БЕЗОПАСНОСТЬ В ЦИФРЕ

Хайретдинов Рустэм
Инфовотч

В цифре любая безопасность цифровая, но

- **За функционал** отвечает внутренний заказчик
- **За реализацию** функционала отвечают разработчики и внедренцы (свои или чужие)
- **За инфраструктуру** отвечает ИТ-департамент
- **За поддержку** клиентов - колл-центр
- **За безопасность** – служба информационной безопасности

Часто у них разные цели и критерии их достижения

Риски нарушения процессов

- Кибератаки
- Финансовое мошенничество
- Инсайд, торговля информацией
- Информационные атаки, fake news
- Воровство материальных активов
- Кражи секретов и интеллектуальной собственности
- Компьютерные сбои
- Ошибки в изменениях процессов
- Ошибки операторов и системных администраторов

Старый подход к безопасности не успевает

- Нет детального описания систем, не понятно, где сбой, а где плановое функционирование
- Много ложных срабатываний – велик риск остановить легальный процесс
- Уход в пассив - признание невозможности предотвращать угрозы и отражать атаки
- Рост расходов ресурсов на мониторинг
- «Кусочная» безопасность приводит только к увеличению расходов, эффективность которых нельзя посчитать

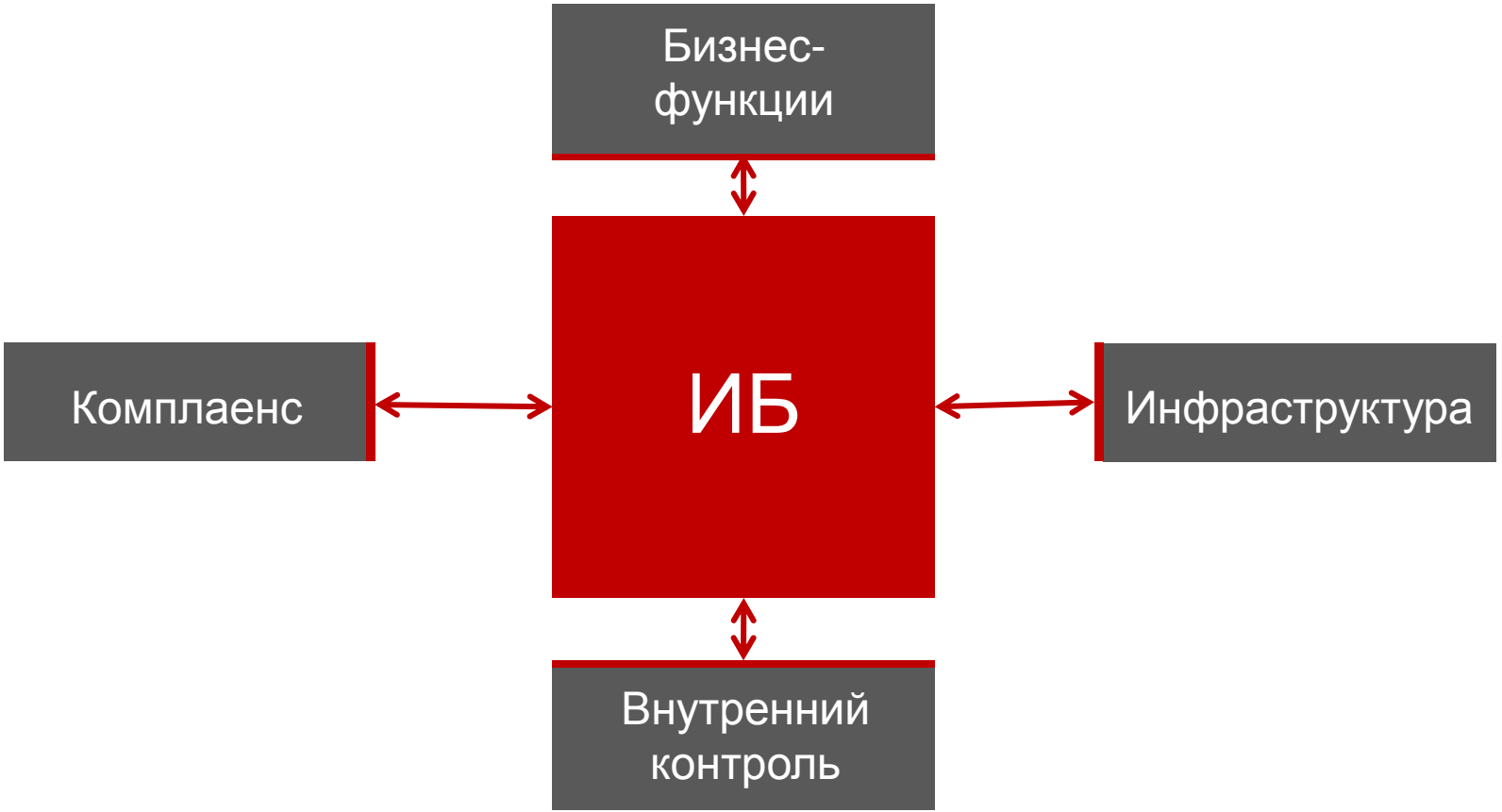
Что изменяется в безопасности в «цифре»?

