

Л Е Т

ФОРМИРУЕМ ТРЕНДЫ  
ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ

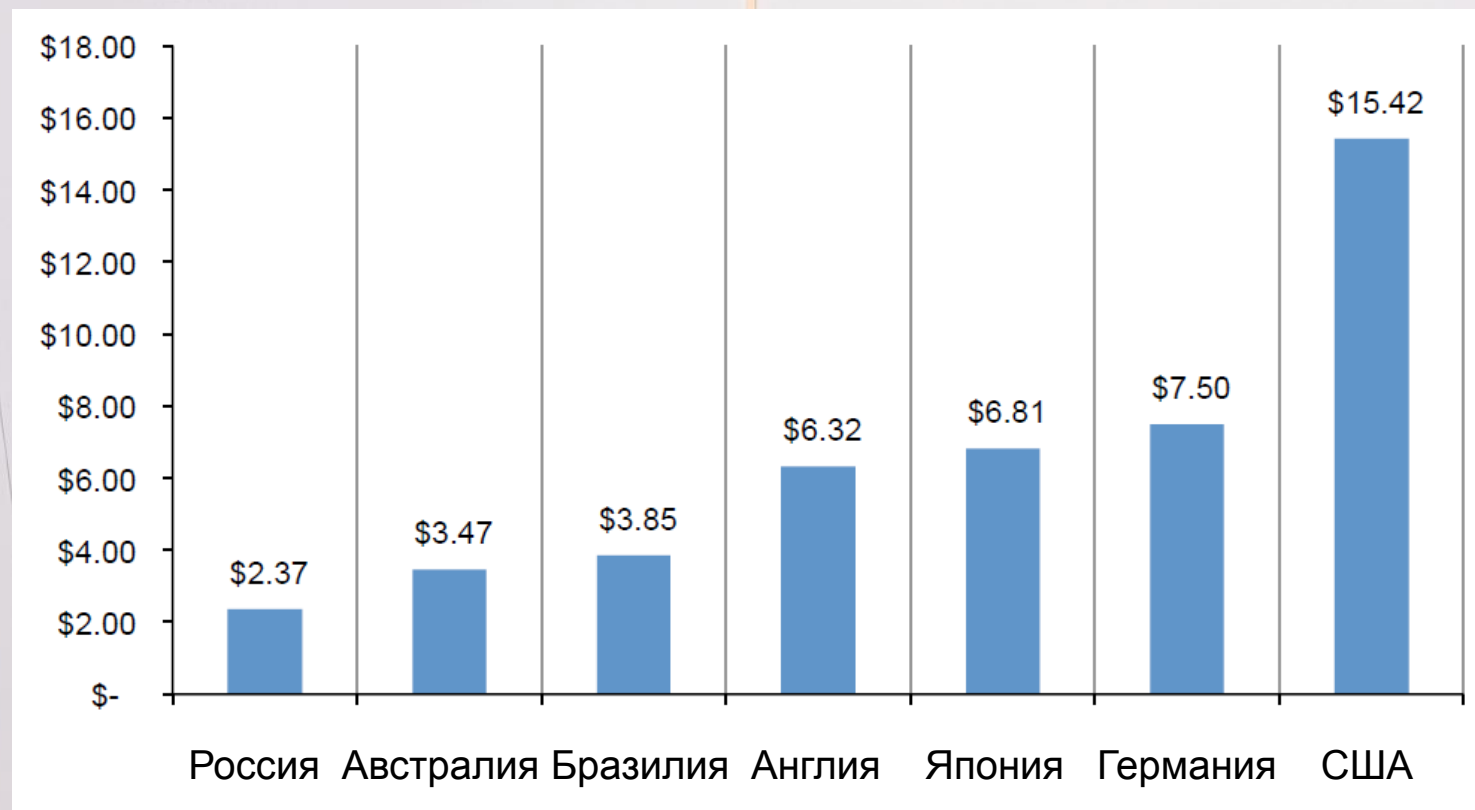
ИНФОСИСТЕМЫ ДЖЕТ



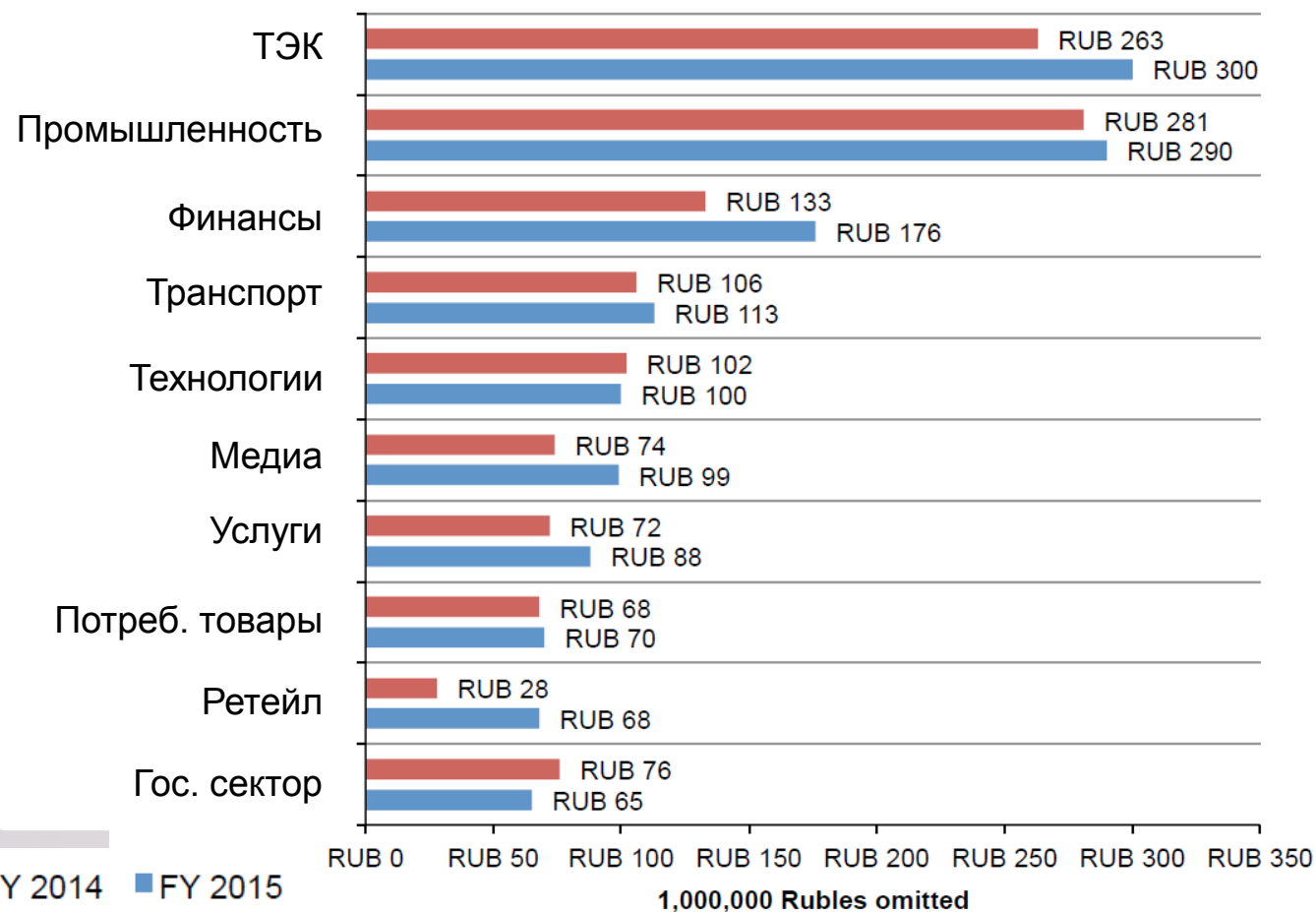
# Правила SOC. Метод «Инфосистемы Джет»

Тимур Ниязов,  
руководитель направления SOC и  
защиты баз данных  
Центра информационной безопасности

