



**ГАЗПРОМБАНК**

SOC-Forum v 2.0,  
Практика противодействия кибератакам и  
построения центров мониторинга ИБ

# Сценарии применения SOC: борьба с инсайдерами

**Плешков Алексей Константинович**

Начальник Управления УРИБ ДЗИ ГПБ (АО)

Москва, 16.11.2016



# Инсайдер – это ...



\* - Федеральный Закон от 27.07.2010 № 224

«О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком...»



# Нарушитель

---

Нарушитель информационной безопасности, нарушитель ИБ - субъект, реализующий угрозы ИБ организации БС РФ\*, нарушая предоставленные ему полномочия по доступу к активам организации БС РФ или по распоряжению ими.

## Инсайдер ?

\* - "Стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения" СТО БР ИББС-1.0-2014" (Распоряжение Банка России от 17.05.2014 N P-399)



# Инсайдер в банке - это ...

**10**

**отдельных  
глав в  
3379-у\***

**8**

**ВИДОВ  
владельцев  
инсайдерской  
информации**

**120+**

**ТИПОВ  
инсайдерской  
информации**

\* - указание Центрального Банка РФ от 11.09.2014 № 3379-У  
«О перечне инсайдерской информации лиц, указанных в пунктах 1 - 4, 11 и 12  
статьи 4 Федерального Закона «О противодействии неправомерному  
использованию инсайдерской информации и манипулированию рынком...»

# Модель инсайдера



# Реализация





# Решение

## Алгоритм

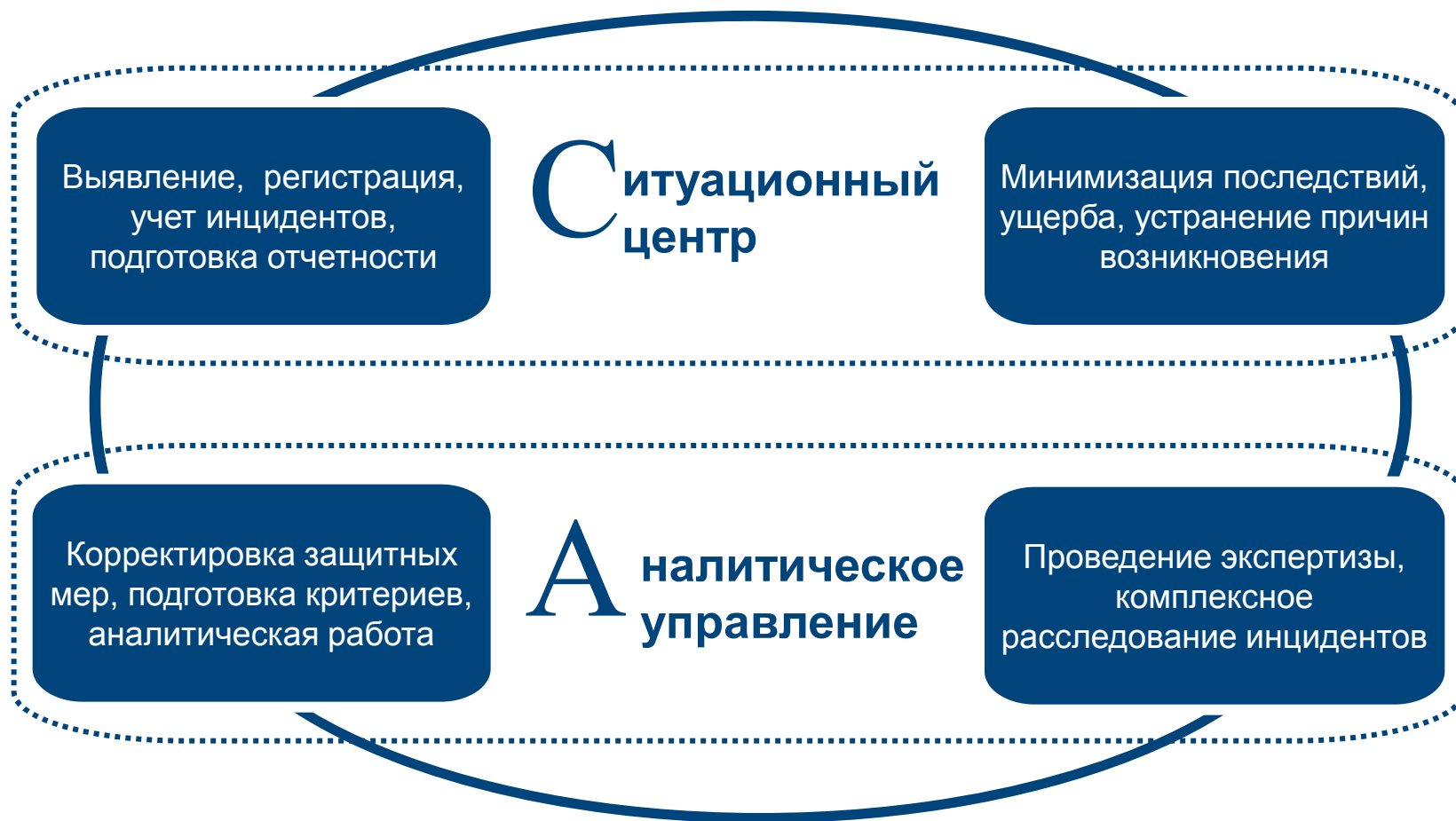
- ✓ Внедрение и актуализация метрик / пороговых значений
- ✓ Развитие экспертизы
- ✓ Накопление статистики и создание типовых профилей
- ✓ Подключение новых источников данных
- ✓ Ретроспективный анализ
- ✓ Создание технологических карт процессов
- ✓ Паспортизация систем





