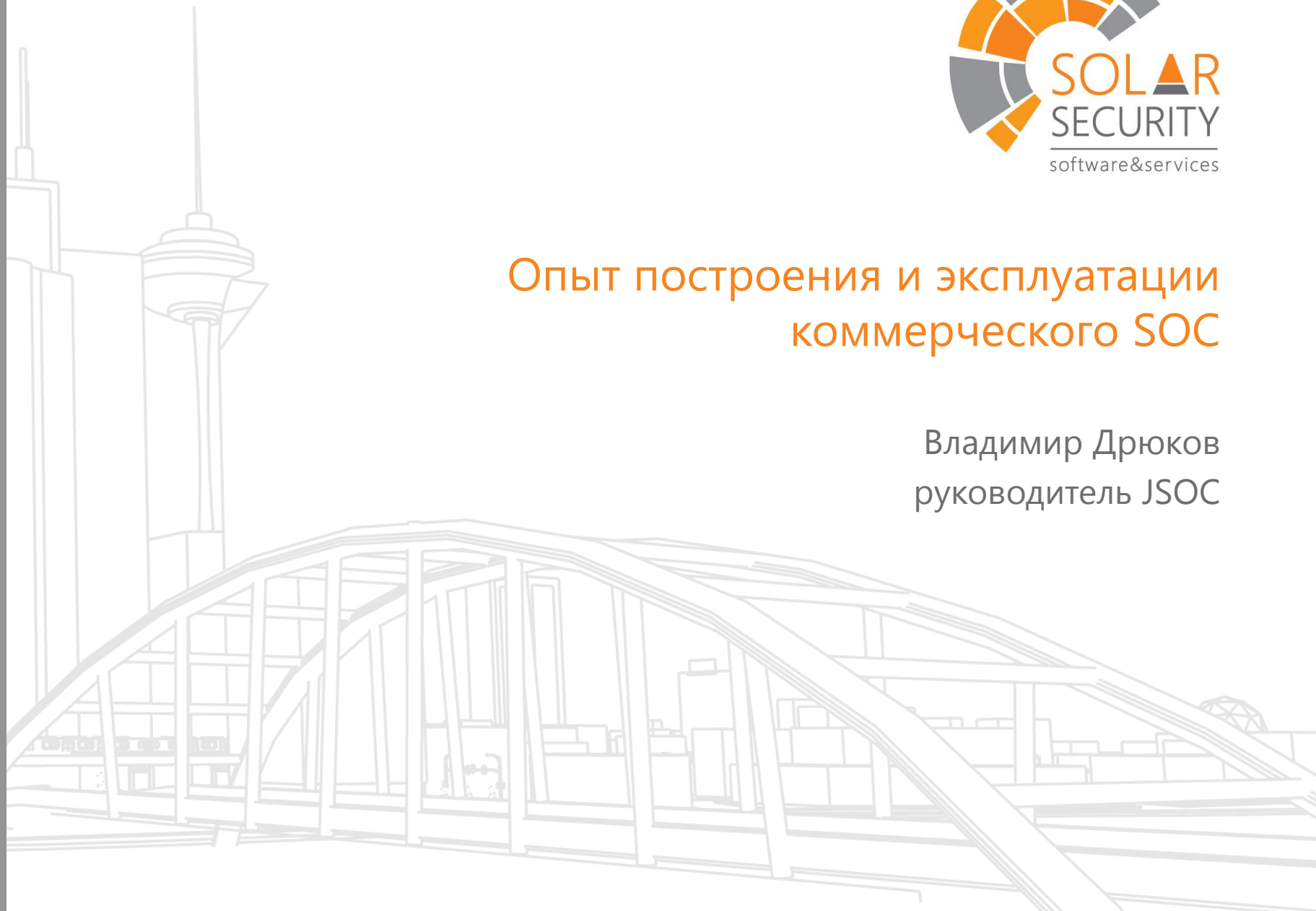


SOLAR SECURITY
software&services

Опыт построения и эксплуатации коммерческого SOC

Владимир Дрюков
руководитель JSOC

SOC – определения

Not every SOC has the same role. There are three different focus areas in which a SOC may be active, which can be combined in any combination:

- Control - focusing on the state of the security with compliancy testing, penetration testing, vulnerability testing, etc.
- Monitoring - focusing on events and the response with log monitoring, SIEM administration, and incident response
- Operational - focusing on the operational security administration such as identity & access management, key management, firewall administration, etc.