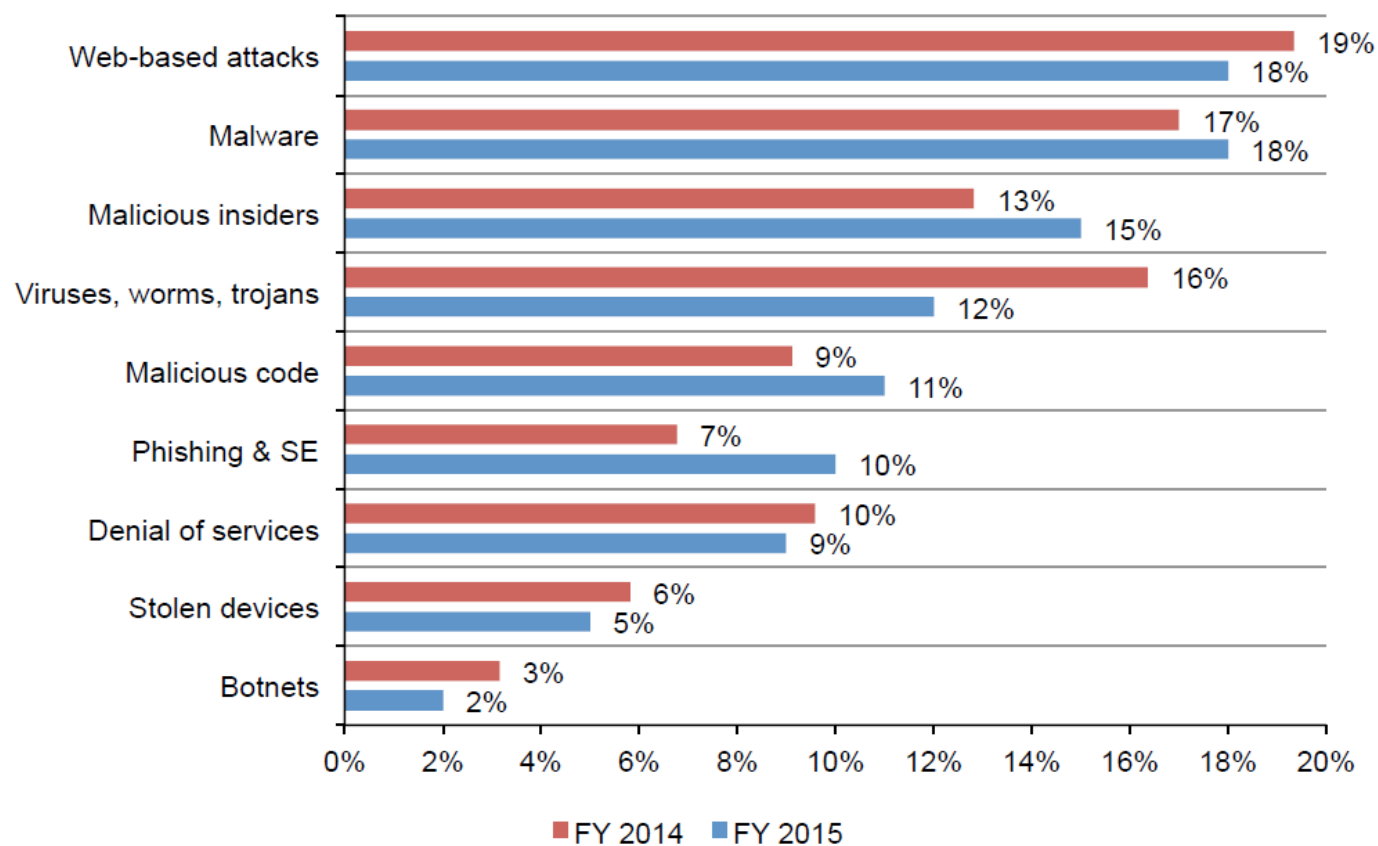
# Статистика по странам за 2015 год



