



**2025**

## **СОС-НАЯ КАРЬЕРА**

**Калугина  
Алёна**

Ведущий инженер по информационной безопасности  
Центра информационной безопасности «Инфосистемы Джет»  
[as.kalugina@jet.su](mailto:as.kalugina@jet.su)



## Калугина Алёна Сергеевна

### Ведущий инженер по ИБ

Опыт работы в ИБ – более 6 лет

Образование: Университет ИТМО, Факультет безопасности информационных технологий

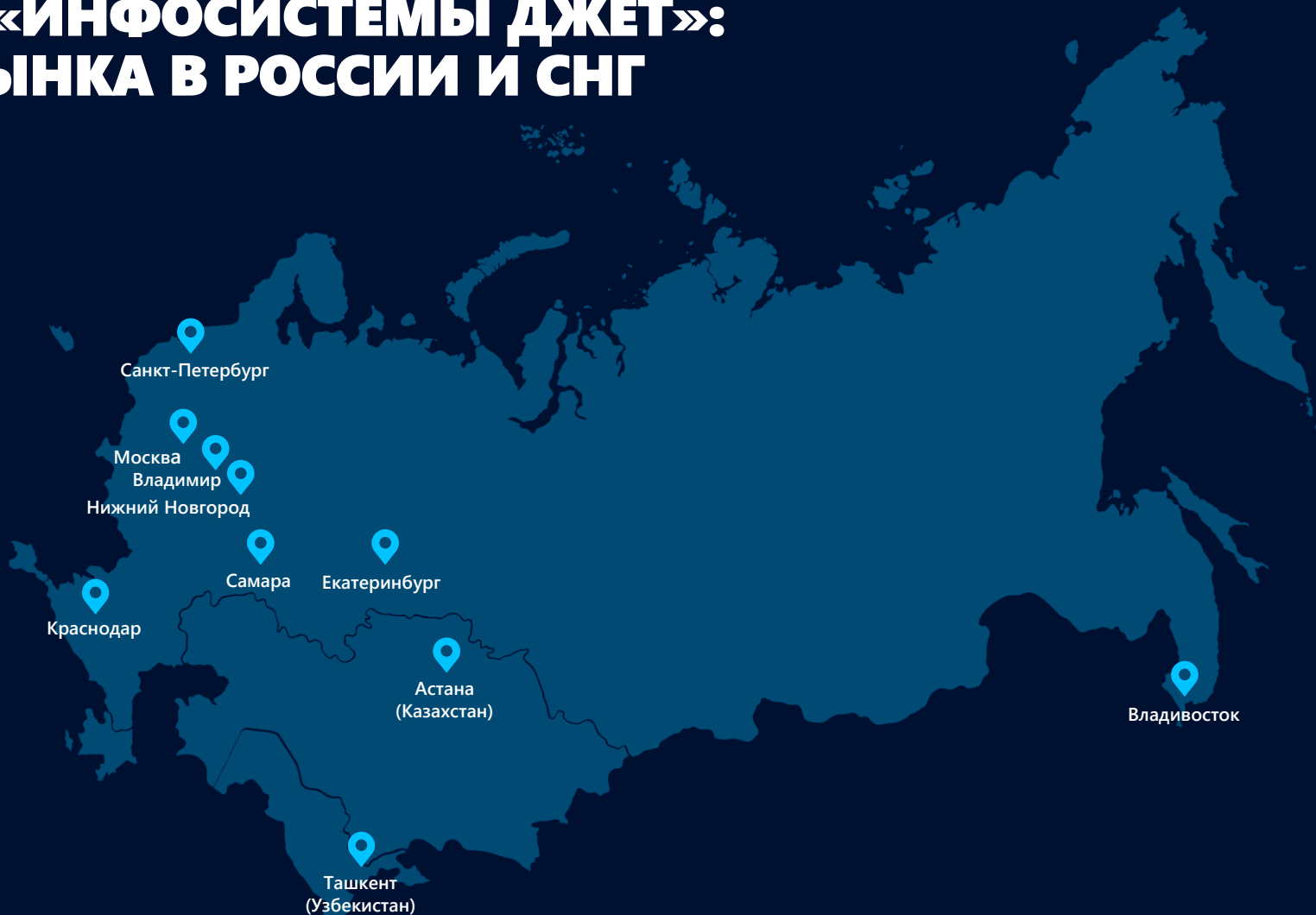
#### Направления работы:

- Построение гибридных, облачных и In-house SOC;
- Проектирование и внедрение средств защиты информации классов: SIEM, SOAR, VM, UEBA, EDR;
- Экспертный аудит SOC.