WIKIPEDIA
The Free Encyclopedia

Cybersecurity breaches at various organizations are becoming common news published almost daily. Another trend we can see from ICS-CERT alerts is that security breaches in utilities are also increasing. Irrespective of the size or type of the utility organization, it is important to ensure that there is an appropriate team with right skills and tools to identify, detect and defend against such breaches. Building a dedicated security team that provides SOC (Security Operations Centre)

SANS

"The SOC is responsible for monitoring, detecting, and isolating incidents and the management of the organization's security products, network devices, end-user devices, and systems. This function is performed seven days a week, 24 hours per day. The SOC is the primary location of the staff and the systems dedicated for this function."

McAfee

Функции SOC

- Готовность к отражению атаки – контроль защищенности инфраструктуры
  - Выявление и устранение уязвимостей
  - Контроль конфигураций сетевого оборудования
  - Обеспечение полноты покрытия и функционала СЗИ
  - Своевременное выявление «болевых точек» инфраструктуры и бизнес-процессов
  - Сбор информации по киберугрозам, разработка мер выявления и противодействия

- Управление инцидентами:
  - Своевременное выявление и анализ атаки (как внешней, так и внутренней)
  - Оперативное противодействие (в течении нескольких часов или быстрее)
  - Выработка мер по неповторению инцидента

- Технический контроль compliance:
  - Внутренний анализ рисков и политика ИБ
  - Требования регуляторов

Функции SOC, которые можно передать на аутсорсинг

- Готовность к отражению атаки – контроль защищенности инфраструктуры
  - Выявление и устранение уязвимостей
  - Контроль конфигураций сетевого оборудования
  - Обеспечение полноты покрытия и функционала СЗИ
  - Своевременное выявление «болевых точек» инфраструктуры и бизнес-процессов
  - Сбор информации по киберугрозам, разработка мер выявления и противодействия

- Управление инцидентами:
  - Своевременное выявление и анализ атаки (как внешней, так и внутренней)
  - Оперативное противодействие (в течении нескольких часов или быстрее)
  - Выработка мер по неповторению инцидента

- Технический контроль compliance:
  - Внутренний анализ рисков и политика ИБ
  - *Требования регуляторов*

