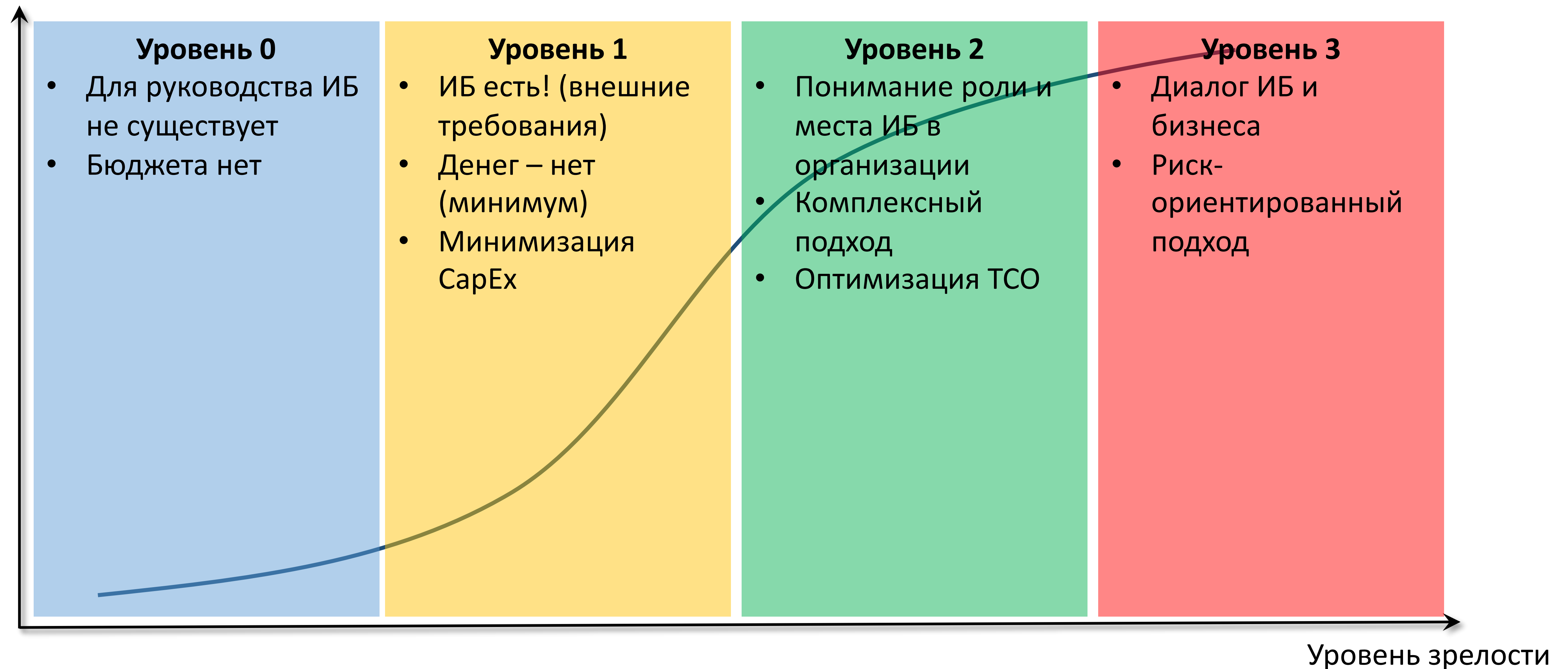
Настоящий проект стандарта не подлежит применению до его утверждения

