Сервисная модель промышленной безопасности

Текущие угрозы кибербезопасности

Апрель 2017

Массовый взлом сайтов государственных органов Республики Казахстан

Март 2017

Массовая атака на банки второго уровня Республики Казахстан

Декабрь 2015

Успешная кибератака на электрические сети на Украине

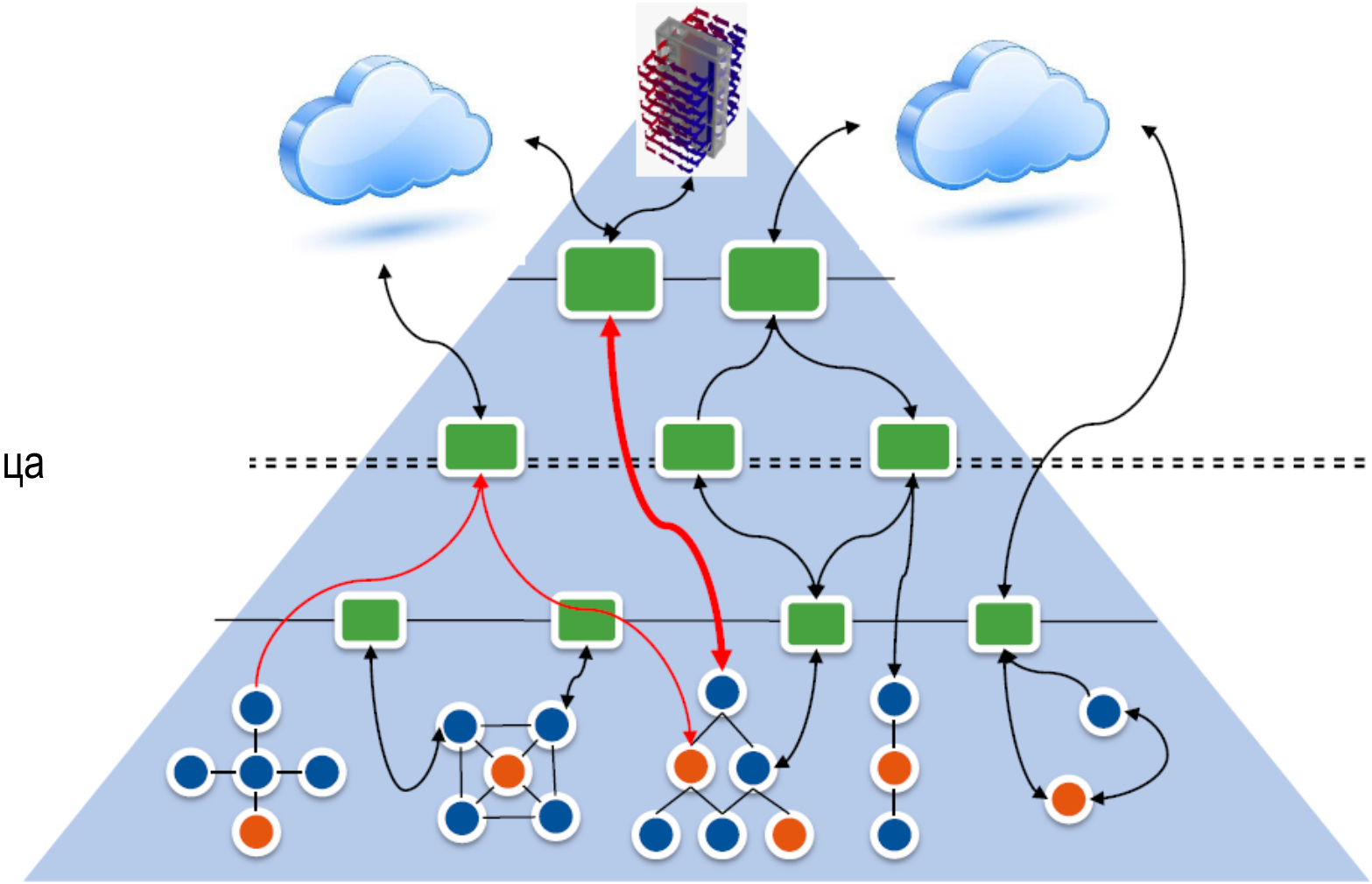
Законодательные требования

- Концепция кибербезопасности РК
- Единые правила в области информационно-коммуникационных технологий и обеспечения информационной безопасности