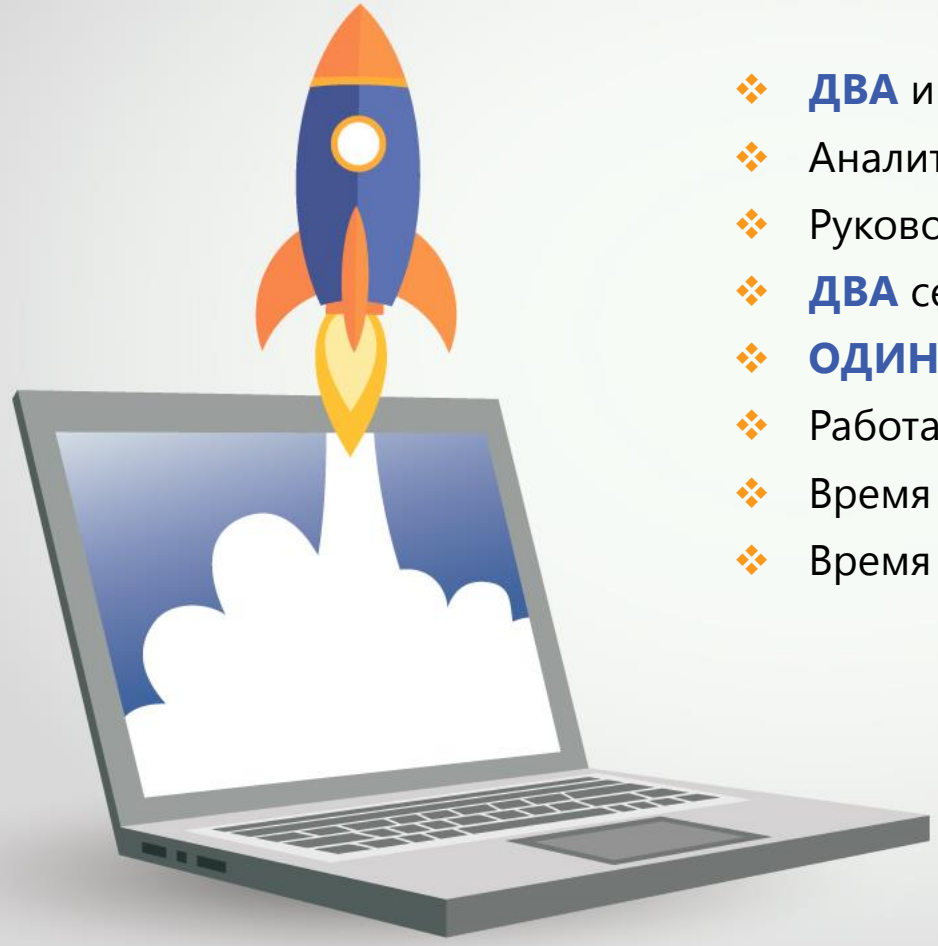
JSOC – TTX

26 клиентов	**192** инцидента ИБ в день	**82** системы ИБ в эксплуатации
80+ запросов эксплуатации в день	**10 мин** Время реакции на инцидент	**30 мин** Время анализа/ противодействия

Основные сервисы:

- Мониторинг и реагирование на инциденты
- Контроль защищенности инфраструктуры
- Защита онлайн сервисов
- Эксплуатация систем ИБ

Стартовые показатели JSOC:



