ПРАКТИЧЕСКИЙ ОПЫТ МОНИТОРИНГА ИНЦИДЕНТОВ ИБ

Роман Кобцев
Директор по развитию бизнеса
ЗАО «Перспективный мониторинг», ГК «ИнфоТеКС»

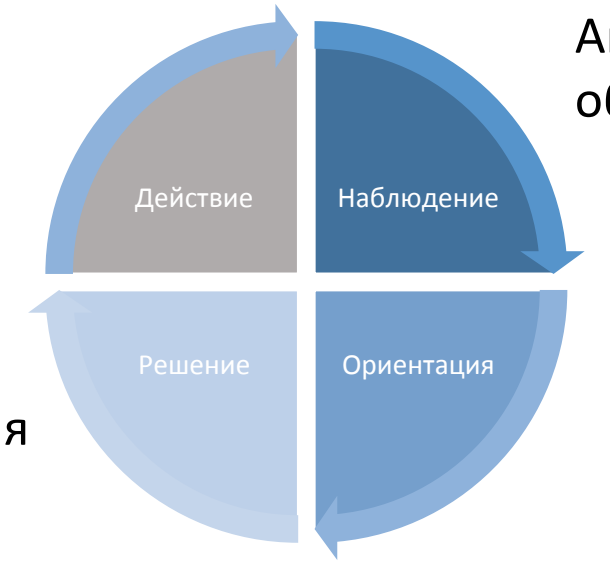
Москва, 11 февраля 2016 г.

Стандарты и лучшие практики

- Стандарты ISO и отечественные (переводные) стандарты
- РС БР ИББС-2.5-2014 "Менеджмент инцидентов ИБ"
- Стандарты и рекомендации NIST, SANS, COBIT, ENISA, ISACA и др. (десятки документов!)

«Цикл Бойда» как модель управления инцидентами

Принятие решения об обработке инцидента



Агрегирование большого объема информации

Окончательный выбор оптимального сценария решения задачи

Декомпозиция задачи на более мелкие элементы, до такой степени, пока она не станет типовой

Пути повышения эффективности

- Увеличение (в количественном измерении) скорости прохождения циклов
- Повышение качества принимаемых решений

Увеличение (в количественном измерении) скорости прохождения циклов

- Оптимизация объема входящей информации;
- Достаточные вычислительные и исследовательские ресурсы;
- Устранение разрывов и достижение минимального времени в процессе взаимодействия между циклами.

Повышение качества принимаемых решений

- Снижение процента ложных срабатываний;
  - Совмещение автоматизированной и экспертной поддержки принятия решений;
  - Постоянная настройка и кастомизация аналитического ядра принятия решений.

Терминологические вопросы

- *Событие информационной безопасности (information security event)*: Идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью.
- *Инцидент информационной безопасности (information security incident)*: Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Выявление, анализ и обработка инцидентов