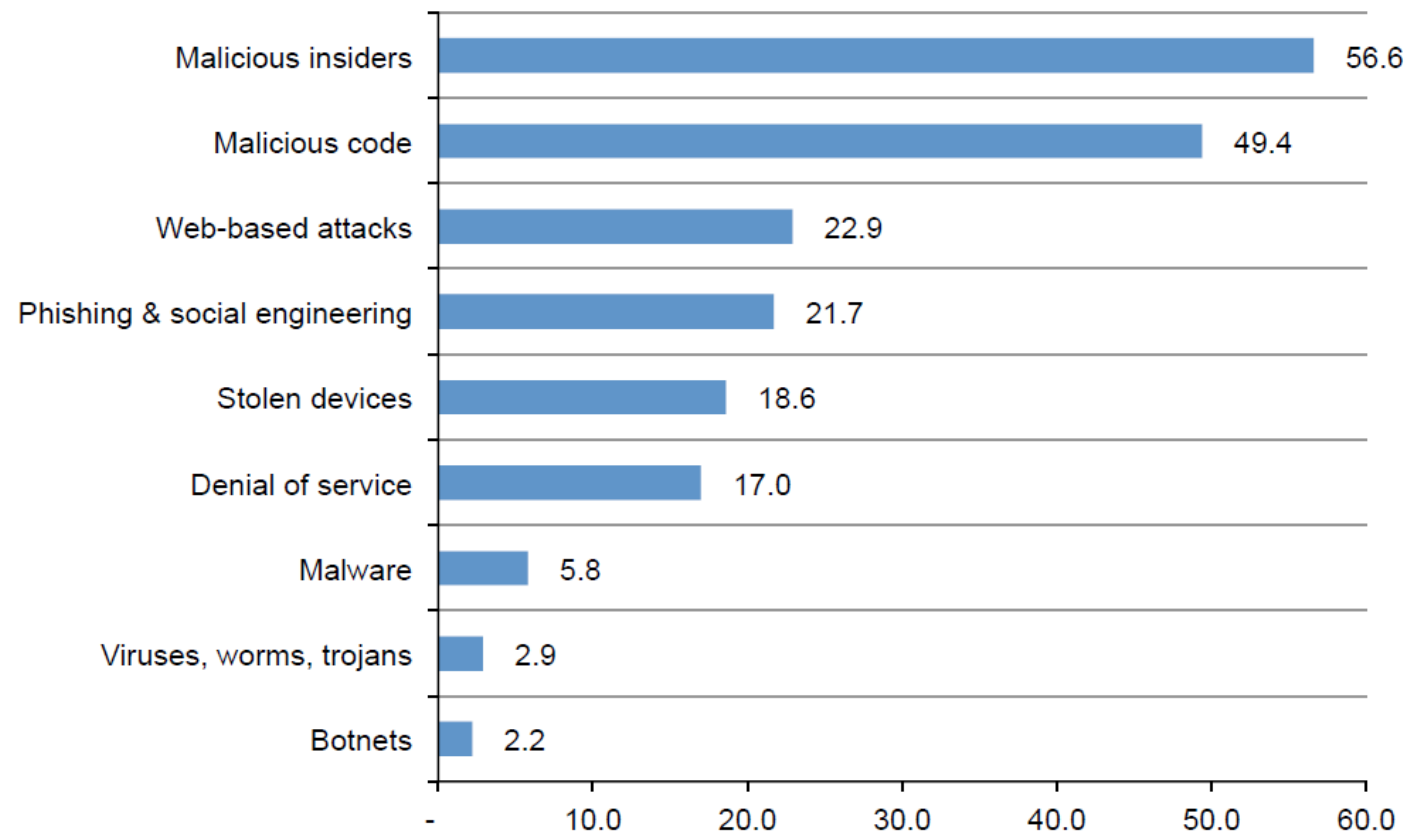
# Статистика по секторам за 2014-2015 год