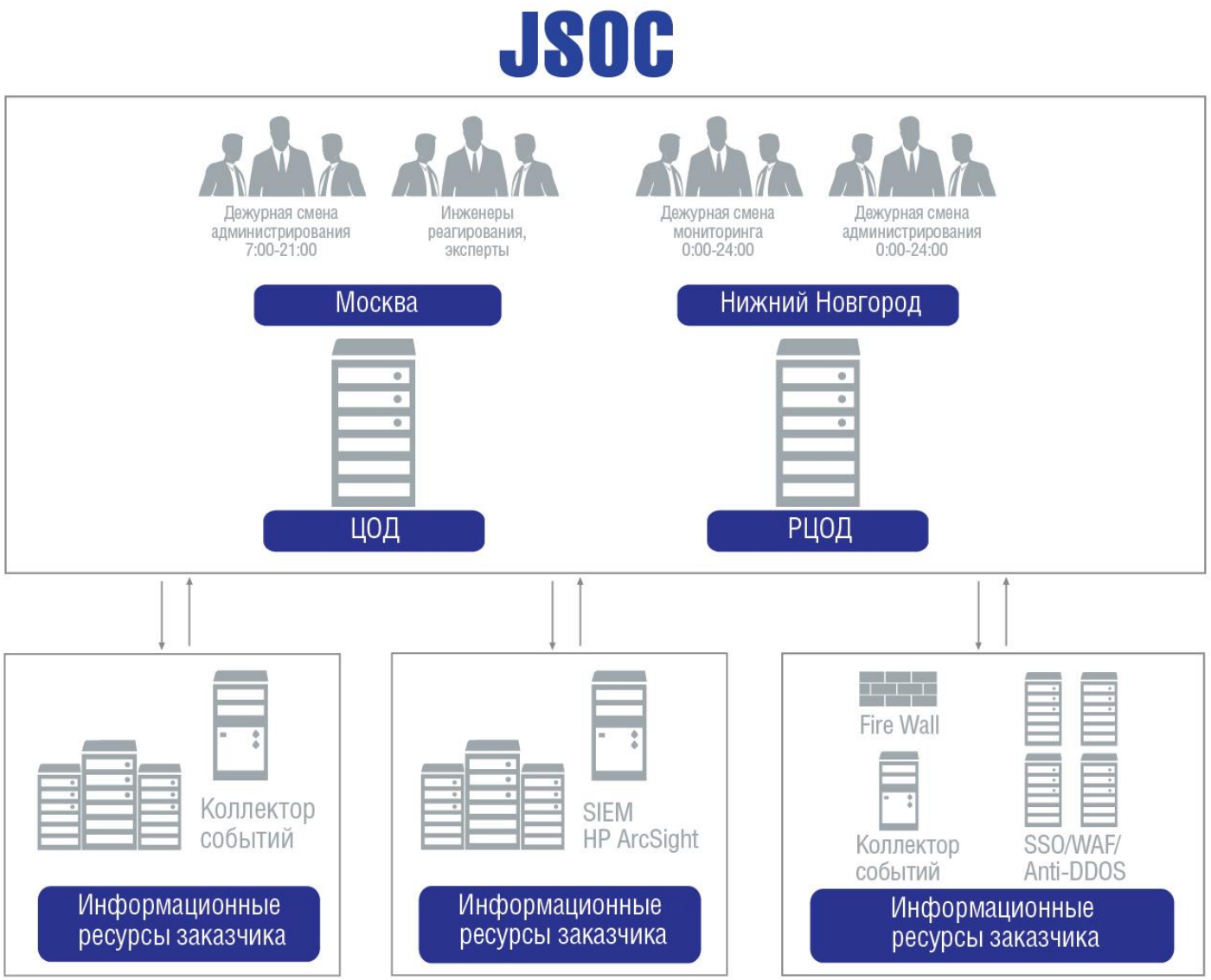
- **ДВА** инженера мониторинга
- Аналитик
- Руководитель направления
- **ДВА** сервера в кластерной конфигурации
- **ОДИН** заказчик, **ТРИ** пилотных проекта
- Работа **8*5**
- Время реакции – **30 МИНУТ**
- Время анализа – **2 ЧАСА**

JSOC – основные вехи

5 граблей на пути к SOC

- Можно доверять «ноу-хау» и практикам вендоров
- 1-я линия может работать по базовым инструкциям
- Нужно контролировать длинные векторы атаки
- Репутационные базы вендоров – просто и удобно
- ИТ и ИБ заказчика все знает о своей инфраструктуре и процессах

Инфраструктура JSOC



Оргструктура JSOC

Руководитель департамента JSOC

Группа развития JSOC

(пресейл-аналитик, архитектор, ведущий аналитик)

Группа управления качеством и бизнес-анализа

(сервис-менеджеры, 4 человека)

Группа разбора инцидентов

Выделенные аналитики (Москва+НН, 5 человек)

Инженеры реагирования и противодействия – 12*5 (Москва, 2 человека)

Инженеры мониторинга – 24*7 (НН, 6 человек)