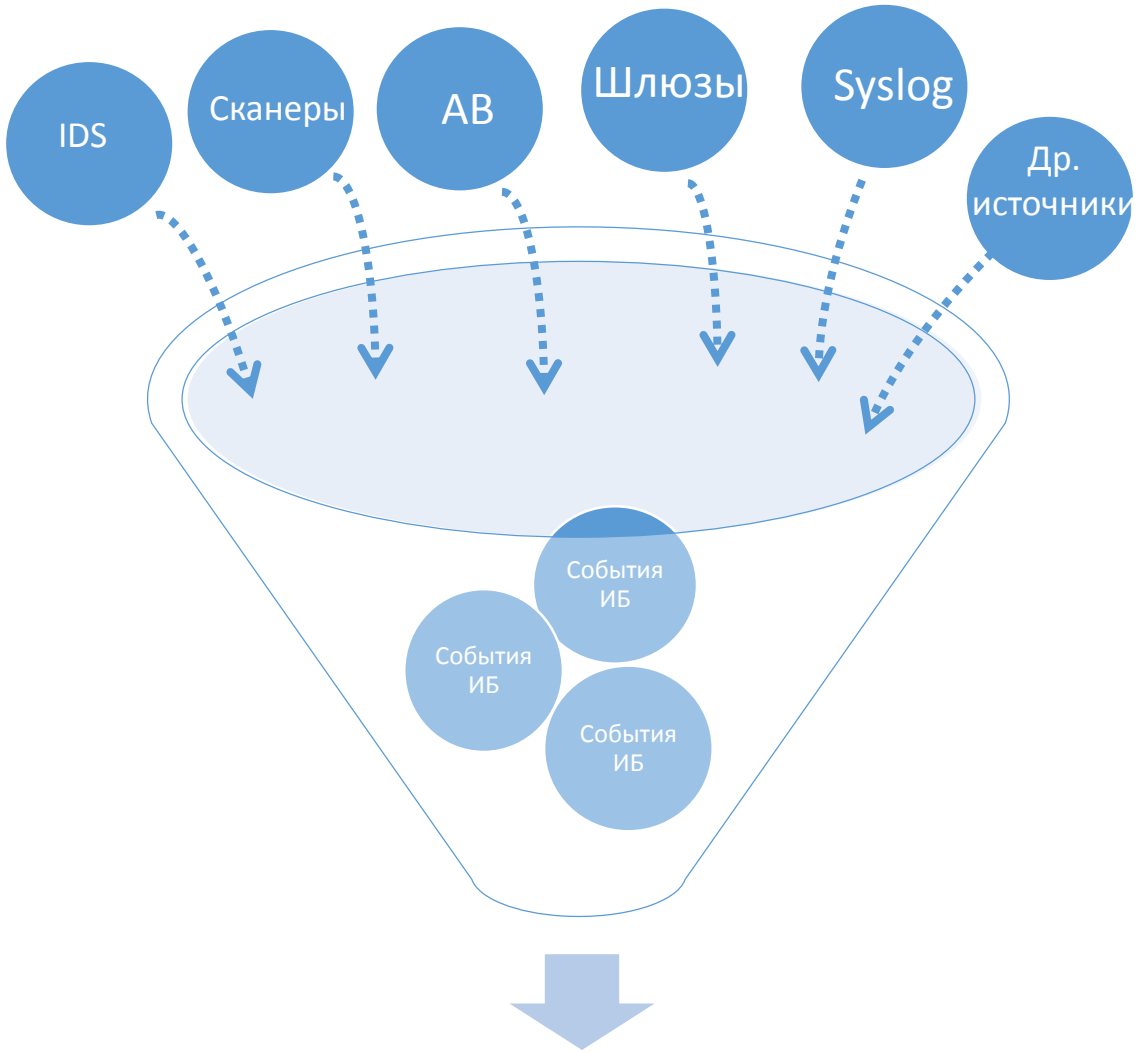
Все события в ИС → 55 000 000 событий

События интересные мониторингу → 286 119 событий

Выявление событий ИБ → 8 187 событий ИБ

Анализ событий ИБ → 732 подозрений на инцидент

Регистрация и обработка инцидентов ИБ → 7 инцидентов



Выявление, анализ и обработка инцидентов

АВТОМАТИЗИРОВАННЫЙ УРОВЕНЬ ПРИНЯТИЯ РЕШЕНИЯ

Все события в ИС

55 000 000 событий