# КОМПАНИЯ «ИНФОСИСТЕМЫ ДЖЕТ»: ЛИДЕР ИТ-РЫНКА В РОССИИ И СНГ



- Опыт реализации крупных проектов федерального и международного масштаба
- Отраслевые решения и собственная линейка продуктов
- Обширная база знаний
- Виртуальный ЦОД для корпоративных заказчиков



- Более 1700 квалифицированных сотрудников
- Крупнейший на территории Восточной Европы Сервисный Центр для решений корпоративного класса
- Развитая региональная сеть:

**БОЛЕЕ**  
**10** **офисов**  
**В РОССИИ И СНГ**

РАБОТАЕТ С **1991 г.**  
НА ИТ-РЫНКЕ

ВХОДИТ В **ТОП 10**  
ИТ-КОМПАНИЙ РОССИИ

**№1**  
В ИТ-АУТСОРСИНГЕ

Все необходимые лицензии и сертификаты, включая:





---

# ЧТО ТАКОЕ SOC И ДЛЯ ЧЕГО ОН НУЖЕН?

# МОНИТОРИНГ ИБ



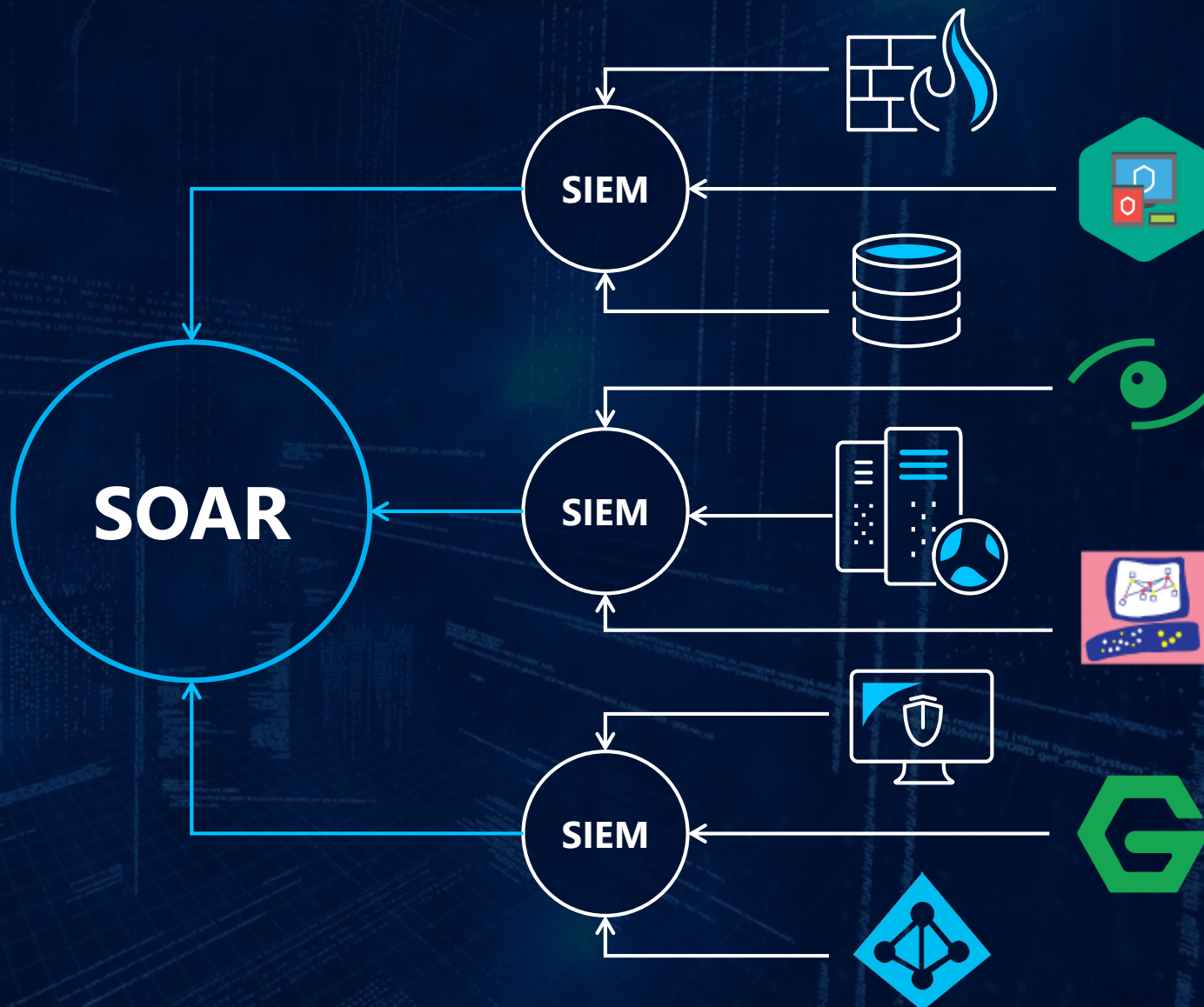
# SIEM/SOAR-СИСТЕМЫ



- **SIEM**  
(Security Information and Event Management)

- **SOAR**  
(Security Orchestration, Automation and Response)

платформа реагирования на инциденты





---

# **ЦВЕТНЫЕ КОМАНДЫ:**

**BLUE TEAM**

**RED TEAM**

**PURPLE TEAM**

**YELLOW TEAM**

# АНАЛИТИКИ МОНИТОРИНГА



Инцидент-менеджер



## Линия 3

- Глубокий анализ и расследование инцидентов (APT-атаки)
- Проактивный поиск угроз ИБ (Threat Hunting)
- Управление данными об угрозах ИБ (Threat Intelligence)
- Форензика
- Реверс-инжиниринг
- RND

## Линия 2

- Глубокий анализ инцидентов и расследование инцидентов
- Управление уязвимостями
- Разработка и актуализация контента SOC
- Подготовка отчетов

## Линия 1

- Мониторинг инцидентов 24/7
- Работа с жизненным циклом инцидента
- Базовая аналитика и классификация инцидентов
- Сбор данных и оповещение 2-ой линии