ОРГАНИЗАЦИОННО:
ПОВЫШАЕТСЯ УРОВЕНЬ ОТВЕТСТВЕННОСТИ, ОТВЕТСТВЕННОСТЬ КОНЦЕНТРИРУЕТСЯ В ОДНИХ РУКАХ

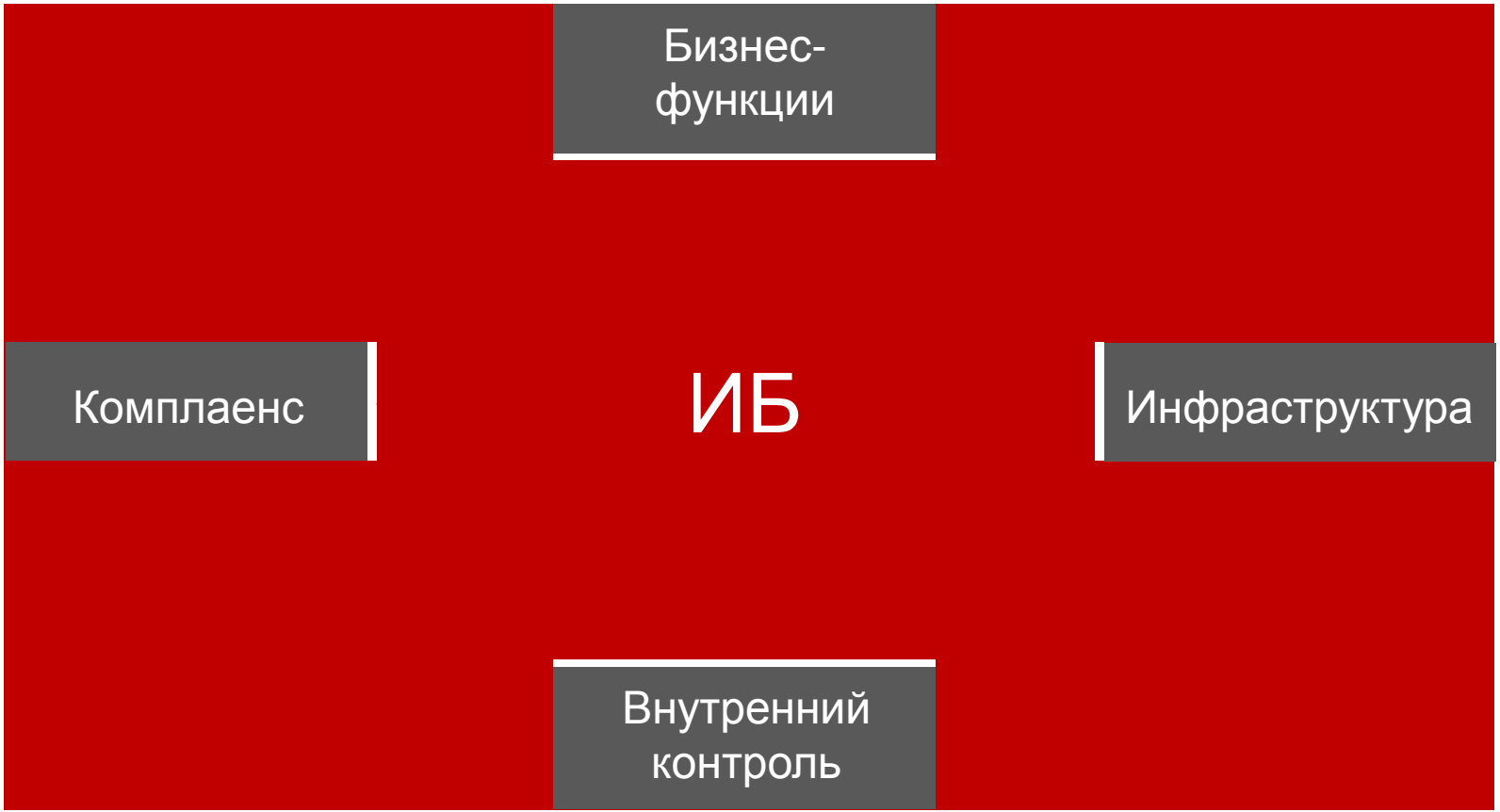
ТЕХНИЧЕСКИ:
Происходит переход от навесных решений к встроенным, интеграция в процессы с фокусом на их устойчивость