Москва
Стандартинформ
201X

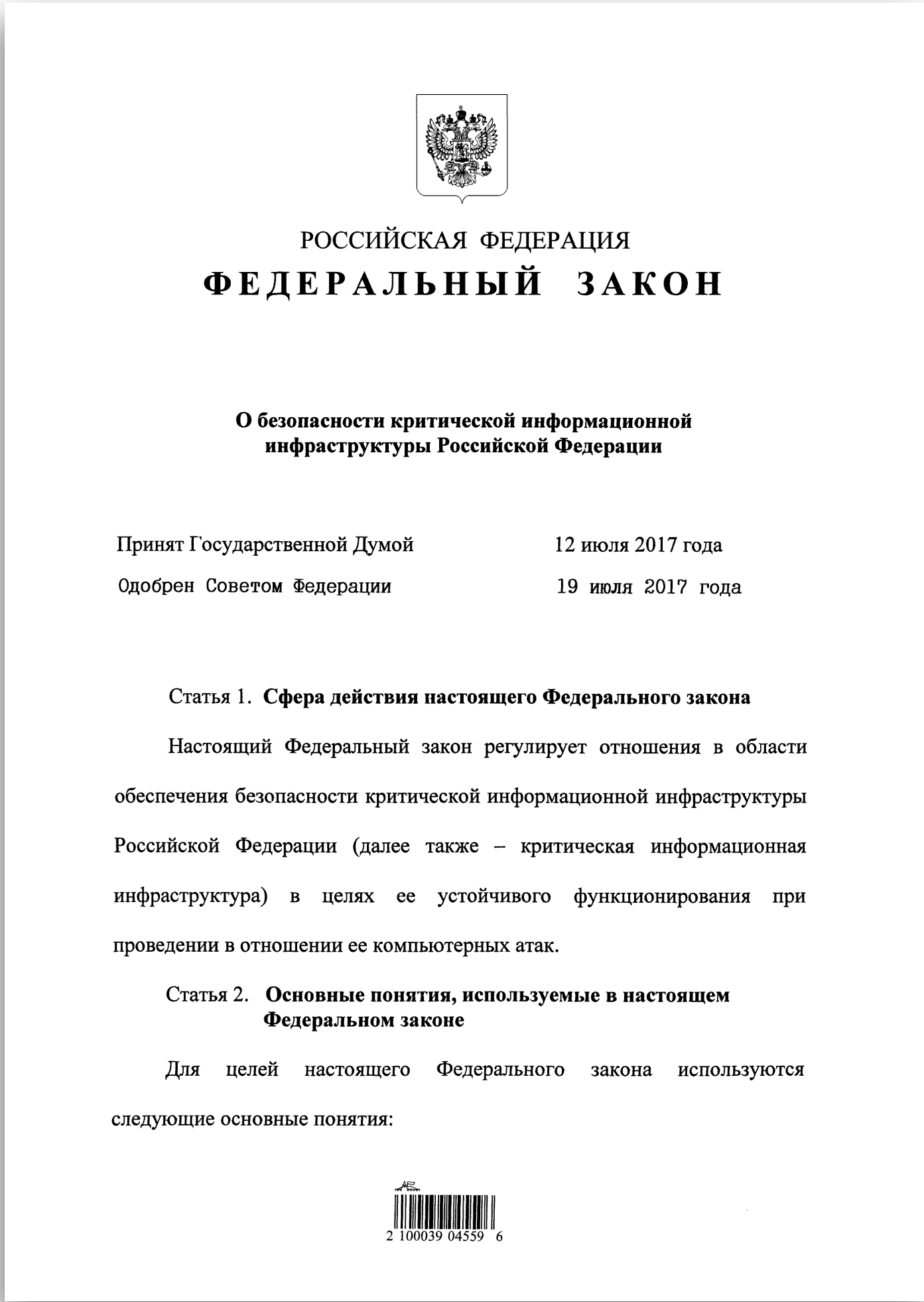
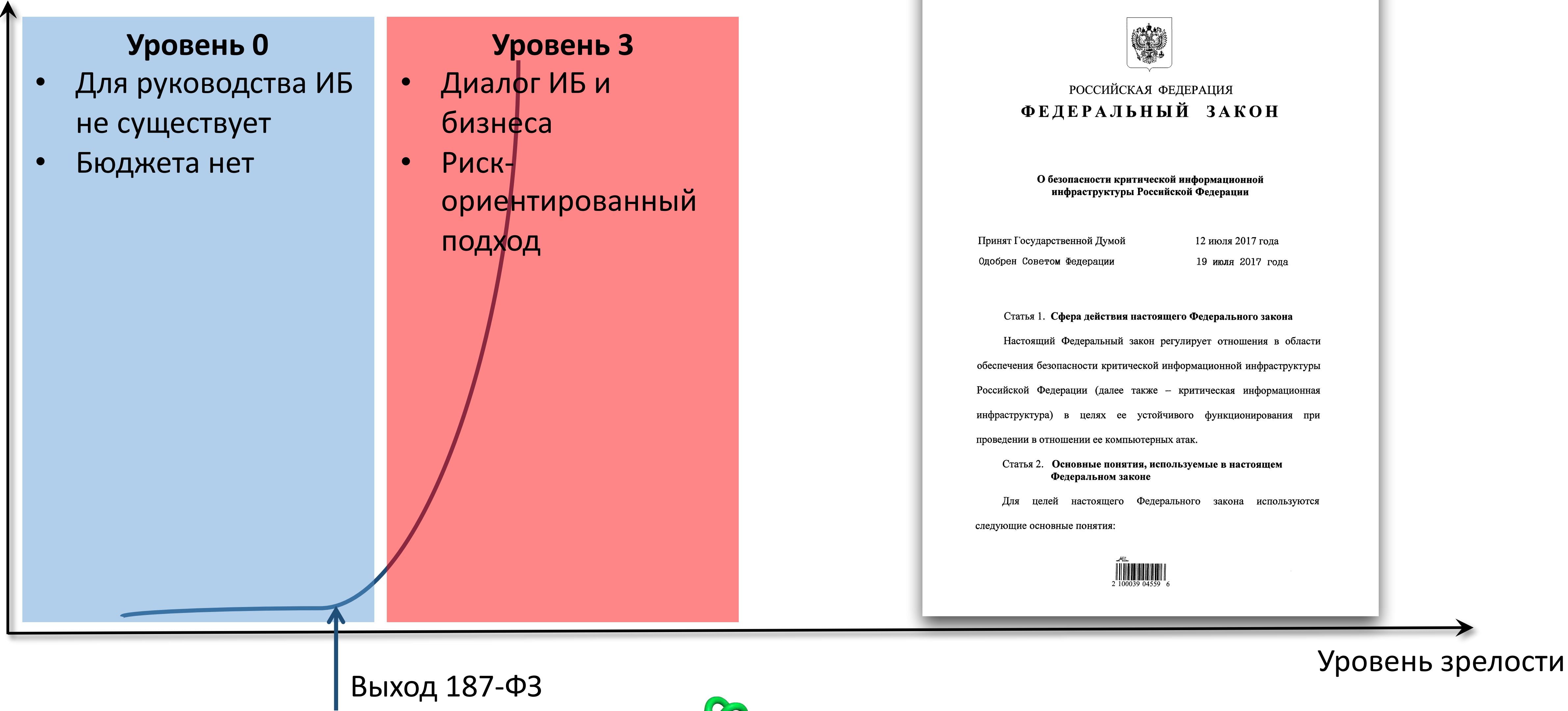
Связь между процессами и технической архитектурой