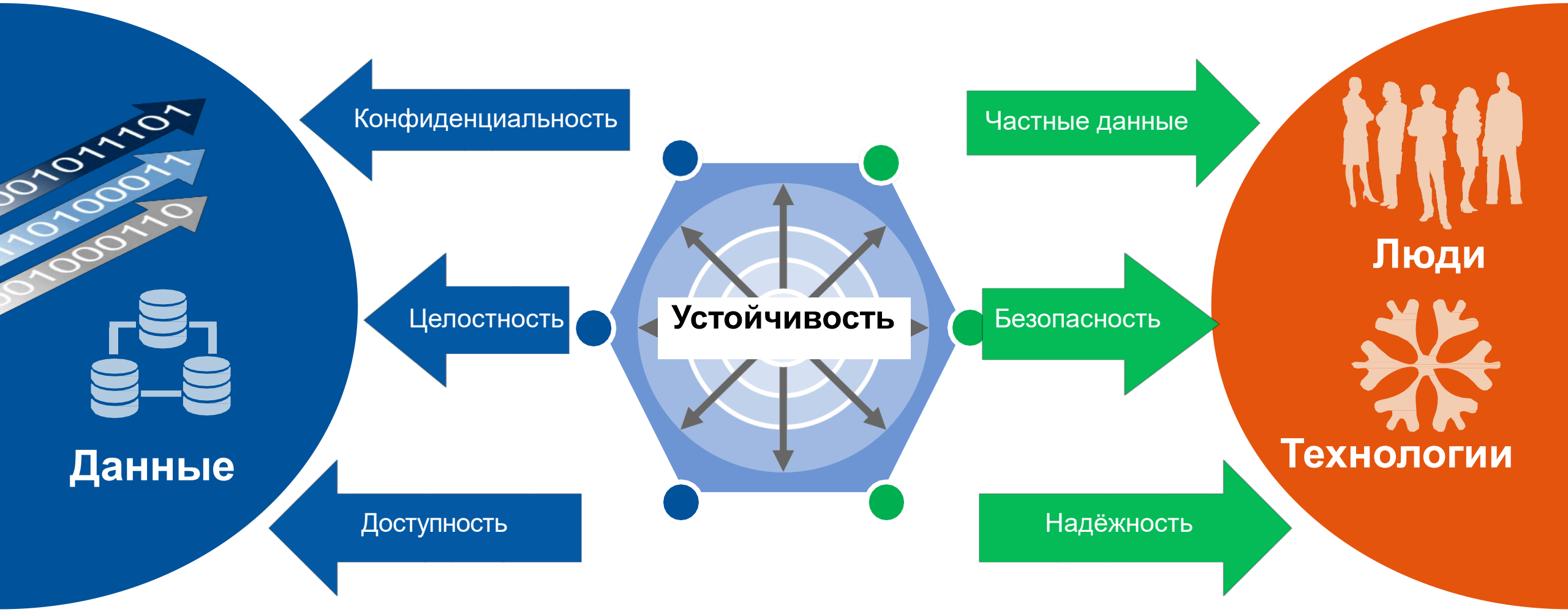
Государственная техническая служба

ISO 27001