КОММУНИКАЦИОННО:
Взаимодействие с бизнесом и другими подразделениями

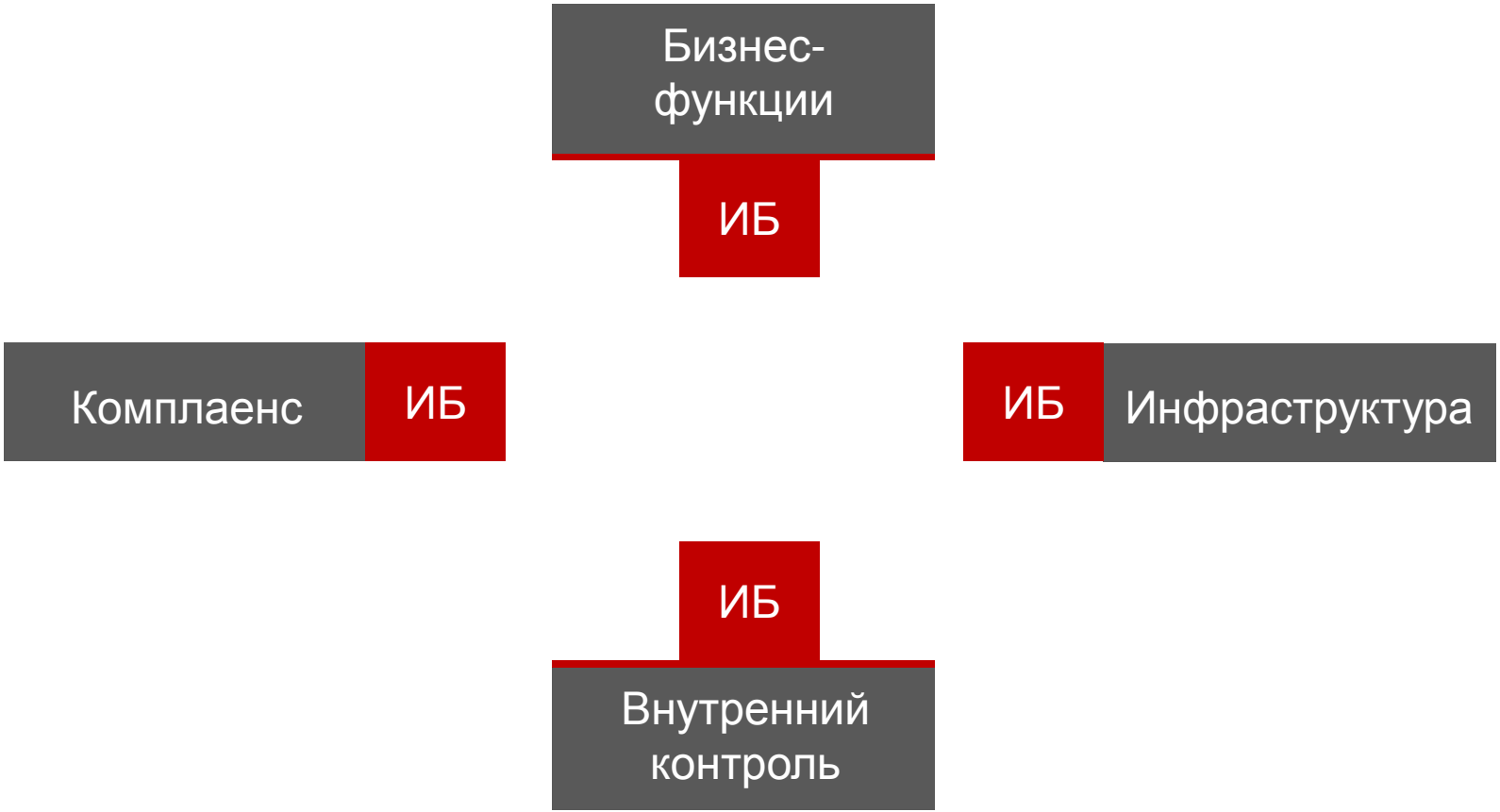
Дублирование функций