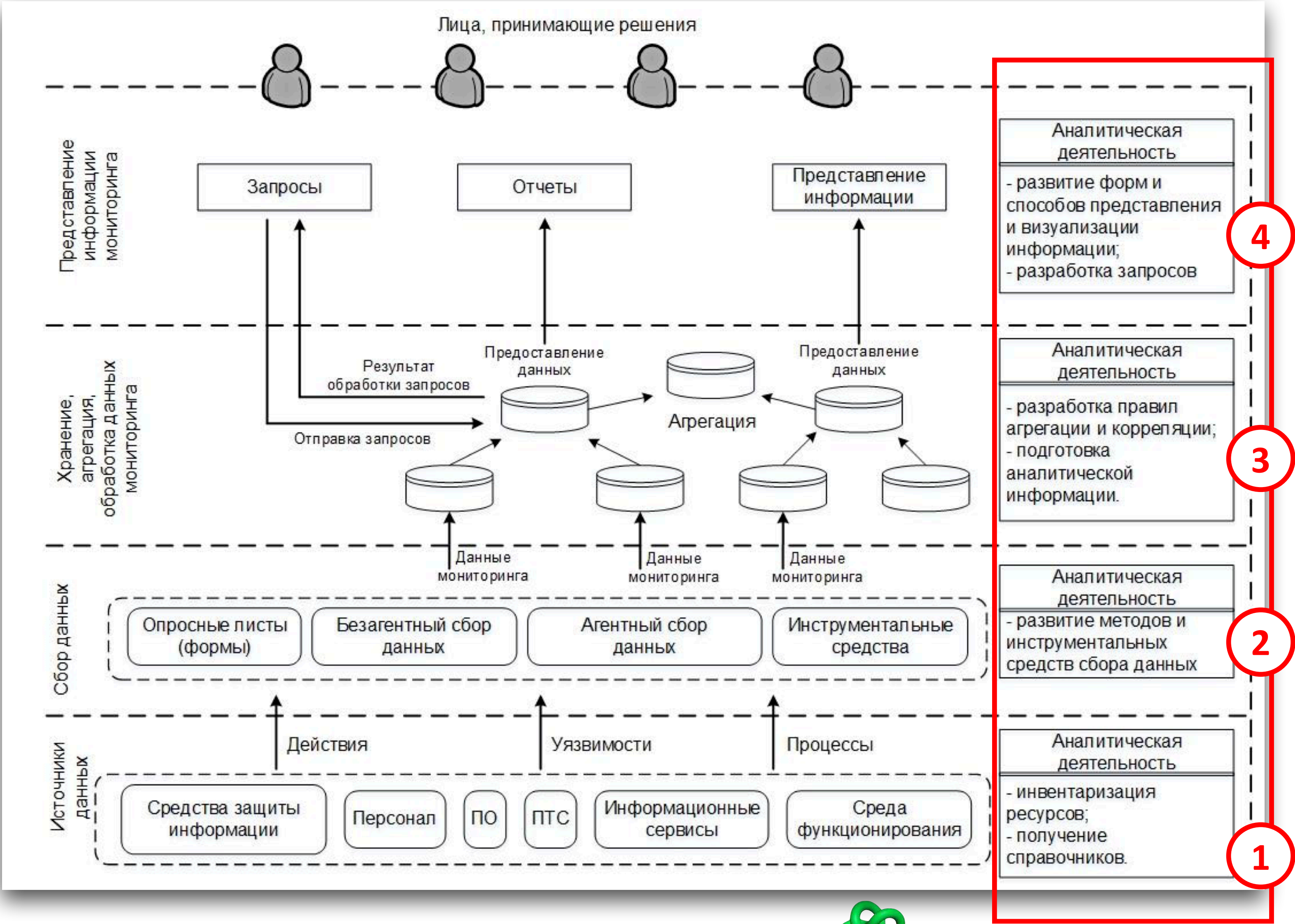
Традиционная модель зрелости процессов обеспечения ИБ



