

# СТЕПАН КЛЕПИКОВ

SOC L2 аналитик



+7(999) 773-26-45 (RU)  
[daniilyashin01@gmail.com](mailto:daniilyashin01@gmail.com)

[Telegram](#)  
[WhatsApp](#)

Я молодой, растущий и компетентный специалист по кибербезопасности с огнем в глазах и невероятным желанием быть полезным интернет-сообществу (например – работая в CERT). У меня достаточно сильная техническая подготовка и довольно большой опыт работы с различными и меняющимися решениями в области кибербезопасности. В случае, если у меня нет работы в течение рабочего дня - я нахожу ее и предоставляю полный отчет в конце. Я быстро учусь, трудолюбив, и у меня очень серьезная мотивация расти в данной области.

## Образование (III курс)

[Российский Университет  
Транспорта](#)

[Кафедра вычислительные  
системы, сети и  
информационная  
безопасность](#)

Профиль: Безопасность  
компьютерных систем

## Курсы

2022:

[YouTube курс для  
начинающих в IT](#)

2023:

[Программа кафедры  
по ML&AI.](#)

## Опыт работы

ПАО Черкизово (Ноябрь 2021 – текущий момент)  
Младший аналитик SOC

### Обязанности:

Мониторинг, ревизия и анализ событий безопасности в системе IRP для определения вредоносной активности. Case by case расследования с использованием показаний AV, IDS, EDR, FW и иных СЗИ. Работа с автоматическими отчетами СЗИ (подозрительная входящая почта, вирусы на некритичных хостах, запуски RAT & TOR). R&D новых сценариев и правил SIEM. Создание папки плейбуков для типичных сработок. Постоянное присутствие в иных проектах отдела киберзащиты.

### Достижения:

- 1) Воссоздание, обновление и ежеквартальная актуализация групповой политики для наиболее критичных ПК\серверов.
- 2) Воссоздание группового почтового ящика отдела кибербезопасности и поддержание его в порядке (исследования подозрительных писем\доменов\иных пользовательских подозрений).

Знаком с продуктами: Cisco, CheckPoint, Kaspersky, Symantec, Positive Technologies.

## Языки

Русский (Родной)

English (B1)

Немецкий (A1)

## Soft skills

Дисциплина,

Обучаемость

Амбициозность,

Инициативность,

## Hard skills

■ ■ ■ □ □  
■ ■ □ □ □  
■ ■ □ □ □  
■ ■ □ □ □  
■ ■ □ □ □

JSOC\IRP  
DFIR  
AV software  
IPS\IDS\EDR  
Win\\*nix

■ ■ □ □ □  
■ ■ □ □ □  
■ □ □ □ □  
■ □ □ □ □  
■ □ □ □ □

Ti\TH  
PowerShell  
IOC  
Sandbox  
WAF