# КАКИЕ ЗНАНИЯ И НАВЫКИ НЕОБХОДИМЫ ДЛЯ СПЕЦИАЛИСТА ИБ 1-ОЙ ЛИНИИ?

Модель ISO/OSI, практически  
навыки работы в CiscoPacketTracer

Администрирование Windows

Администрирование Linux

Понимание основ ИБ

Умение грамотно общаться  
с заказчиком

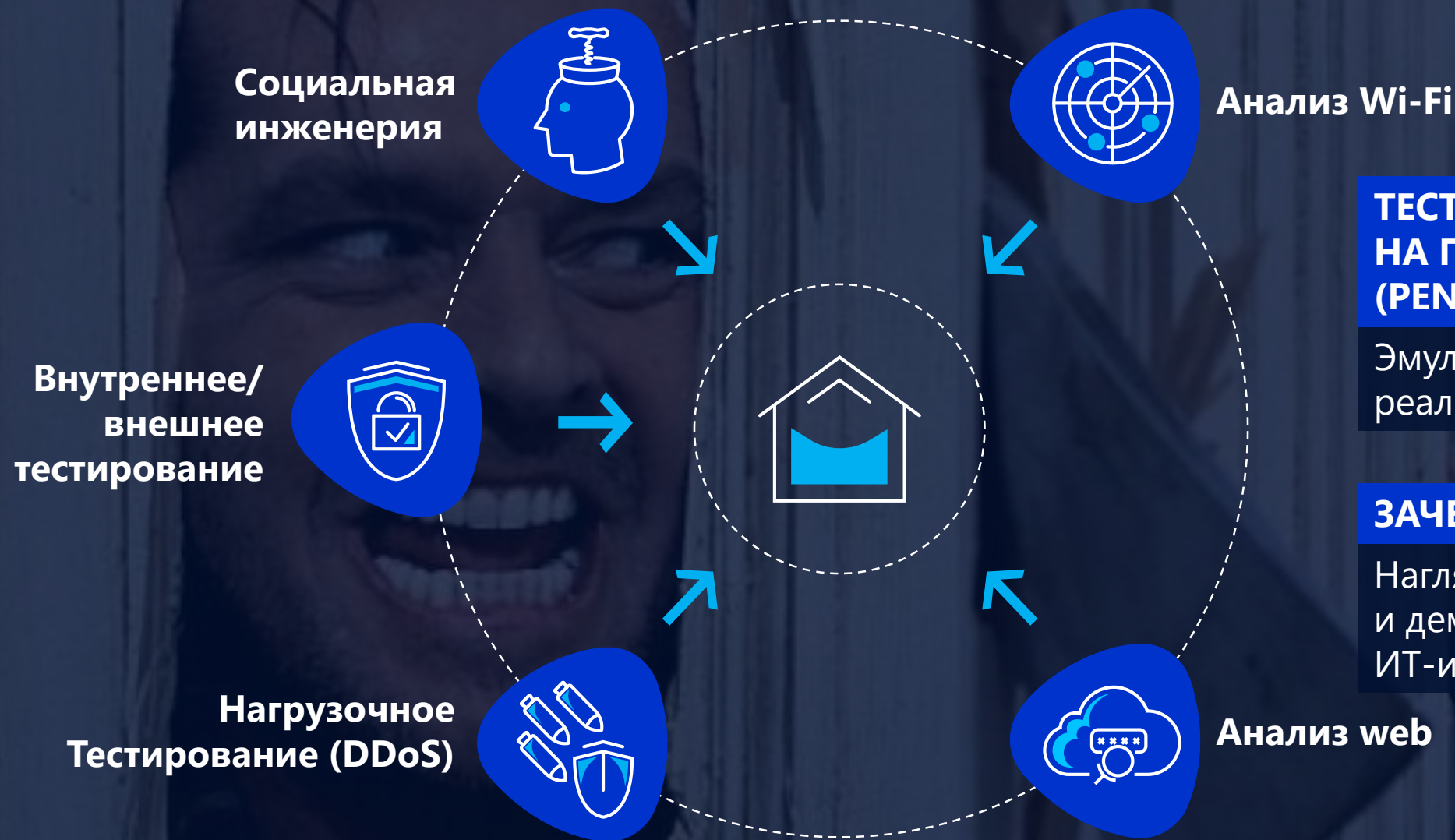
Стрессоустойчивость и готовность  
включиться в работу 24/7