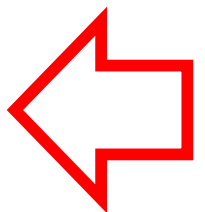
Традиционная модель зрелости процессов обеспечения ИБ



Референсная модель системы мониторинга ИБ



<https://youtu.be/OGKK58zD0IM?t=204>



Готовый план создания системы мониторинга

- Проект ГОСТ Р «Защита информации. Мониторинг информационной безопасности. Общие положения»

Ожидание vs Реальность

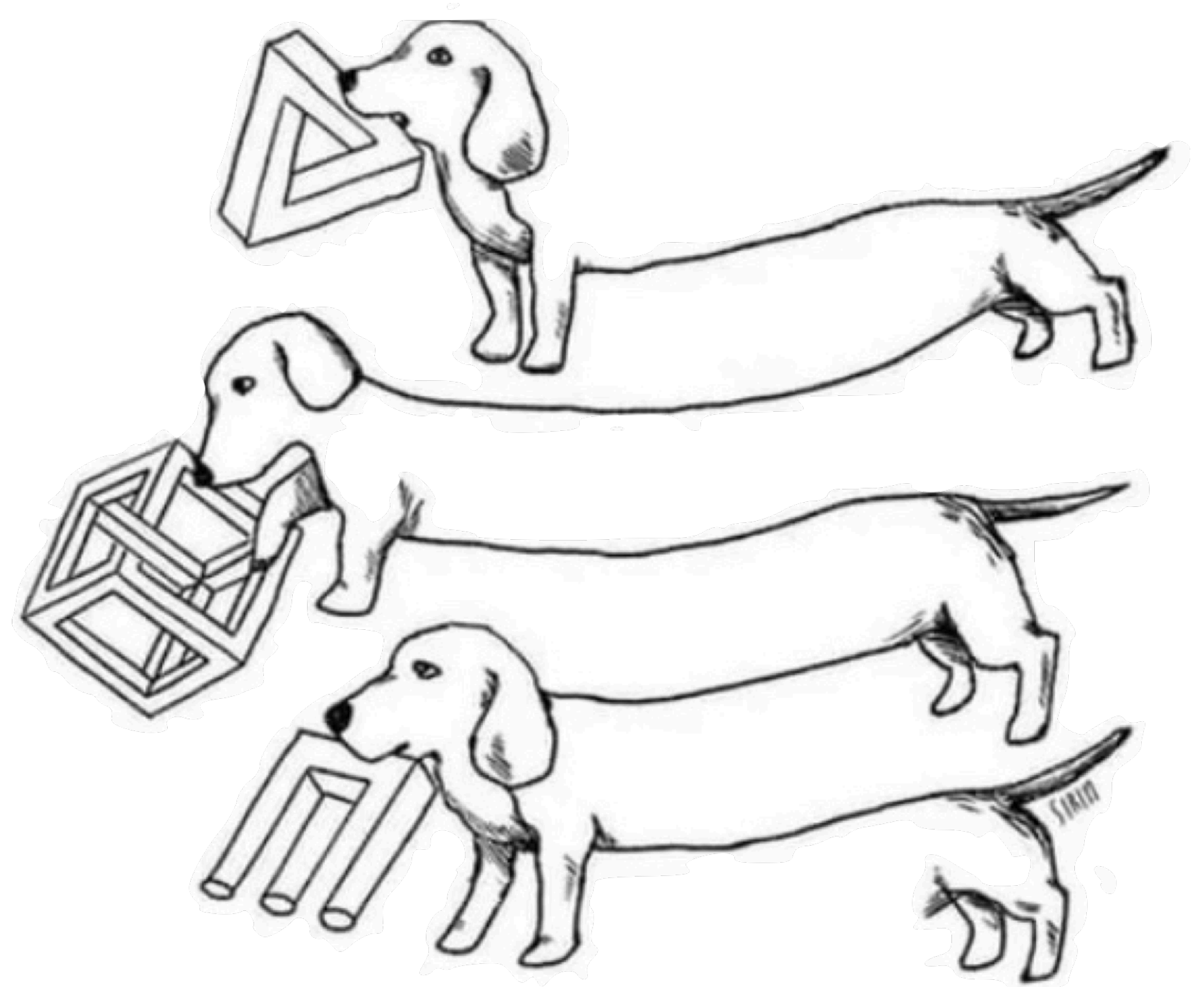
Из реального доклада Заказчика

- >80 тыс. инцидентов для разбора
- >140 сценариев выявления инцидентов
- >30 типов источников событий
- >2700 объектов, охваченных мониторингом
- 1 аналитик и 2,4 FTE (Full-Time Equivalent) для сопровождения



Чем пристальнее смотришь...