# Статистика по типам атак



# Статистика по типам атак





## Security Operation Center

**Технологии**



**Процессы**



**Персонал**





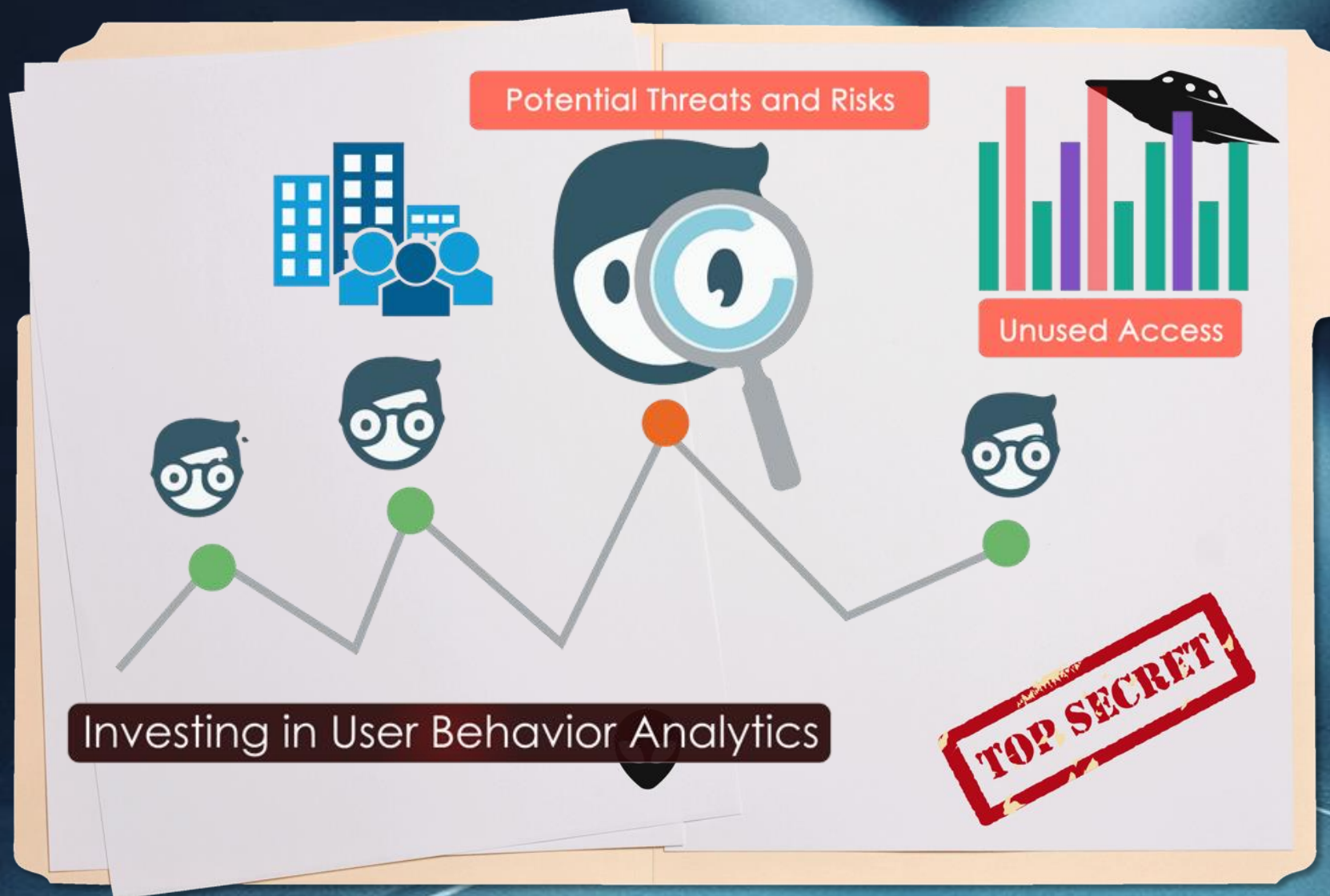


# Outsource VS Insource



Параметр	Insource	Outsource
Контроль	Полный	Частичный
Настройка под себя	Полностью	Стандартные сервисы
Скорость развертывания	До 2 лет	2 месяца
Стоимость	Дешевле через 3-5 лет	Дешевле на старте, OPEX
???	???	Предсказуемое