# КАКИЕ ЗНАНИЯ И НАВЫКИ НЕОБХОДИМЫ ДЛЯ АНАЛИТИКА 2-ОЙ И 3-ЕЙ ЛИНИИ?



# ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ (RED TEAM)



## ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ (PENTEST)

Эмуляция действий реальных злоумышленников

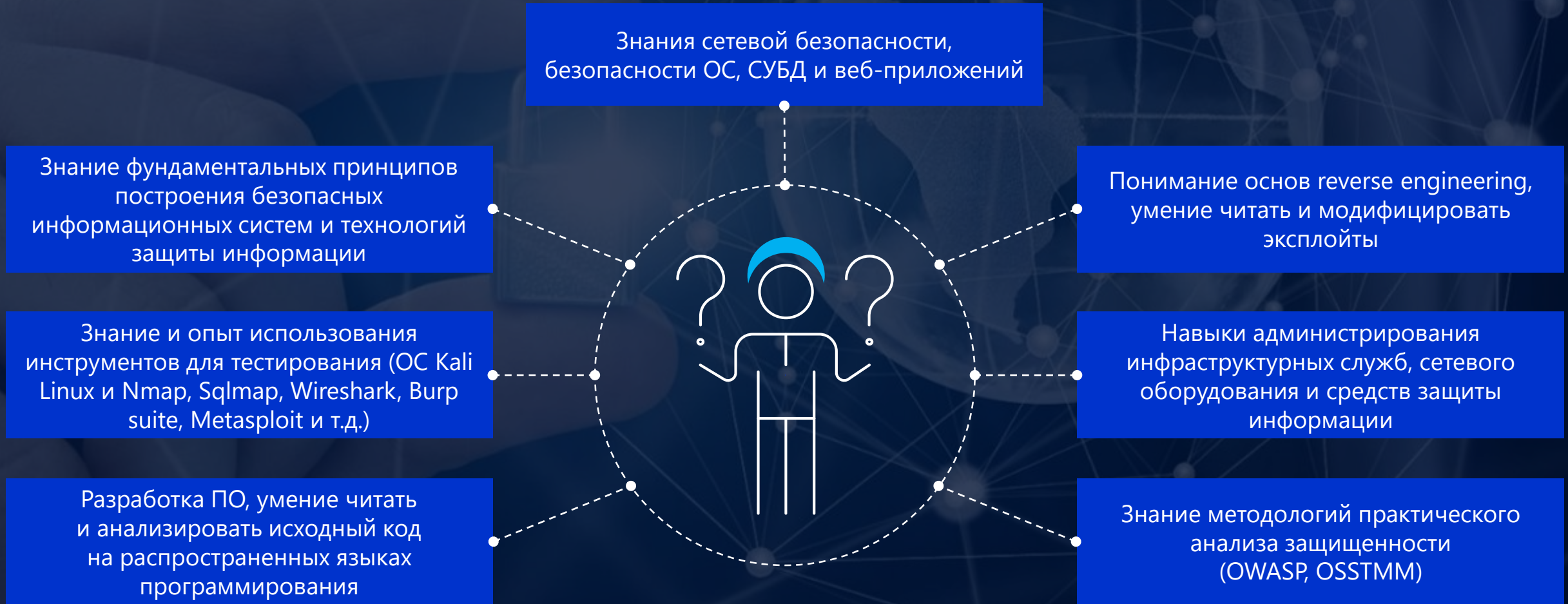
## ЗАЧЕМ

Наглядный способ поиска и демонстрации проблем в ИТ-инфраструктуре

# ОСНОВНЫЕ ЭТАПЫ



# КАКИЕ ЗНАНИЯ И НАВЫКИ НЕОБХОДИМЫ ДЛЯ ПЕНТЕСТЕРА?



# RED TEAM & BLUE TEAM = PURPLE TEAM

## RED TEAM

- Поиск уязвимостей
- Проведение атак
- Уклонение
- Соц. инженерия

## PURPLE TEAM

- Повышение эффективности
- Проработка TTP и kill-chain APT-атак

## BLUE TEAM

- Обнаружение
- Реагирование
- Предотвращение



**PURPLE TEAM** –  
коллаборация Red Team и Blue Team, использующая  
тактики обеих команд, которая поможет повысить  
эффективность вашего SOC!

# ЧТО ТАКОЕ PURPLE TEAMING?



**PURPLE TEAMING** — имитация реальных кибератак с последующим анализом процессов мониторинга и реагирования

## ПРЕИМУЩЕСТВА:

- Имитация атак максимально приближена к реальности
- Возможность протестировать техники и процедуры, с которыми SOC ещё не сталкивался
- Обнаружение неработающих или неправильно настроенных правил выявления инцидентов, неподключенных источников событий и сетевых сегментов, ограничений лицензии ПО

## ОСОБЕННОСТИ ПОДХОДА:

- Red Team имитирует кибератаки, Blue Team анализирует эффективность их выявления и оценивает состояние SOC;
- Работы проводятся «белым ящиком»: Red Team анонсирует свои действия, Blue Team «позволяет» продолжать развитие атак при обнаружении Red Team для полного покрытия kill-chain сценария.