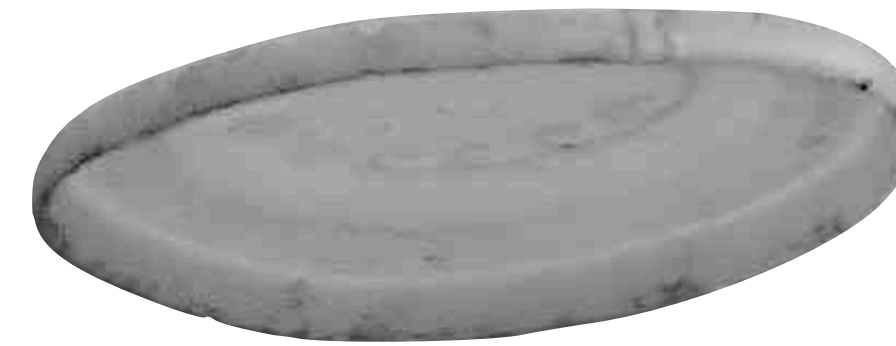
- «Чем больше событий будем собирать, тем больше инцидентов будем выявлять»
- Потребуются значительные вычислительные ресурсы
- Замусоривание ложными срабатываниями
- Трудность актуализации эталонных состояний активов



Чем пристальнее смотришь...