# Системы помощи принятия решения





## Security Operation Center

Технологии



Процессы



Персонал

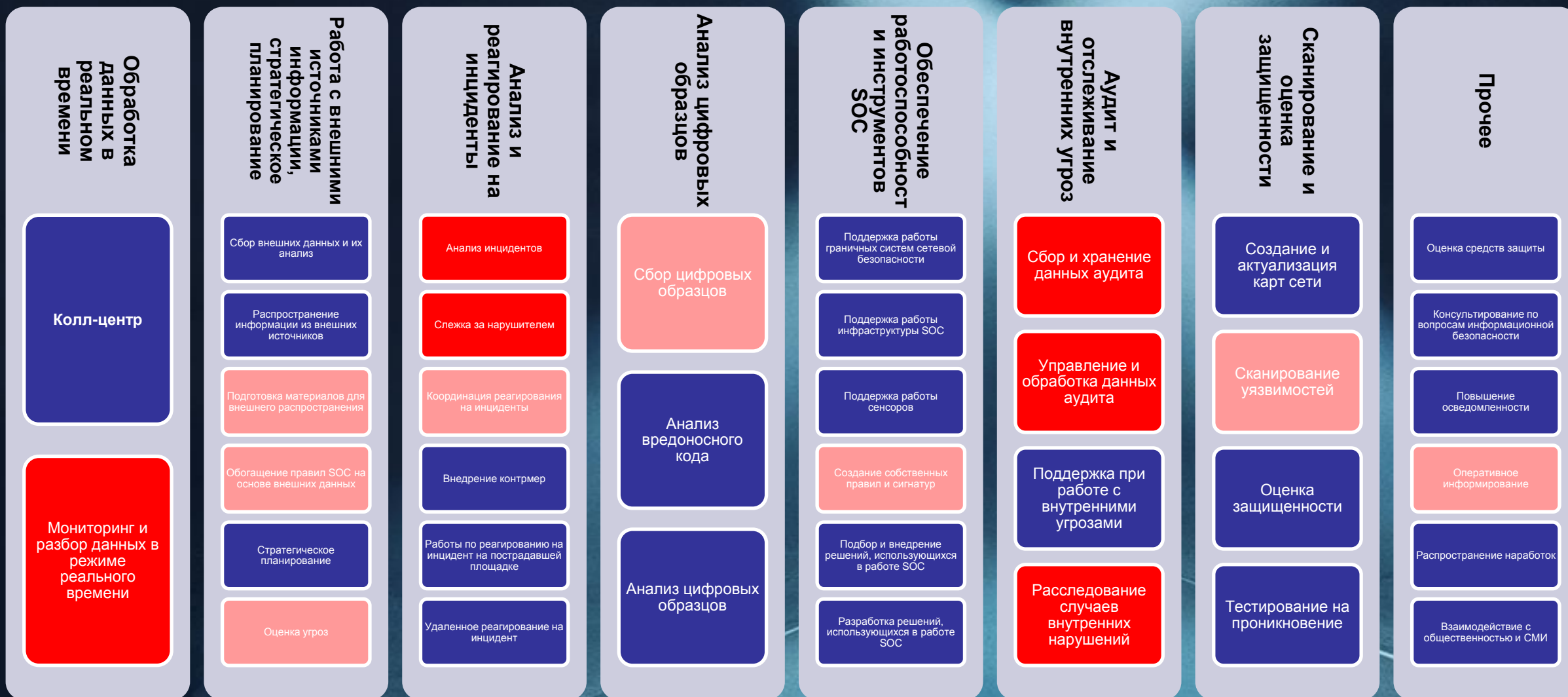


# SOC: функции

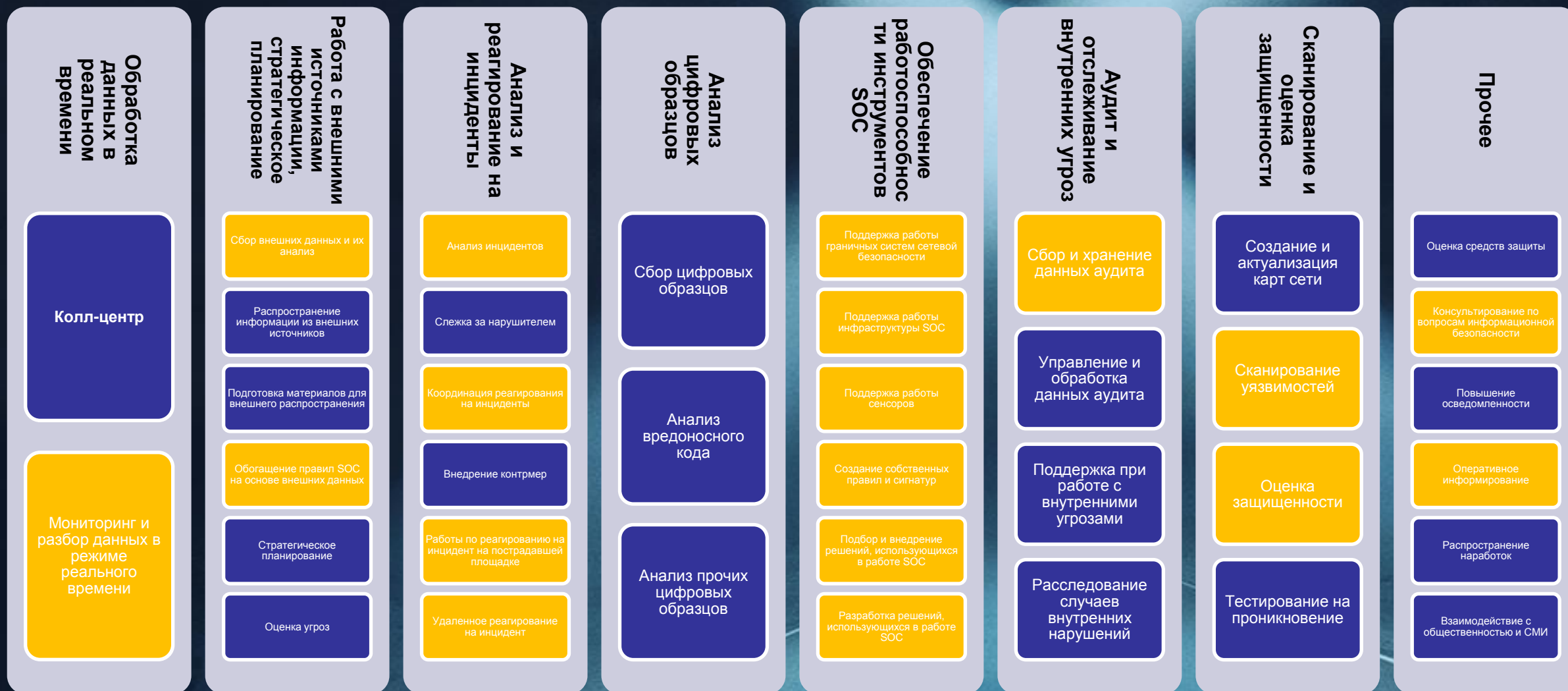




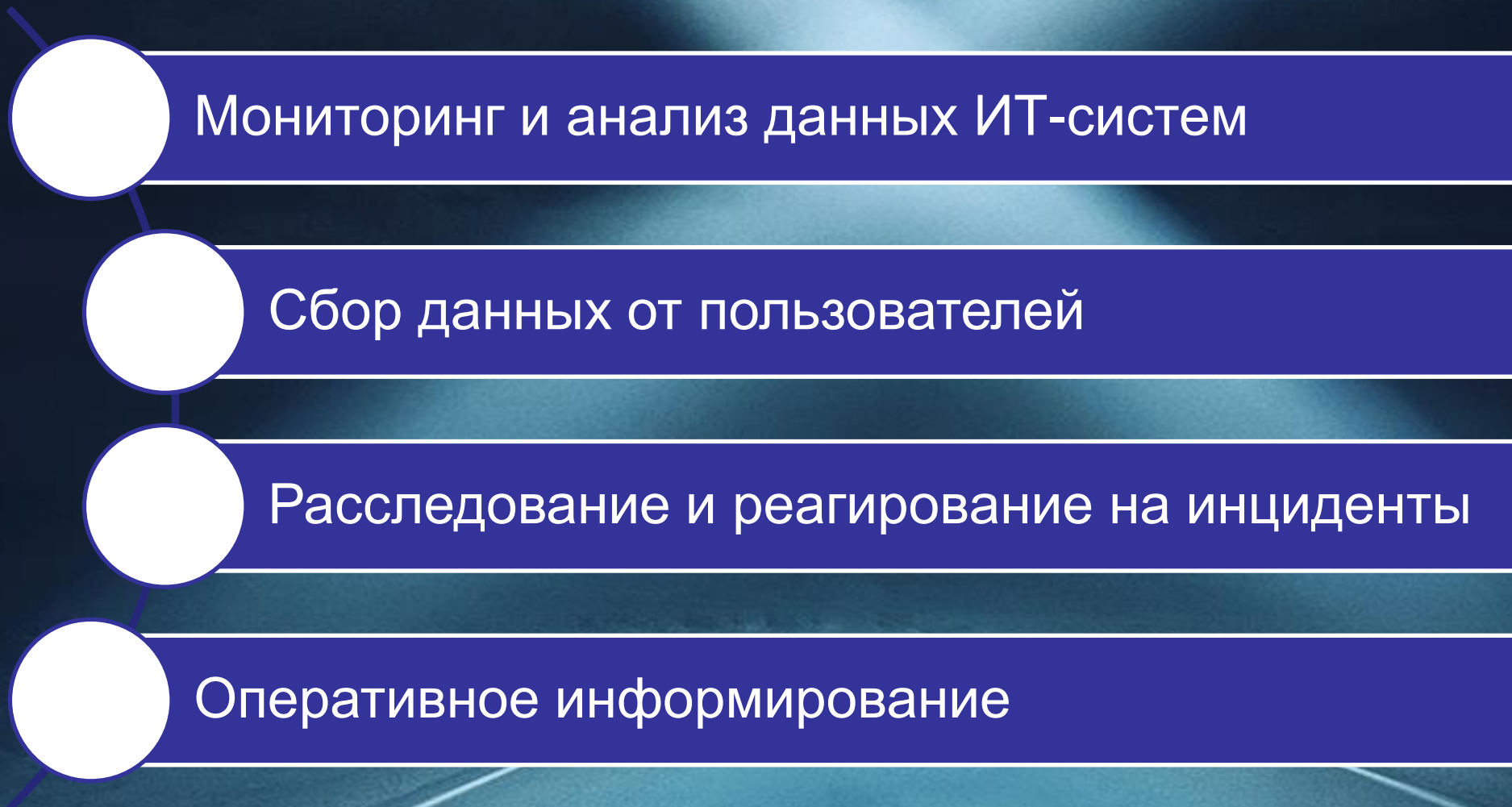
# SOC: использование инструмента SIEM



# SOC: использование инструмента SIEM



## SOC



## Security Operation Center

Технологии



Процессы



Персонал





- ✓ Background: администрирование серверов и сети, практическая безопасность (в т.ч. pentest), программирование
- ✓ Работники компании
- ✓ Ядро – звезды
- ✓ Часть ролей – другие подразделения, аутсорсинг



- ✓ Обучение по продуктам
- ✓ Обучение при приеме на работу
- ✓ Регулярный обмен опытом, ротации внутри SOC
- ✓ Анализ, обработка и распространение новостей в области ИБ
- ✓ Обмен опытом с другими SOC, участие в CERT
- ✓ Ясные KPI для сотрудников
- ✓ Обучение не только сотрудников SOC

ИНФОСИСТЕМЫ ДЖЕТ



Л Е Т

ФОРМИРУЕМ ТРЕНДЫ  
ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ

Спасибо за внимание!

TRUTH