# YELLOW TEAM



Обучение персонала



Процессы ИБ



## ЗАЧЕМ

Документирование процессов по улучшению ИБ

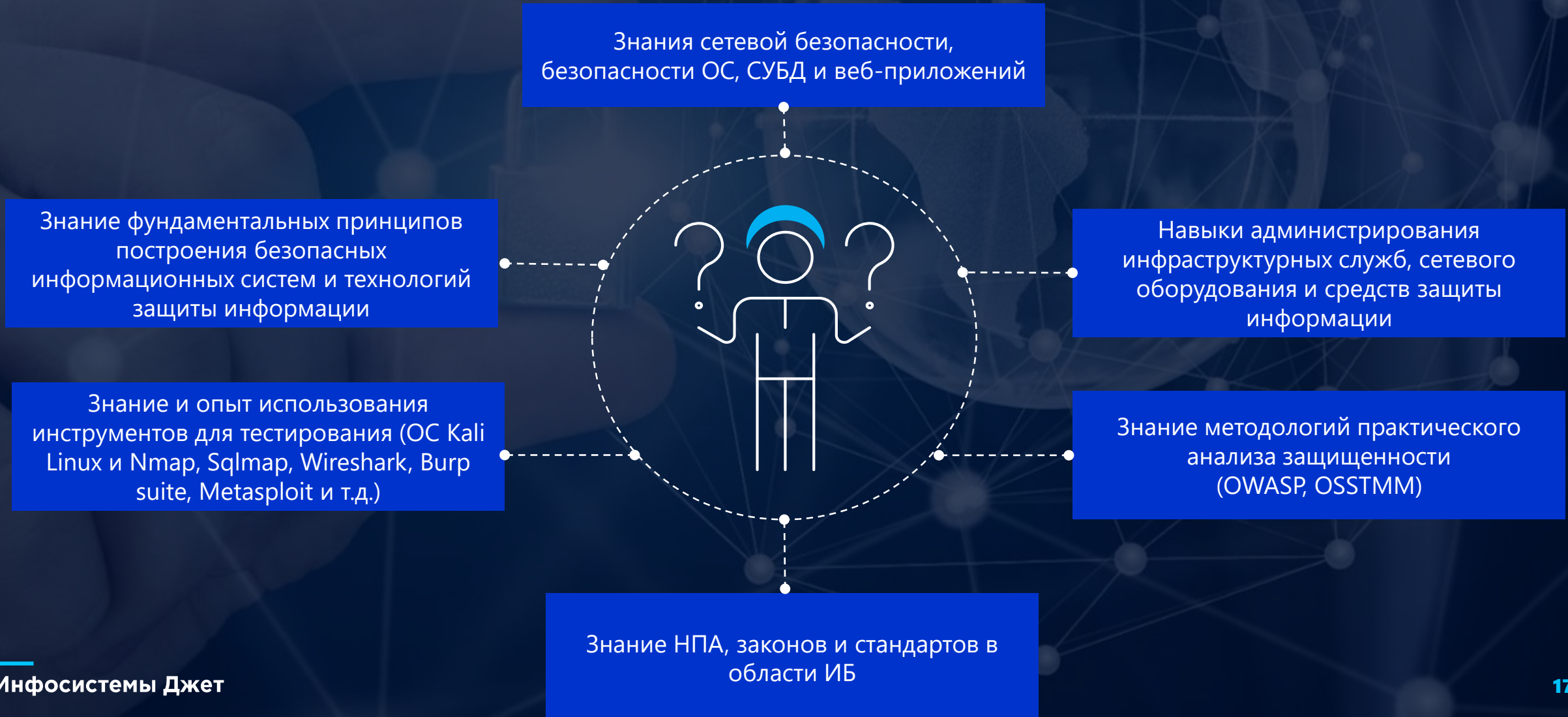
Политики ИБ



Аудит ИБ



# КАКИЕ ЗНАНИЯ И НАВЫКИ НЕОБХОДИМЫ ДЛЯ МЕТОДОЛОГА?



# ОБЯЗАННОСТИ ИНЖЕНЕРОВ ВНЕДРЕНИЯ



Проработка технических решений,  
стендовое моделирование

Разработка архитектуры и  
проектных решений для  
создаваемой системы

Взаимодействие с заказчиками  
на этапе реализации проекта



Внедрение разработанных  
технических решений  
в инфраструктуру заказчика

Взаимодействие  
с вендорами/дистрибьюторами

Разработка и согласование  
функциональных требований к  
создаваемой системе

# ОБЯЗАННОСТИ ИНЖЕНЕРОВ ЭКСПЛУАТАЦИИ SOC



Переработка архитектуры и проектных решений при масштабировании

Эксплуатация технологического ядра SOC на уровне ОС



Внедрение разработанных технических решений в инфраструктуру

Взаимодействие с вендорами/дистрибьюторами



# УСЛУГИ SOC

# С ЧЕГО НАЧИНАЕТСЯ БЕЗОПАСНОСТЬ?

## АУДИТОР SOC



Анализ документации  
и аудит процессов SOC



Аудит технологического  
ядра SOC



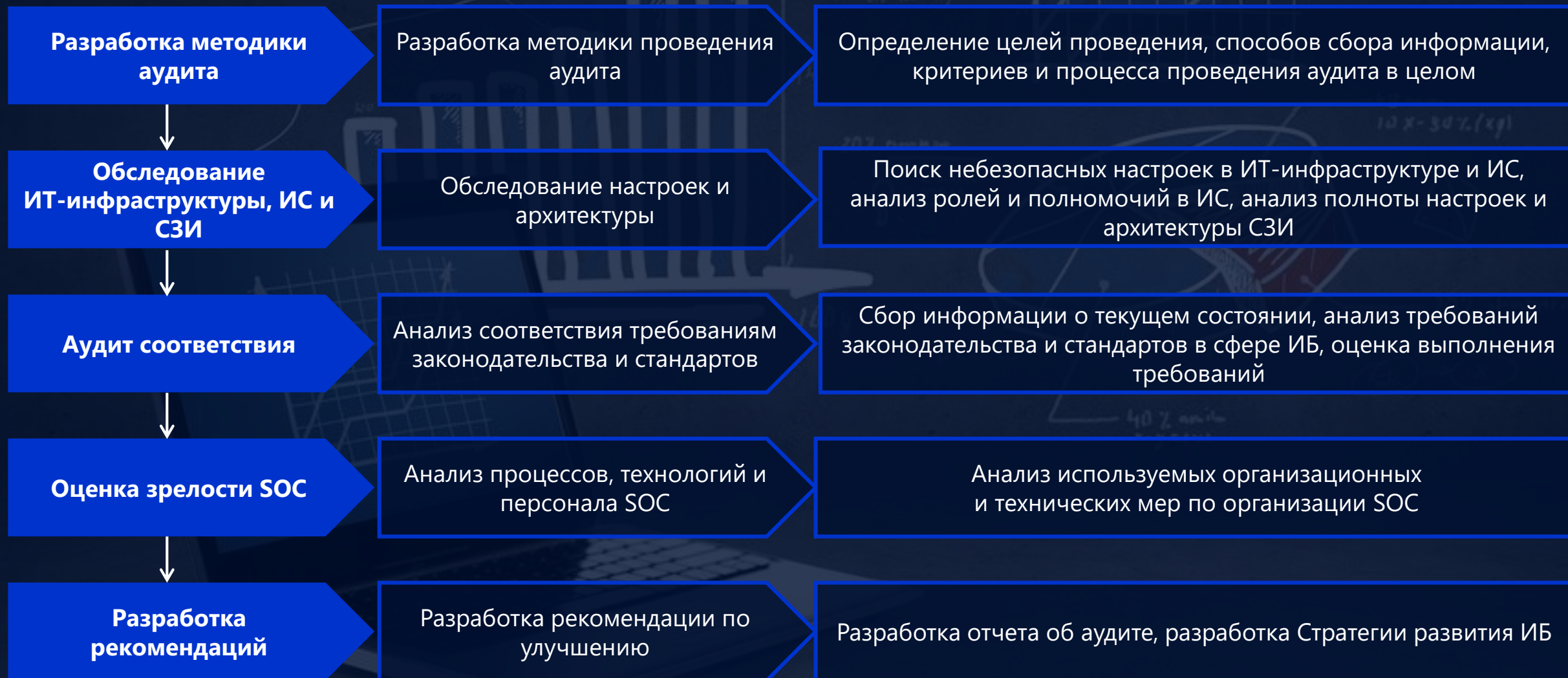
Анализ ключевых  
Процессов SOC



Анализ персонала на  
соответствие требованиям