ЭКСПЕРТНЫЙ УРОВЕНЬ ПРИНЯТИЯ РЕШЕНИЯ

События интересные мониторингу

256 719 событий

АВТОМАТИЗИРОВАННЫЙ УРОВЕНЬ ПРИНЯТИЯ РЕШЕНИЯ

Выявление событий ИБ

8 187 событий ИБ

Анализ событий ИБ

732 подозрений на инцидент

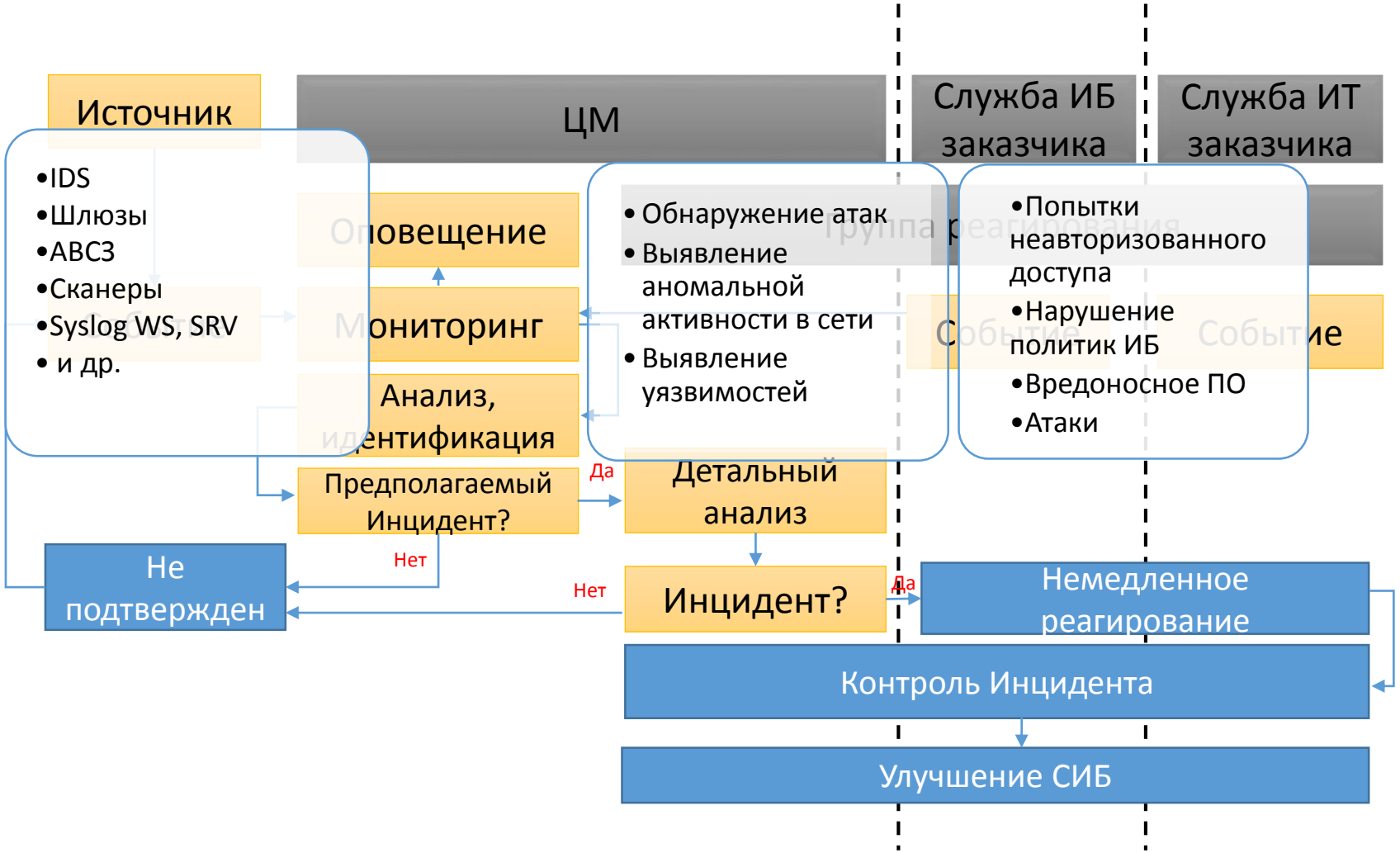
ЭКСПЕРТНЫЙ УРОВЕНЬ ПРИНЯТИЯ РЕШЕНИЯ

Регистрация и обработка инцидентов ИБ

7 инцидентов

Инциденты

Выявление, анализ и обработка инцидентов



СПАСИБО ЗА ВНИМАНИЕ!