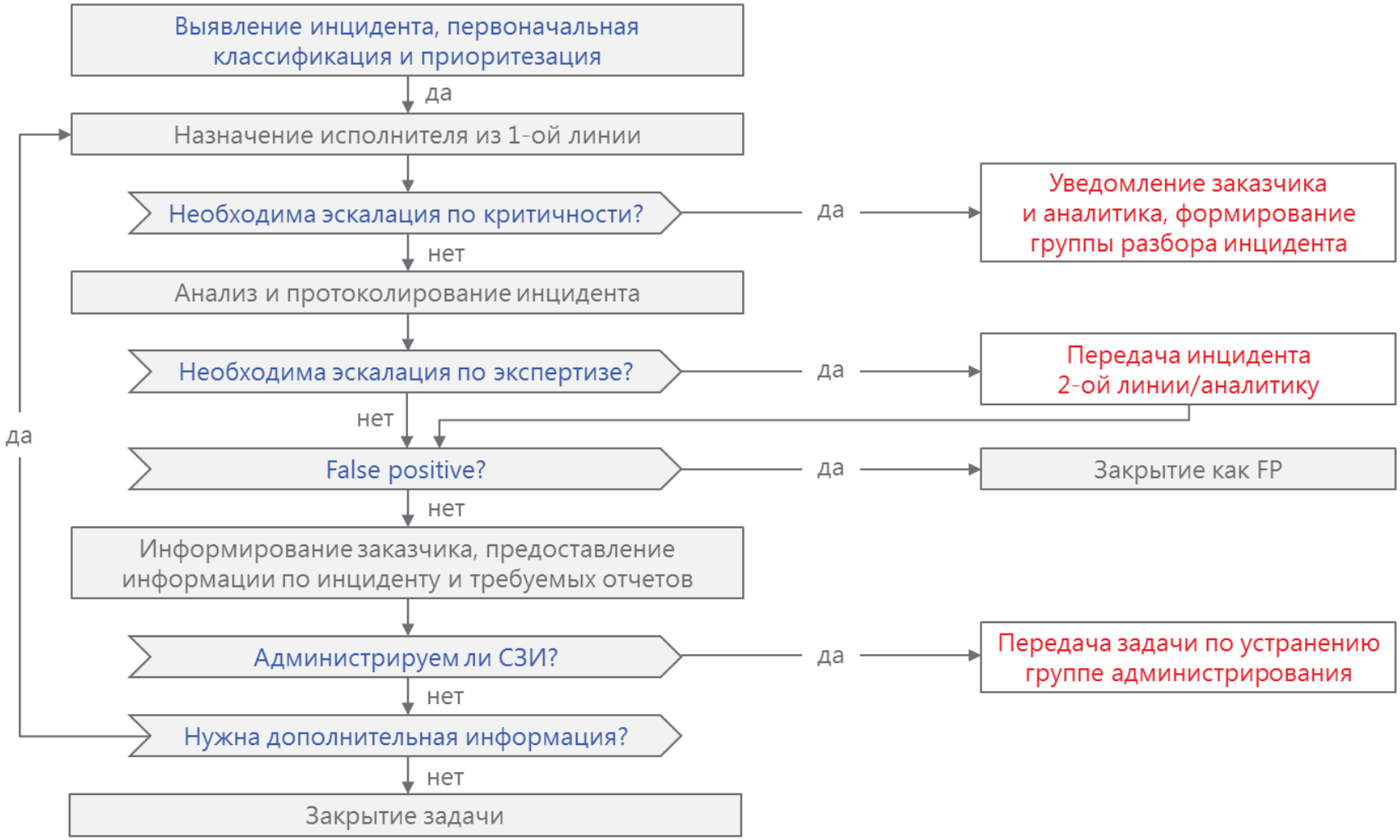
Группа эксплуатации

Администраторы ИБ – эксперты (Москва, 2 человека)

2-ая линия администрирования – 12*5 (Москва+НН, 5 человек)

1-ая линия администрирования – 24*7 (НН, 6 человек)

Процессы JSOC



Задачи JSOC

- Быстрое предоставление функции безопасности клиенту

- Получение объективной картины защищенности и состояния ИБ компании

- Сбор эффективной информация о киберугрозах и противодействие атакам

- Бизнес-анализ ИБ, выявление и контроль ключевых болевых точек

Дрюков Владимир,
Solar JSOC
v.dryukov@solarsecurity.ru
+7 (926) 589 92 85