# ЭТАПЫ АУДИТА



# КИБЕРКРИМИНАЛИСТ



Прикладная наука о раскрытии преступлений, связанных с использованием компьютерных технологий, об исследовании цифровых доказательств, методах поиска, получения и закрепления таких доказательств

Детальный анализ инцидента

Получить более подробный профиль атакующего или внутреннего злоумышленника

Восстановить последовательность действий, установить ущерб и точку проникновения

Подготовить и задокументировать цифровые доказательства



# DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR-СПЕЦИАЛИСТ)

## JET CSIRT

ИБ-координатор

ИТ-координатор

DFIR  
Lead

- Расследование инцидента
- Проработка оперативного плана восстановления
- Помощь в восстановлении инфраструктуры и настройке средств защиты информации
- Разворачивание временной защищенной инфраструктуры



## ЗАКАЗЧИК

ИТ

ИБ

Менеджмент

PR

- Сбор необходимых событий ИБ/артефактов
- Определение приоритетов восстановления
- Восстановление инфраструктуры и настройка средств защиты информации

## МЕНЕДЖЕР АКТИВНОСТИ



**2025**

# **СПАСИБО ЗА ВНИМАНИЕ**

**Калугина  
Алёна**

Ведущий инженер по информационной безопасности  
Центра информационной безопасности «Инфосистемы Джет»  
[as.kalugina@jet.su](mailto:as.kalugina@jet.su)