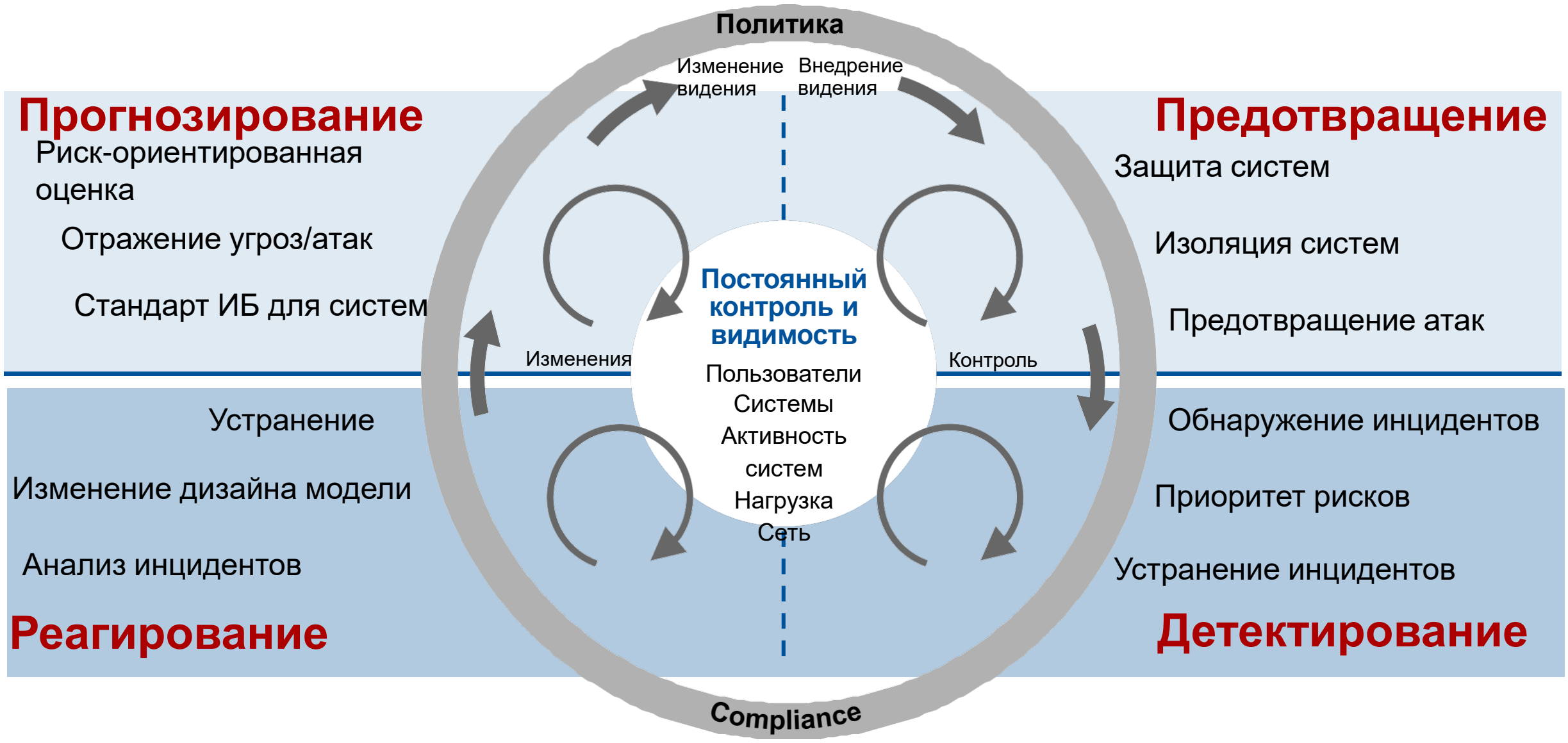
Потоки данных определяют стратегию кибербезопасности