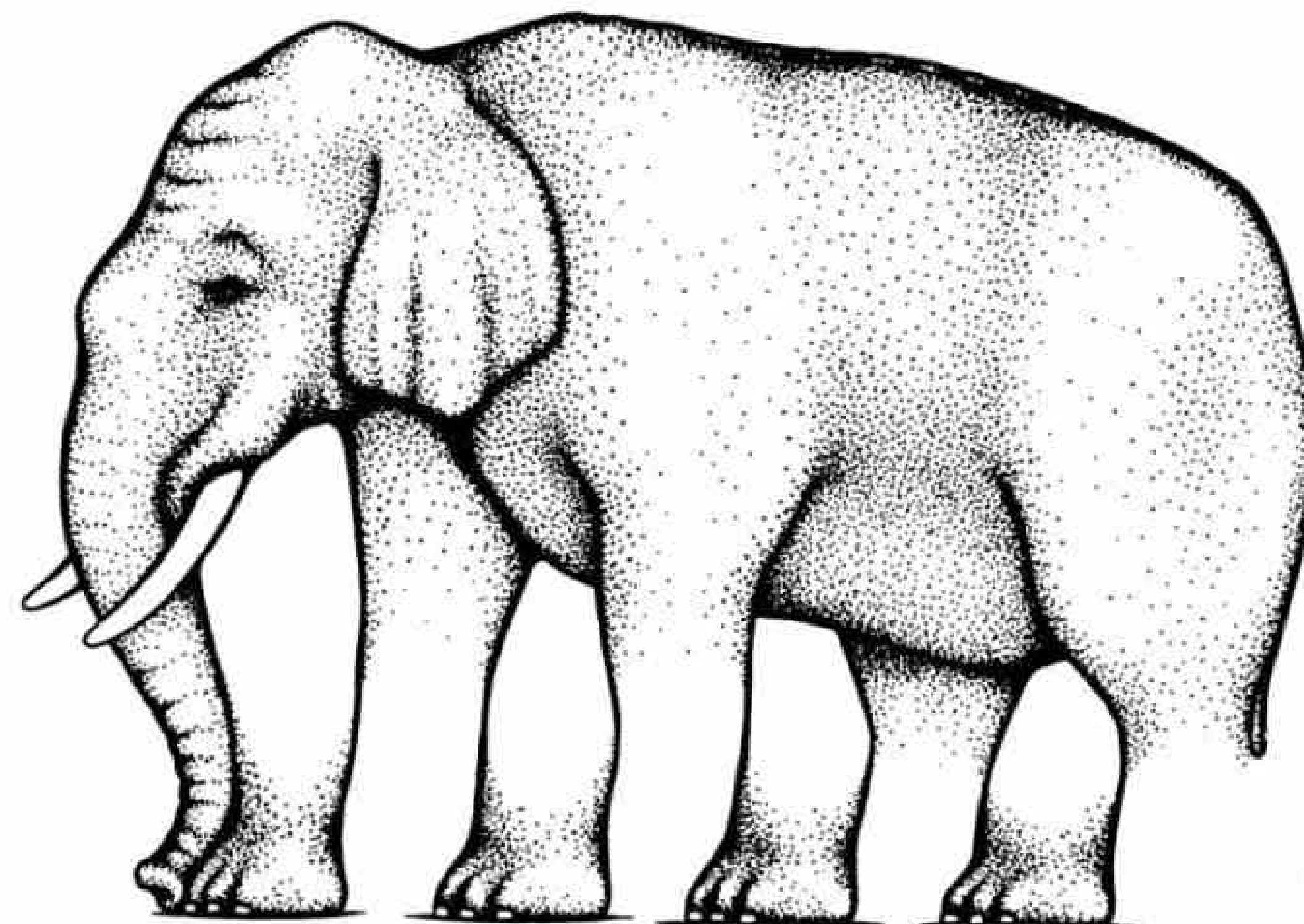
...тем меньше видишь

- Корректное отнесение событий к инцидентам
- Корректные «белые списки» для процессов, ПО и подключенных устройств для объектов защиты
- Агрегация и корреляция событий («схлопывание» событий в один реальный инцидент)



Большое видится...

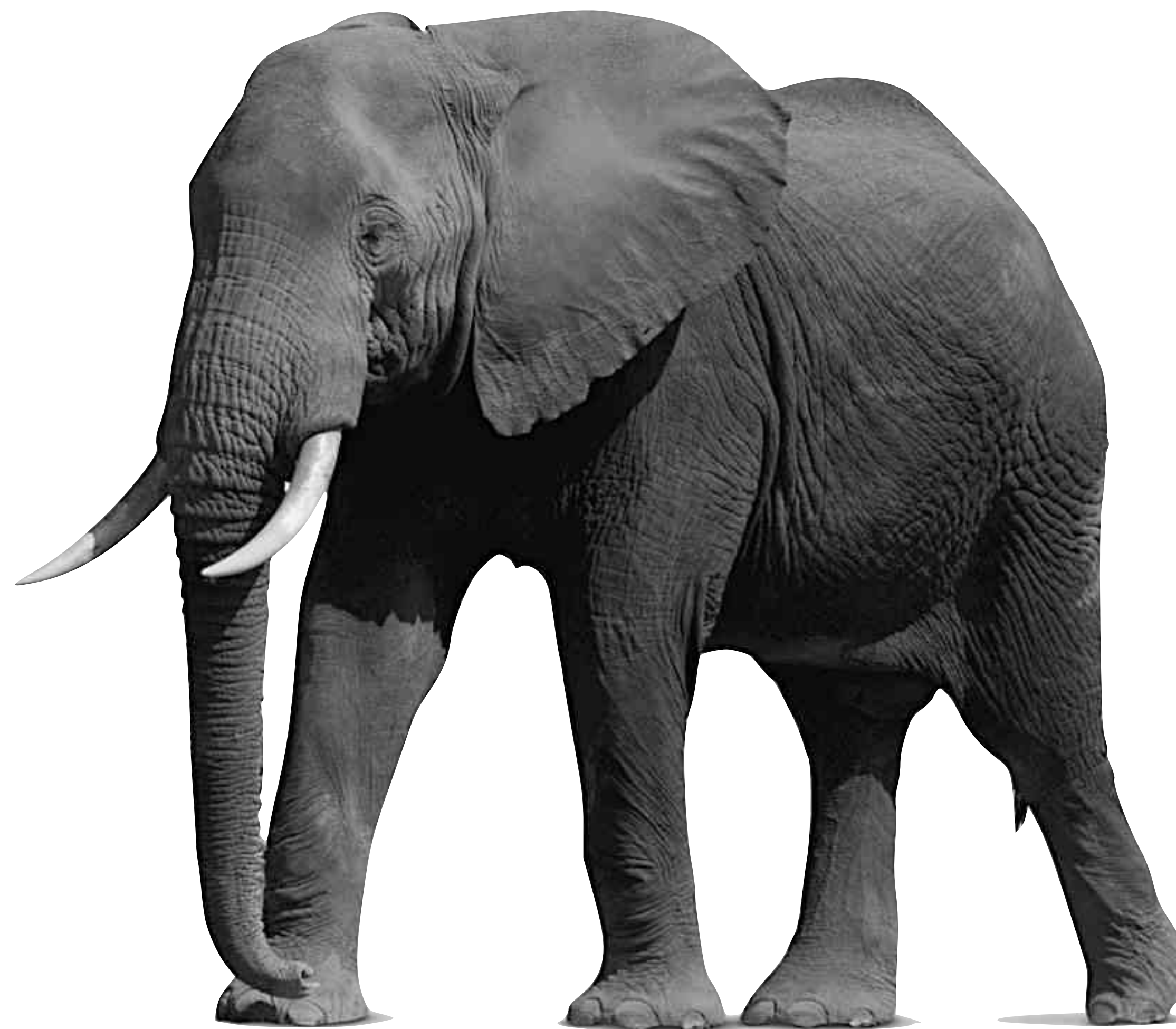
- «Оценка активов на регулярной основе не требуется»
 - Излишний анализ событий со всех объектов, а не только действительно критичных
 - Отсутствие актуальной информации для обогащения инцидентов
 - Инфраструктура АСУТП в действительности довольно часто меняется



Большое видится...

