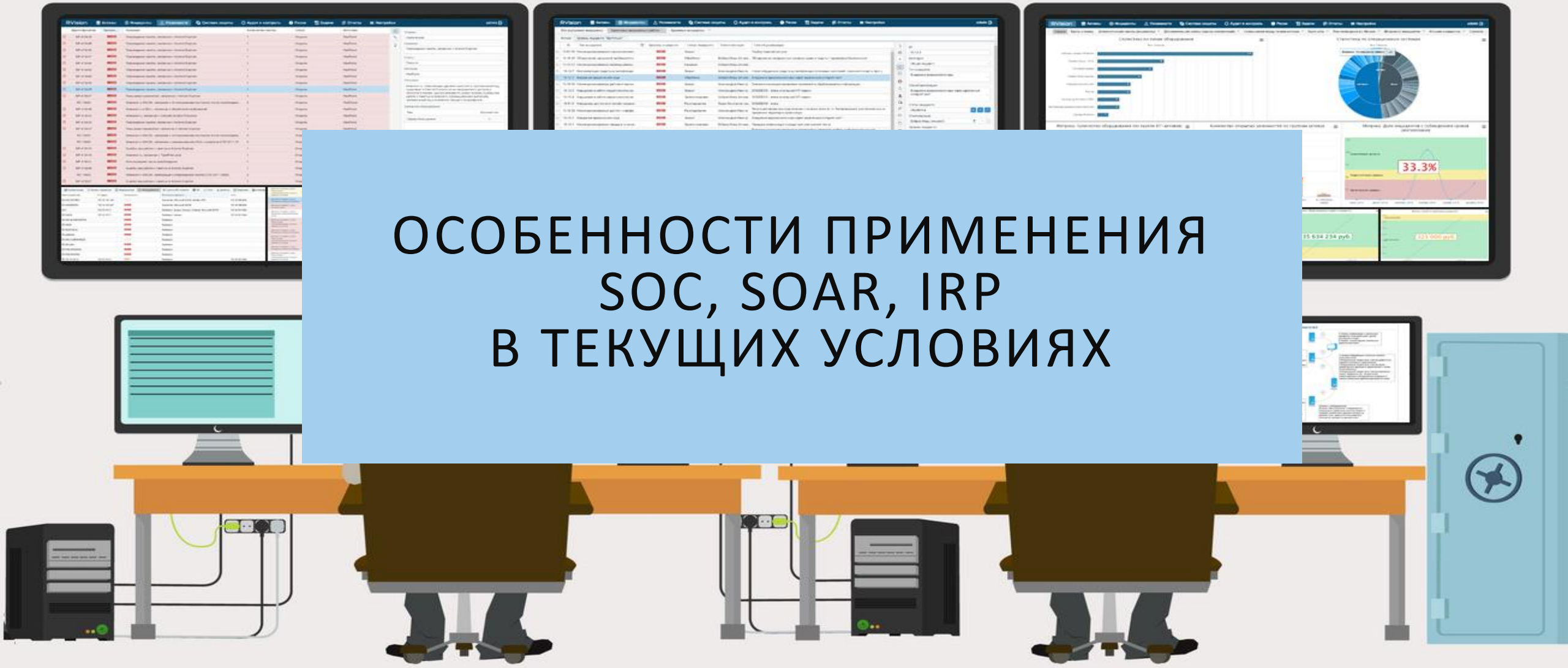


ОСОБЕННОСТИ ПРИМЕНЕНИЯ SOC, SOAR, IRP В ТЕКУЩИХ УСЛОВИЯХ

КОНСТАНТИН САМАТОВ

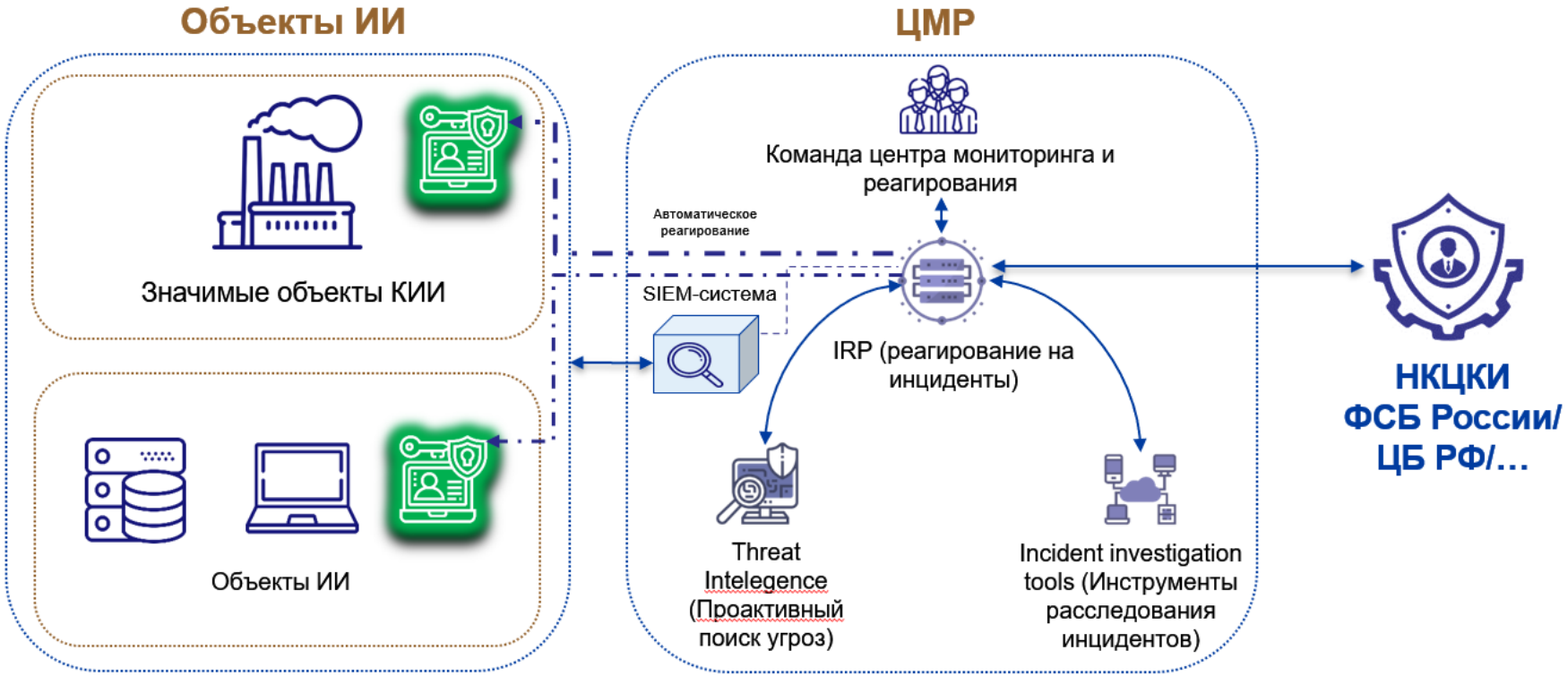
Член Правления Ассоциации руководителей служб информационной безопасности

ИМПОРТОЗАМЕЩЕНИЕ АББРЕВИАТУР

Security Operation Center (SOC) – Центр мониторинга и реагирования на инциденты информационной безопасности (ЦМРИИБ) или КЦ ГосСОПКА (подвид)

Security Orchestration, Automation and Response (SOAR) – система автоматизации реагирования на инциденты ИБ (САРИИБ)

Incident Response Platform (IRP) – платформа автоматизации реагирования (расследования) на инциденты ИБ (ПАРИИБ)



ОСОБЕННОСТИ ТЕКУЩИХ УСЛОВИЙ

Массовые атаки

- (Бот) Сканирование внешнего периметра
- Вредоносные спам рассылки
- Роботизированный фишинг
- Атаки направленные на отказ в обслуживании (D(D)OS)