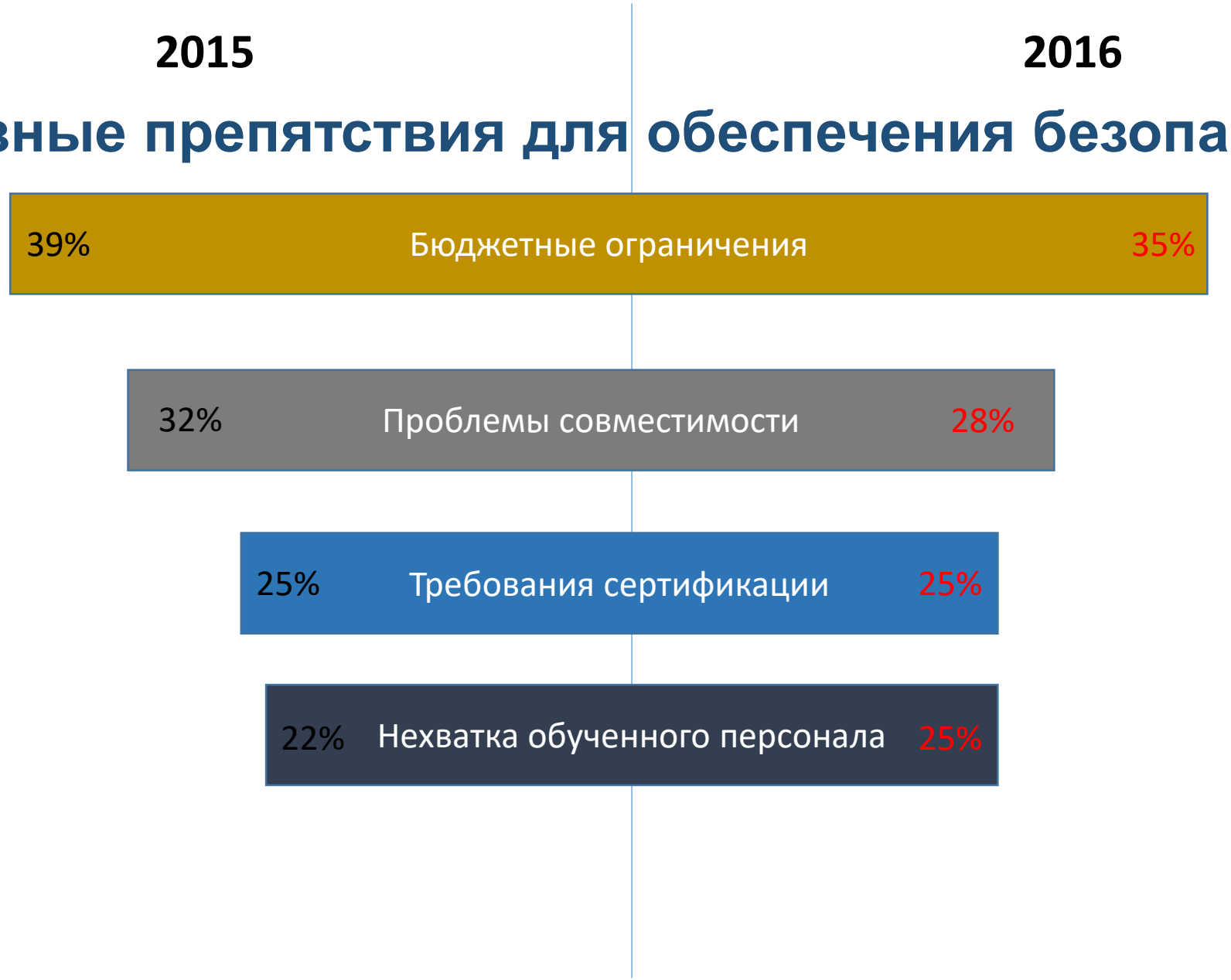
Новая модель цифровой безопасности



Архитектура кибербезопасности

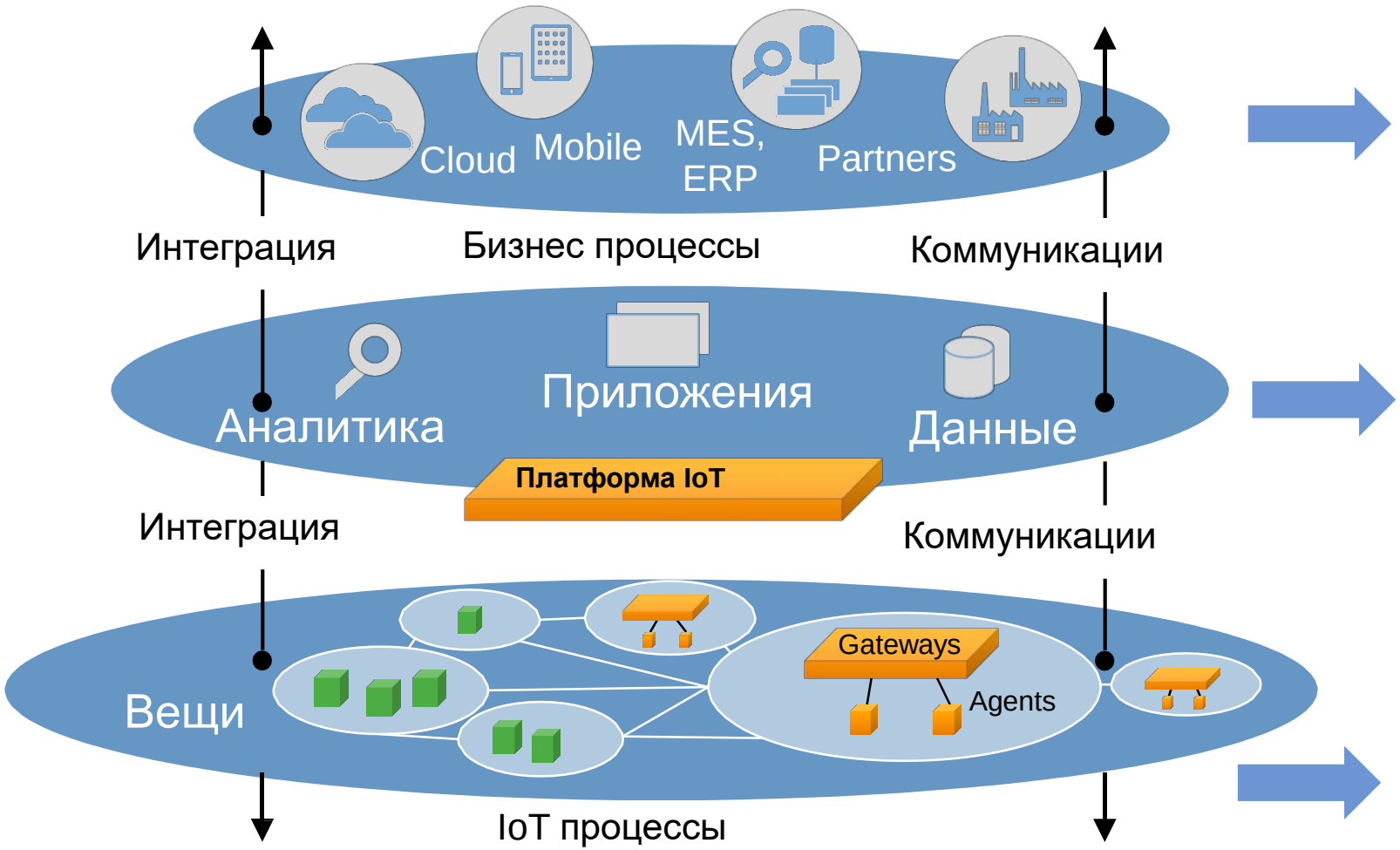


Серьёзные препятствия для обеспечения безопасности



Согласно годовому отчёту по безопасности от CISCO за 2017 год

Безопасность распространяющейся информатизации



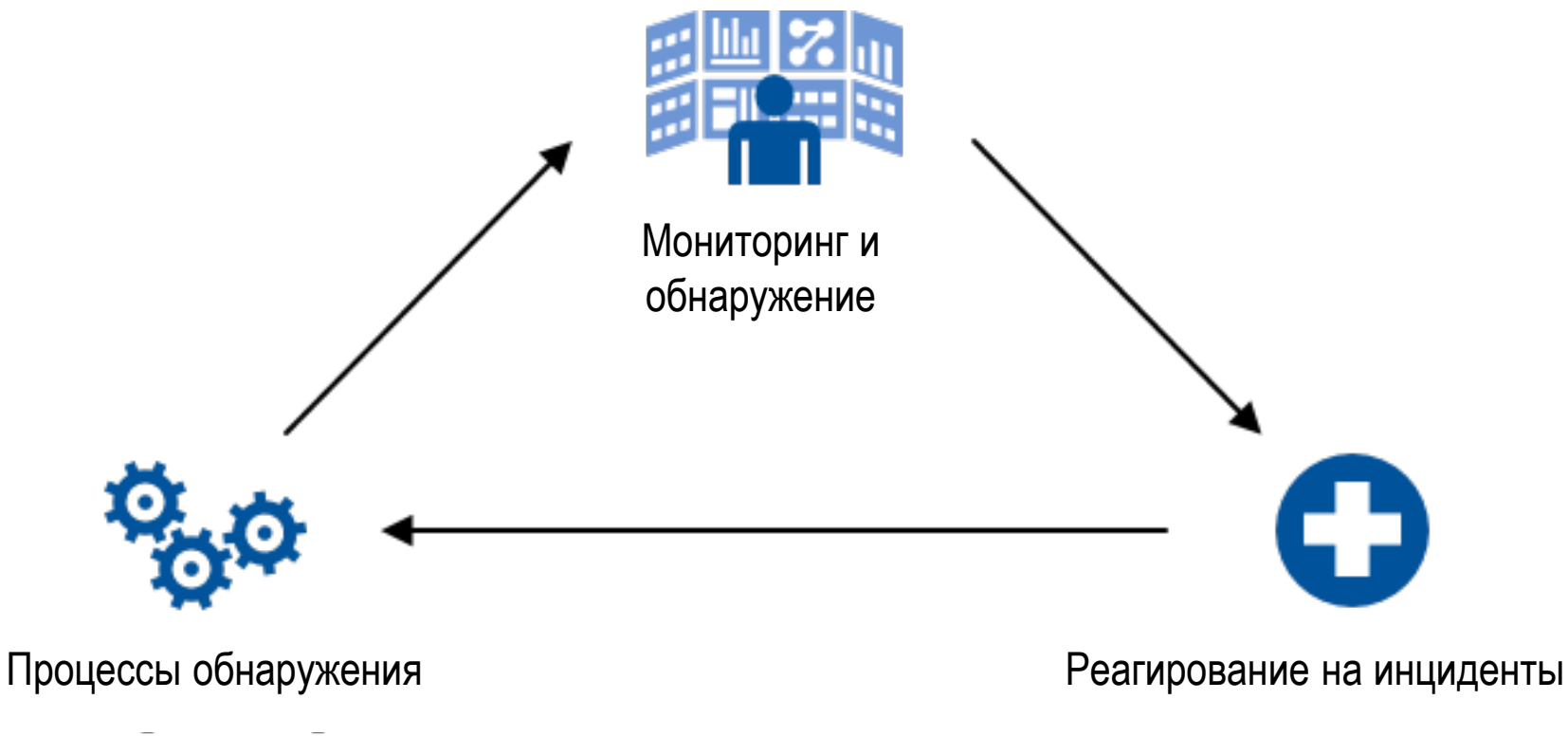
Риски

- Нарушение бизнес-процессов
- Шпионаж и фрод
- Финансовые потери

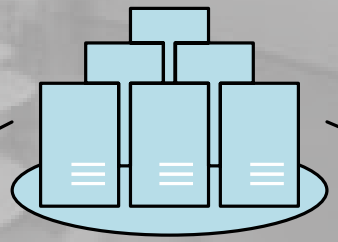
- Взлом платформы
- Утечка данных