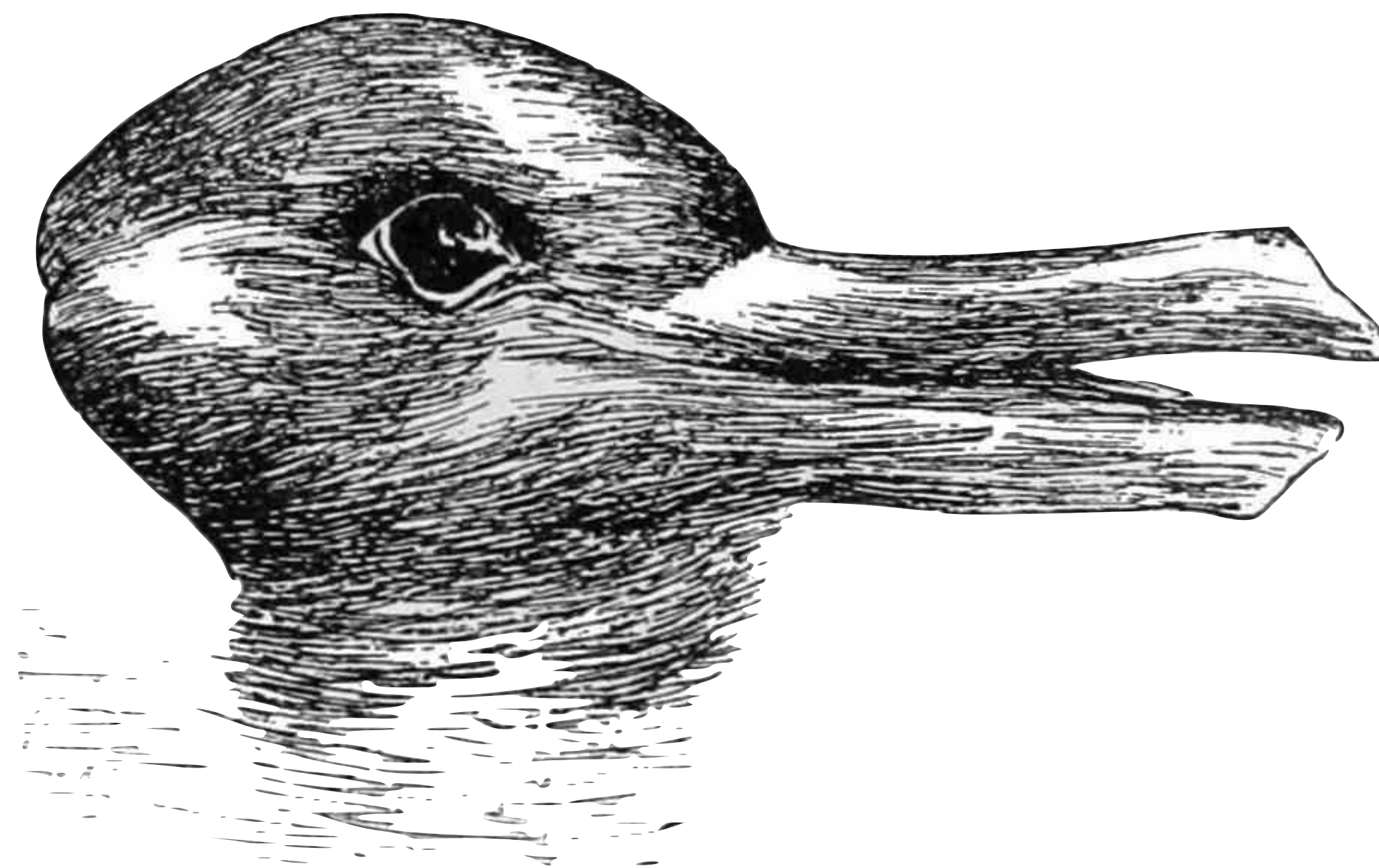
...на расстоянии

- Своевременна оценка и переоценка активов на всех этапах их жизненного цикла
- Грамотный консалтинг на этапе проектирования и внедрения
- Максимальное задействование типов источников событий (но не объектов мониторинга!)