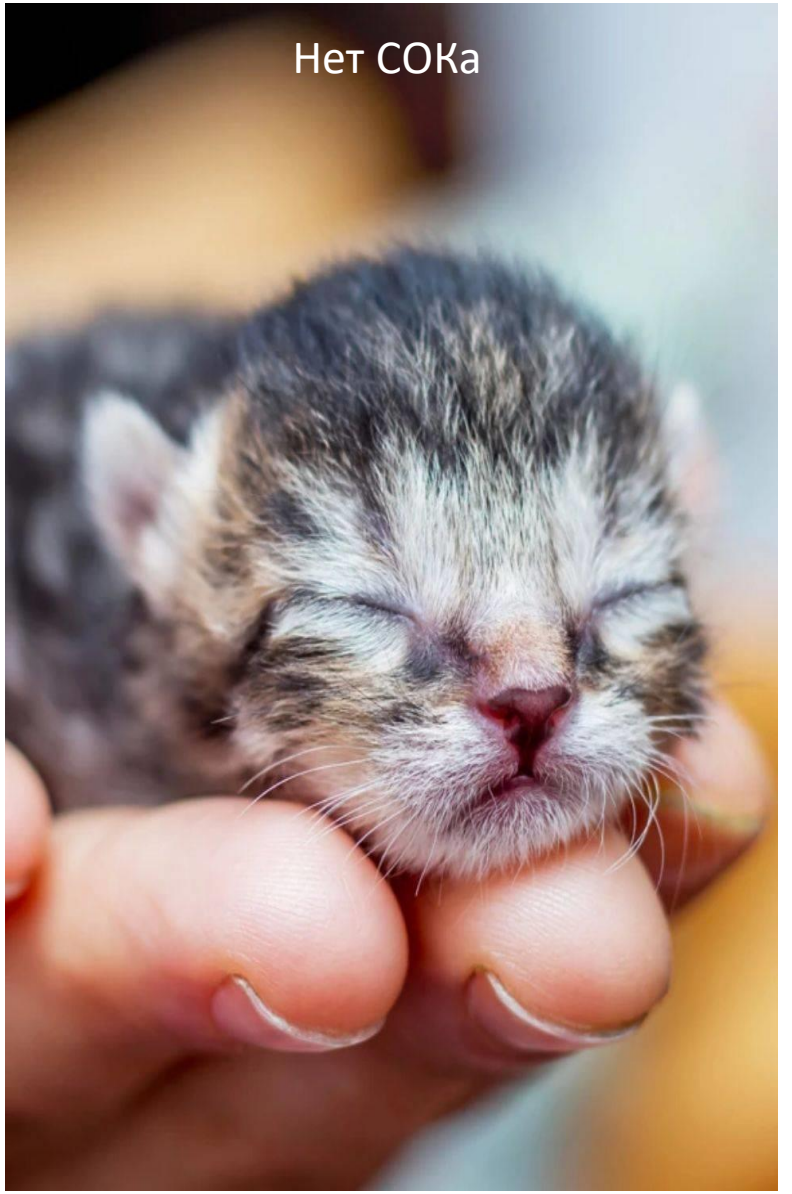
Сотрудник ГРИИБ

Счастливый
Довольный
Востребованный

Таргетированные атаки

- Распространение вредоносных файлов (программ) через фишинговые рассылки
- Проникновение в локальную сеть
- Эксплуатация уязвимостей
- Целенаправленные атаки APT-группировками (Advanced Persistent Threat)
- Атаки через поставщиков

Особенности применения ЦМР



Особенности применения САРИИБ (SOAR) и ПАРИИБ (IRP)

Жесткие настройки по рекомендациям регуляторов

Не решает организационные вопросы: реагирование на КА и КИ в нерабочее время

Стандартные алгоритмы реагирования (playbook) не работают

Нестандартные атаки для которых нет настроек

Спасибо за внимание!