- Саботаж автоматизации и устройств

- Подмена устройств
- Взлом устройств
- Слежение, вмешательство
- Разрушение, повреждение

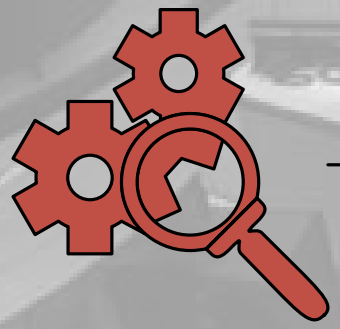
SOC – ответ угрозам кибербезопасности



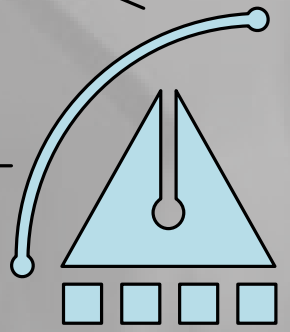
Сервисы SOC



Управление инцидентами



Управление уязвимостями



Услуги киберразведки

Аналитика кибербезопасности

Описание	Диагностика	Прогнозирование	Предписание
Что произошло?	Почему так произошло?	Что произойдёт дальше?	Что я должен делать дальше?
Зловредное ПО на рабочей станции соединяется с командным центром	Сотрудник открыл вложение в электронной почте	Файл A на сервере XYZ будет украден с помощью логина AA	Сменить пароль взломанного аккаунт, удалить файл на сервере account, внедрить правило SIEM

Базовая аналитика	Улучшенная аналитика
Простая арифметика	Управление данными
Отчётность/Визуализация	Решение бизнес-проблем
Общие BI платформы	Математические инструменты
"Знакомое"	"Поражающее"

Вопросы?

Тынымбаев Болат
CISM
Эксперт ИБ

https://www.linkedin.com/in/bolat-tynymbayev-7a1693b8/