Глаза страшатся...

- «Единой внедрённая система мониторинга не требует непрерывного сопровождения и развития»
- Рост системных требований у новых версий ПО средств мониторинга
- Нужны специфичные знания у персонала
- Без сопровождения система быстро деградирует



Глаза страшатся...

...а руки делают

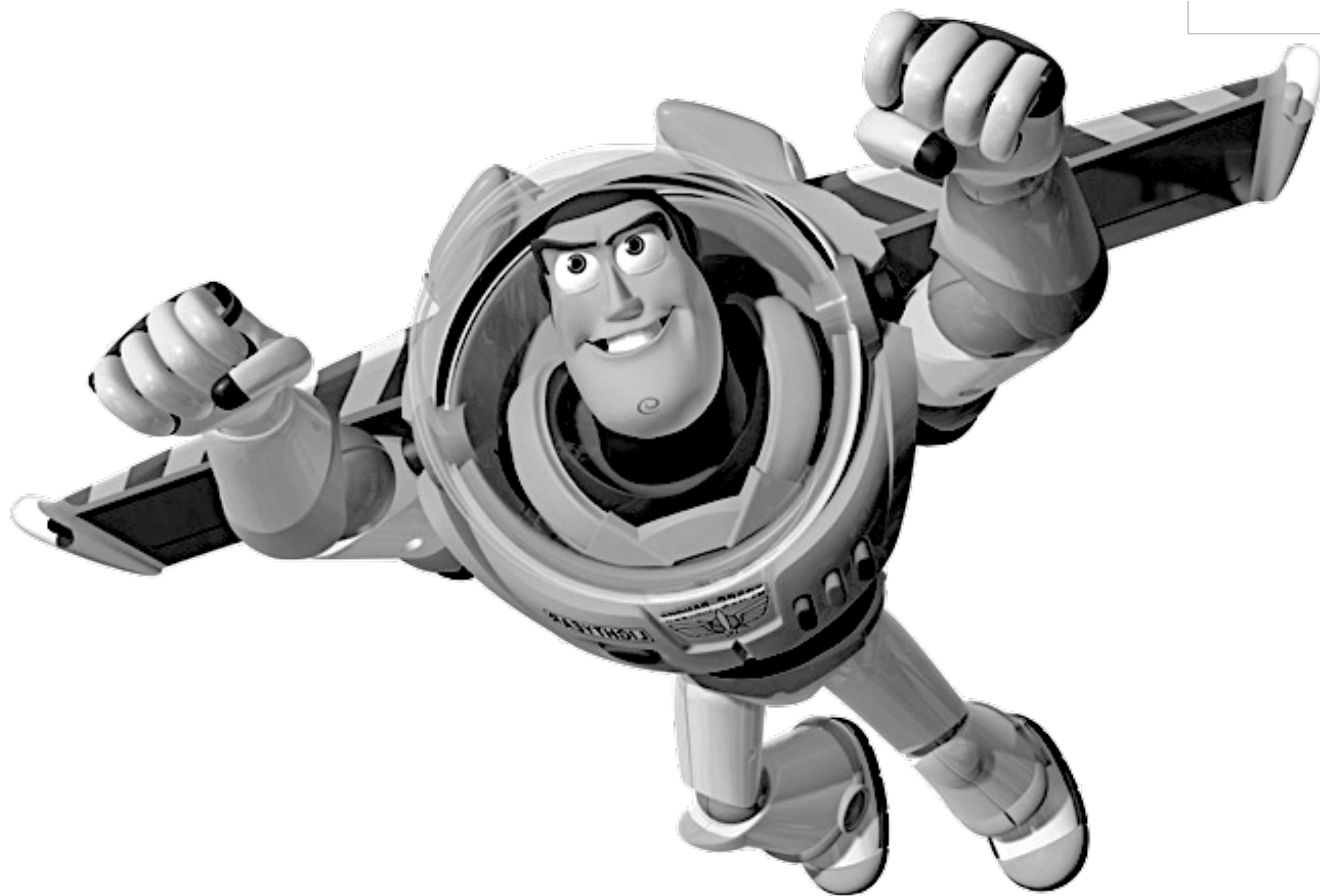
- Выбор многоуровневой иерархической системы
- Аутсорсинг процесса мониторинга (полный либо частичный)
- Аренда отдельных ключевых компонентов системы мониторинга (Software-as-a-Service)



Мониторинг - не предел!!!

GRC, SOAR, SOC... ГосСОПКА

- Процедуры реагирования на инциденты
- Процессы отработки выявленных уязвимостей
- Расследование инцидентов
- Совершенствование системы обеспечения информационной безопасности
- Взаимодействие с НКЦКИ





Спасибо!

<https://ZLONOV.com>