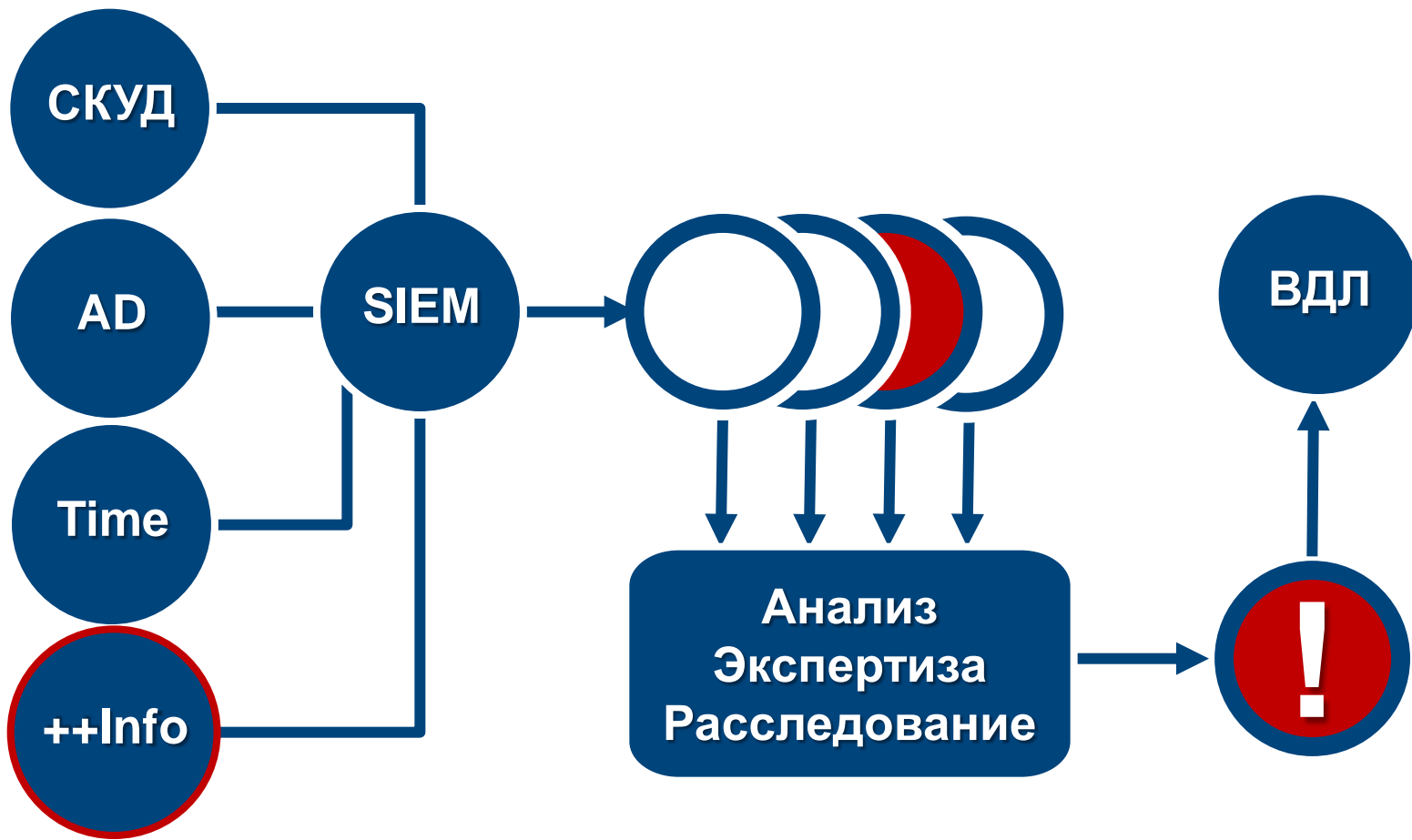


# Что первично?

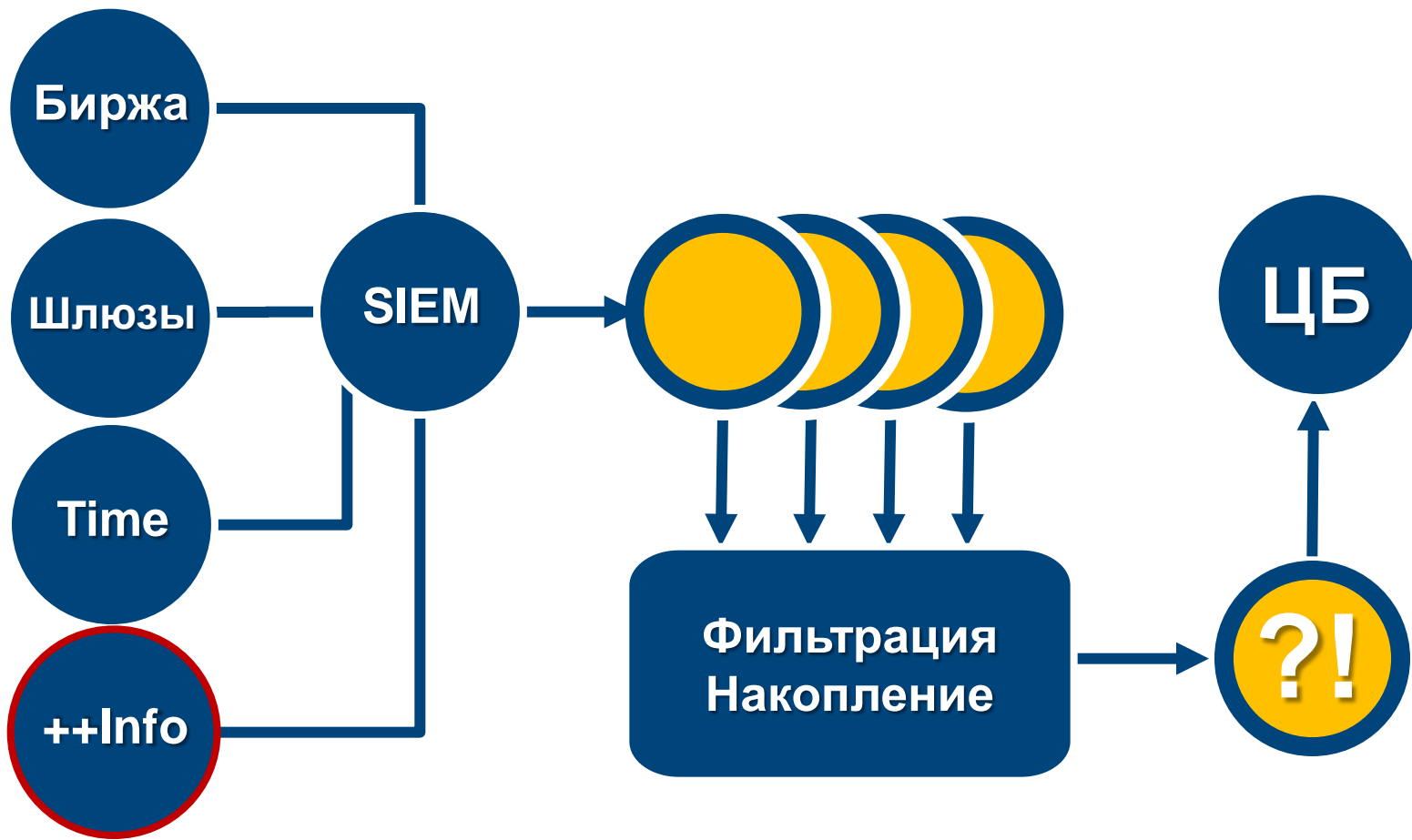




# Сценарий № 1



# Сценарий № 2





**Б**лагодарю за внимание !

**Плешков Алексей Константинович**

**начальник Управления**

**режима информационной безопасности**

**Департамент защиты информации**

**Банк ГПБ (АО) г. Москва**

e-mail: [Alexey.Pleshkov@gazprombank.ru](mailto:Alexey.Pleshkov@gazprombank.ru)

тел: 8(495)-428-5045