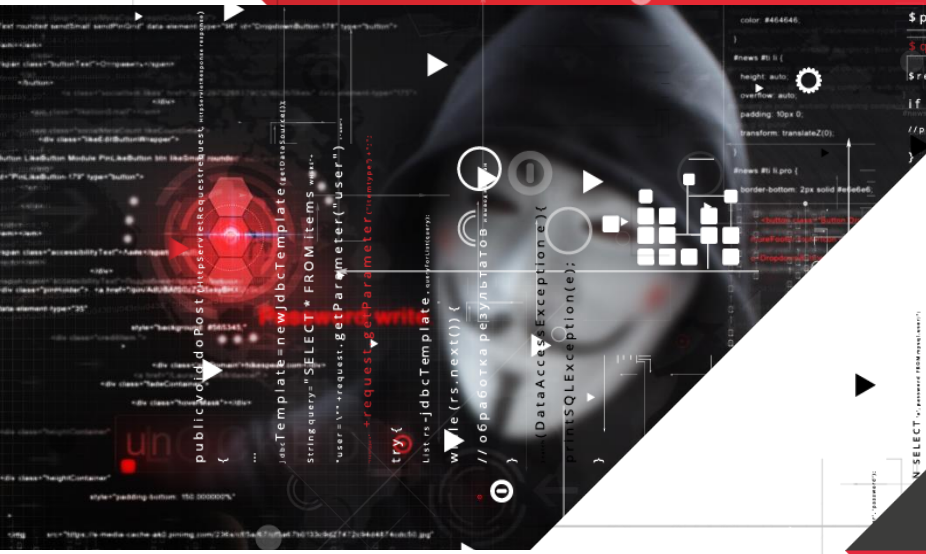


Вариант развития 1



Вариант развития 2





Спасибо за внимание!

Хайретдинов Рустэм
rustem@khairetdinov.com
+7 (903) 961-7312