КАРТА КАРЬЕРНЫХ КОМПЕТЕНЦИЙ SOC (2025)

АНАЛИТИК И ИНЖЕНЕР. РОССИЯ / СНГ. JUNIOR→SENIOR

ОТКРЫТЬ ОГЛАВЛЕНИЕ

🧩 Карта карьерных компетенций SOC: от первой линии до стратегического уровня

Этот документ — результат прикладного анализа компетенций специалистов в области кибербезопасности, работающих в составах Security Operations Center (SOC) в условиях российского и СНГ-региона.
Он предназначен для систематизации требований к ключевым ролям, формализации ожиданий по уровням зрелости и создания прозрачной рамки развития внутри команды.

📍 **Рассматриваемые роли:**

- SOC-аналитик, специализирующийся на мониторинге и расследовании инцидентов;
- SOC-инженер, отвечающий за автоматизацию процессов и работу с инфраструктурой информационной безопасности (СЗИ, без DLP).

📍 **Фокус исследования:**
— внутренние SOC крупных компаний (финансовый сектор, телеком, ритейл, ИТ);
— MSSP и централизованные службы реагирования с распределёнными командами;
— реалии 24/7 сменной работы, постоянной нагрузки, автоматизации рутин и взаимодействия с внешними регуляторами.

📍 **Модель грейдов:**
Документ разделён на три уровня зрелости по каждой роли:

- **Junior —** начальный уровень: выполнение рутинных задач, работа по процедурам, обучение и поддержка;
- **Middle —** самостоятельная работа, ответственность за конкретные направления, вовлечённость в развитие процессов;
- **Senior —** экспертный уровень: стратегическое участие, архитектура, наставничество и принятие решений.

📌 **Мы осознанно разделили компетенции на две группы:**

- **Hard skills —** технические и инструментальные навыки: знание систем, умение настраивать, анализировать, писать код, проектировать;
- **Soft skills —** личные и командные качества: коммуникация, стрессоустойчивость, наставничество, управленческое мышление.

Этот документ будет полезен:

- специалистам, которые хотят свериться с актуальными ожиданиями рынка и наметить путь развития;
- тимлидам и руководителям, чтобы выстроить прозрачную систему грейдов и развития команды;
- HR и рекрутерам, чтобы понимать разницу между “давно работает” и “готов к следующему уровню”.

🔎 SOC-аналитик (L1–L3)

📦 Junior SOC-аналитик (L1)

📌 Что делает:

1. Сидит на первой линии и ловит всё, что летит из SIEM;
2. Понимает, где алерт норм, а где прилетело что-то пострашнее;
3. Передаёт дальше по SOP, не мешкая, но и не паникуя.

🛠 Hard Skills:

1. Знание основ ОС (Linux/Windows), понимание TCP/IP, HTTP, DNS, ICMP и прочих трёхбуквенных чудовищ;
2. Умение читать логи и находить в них суть (или хотя бы ошибку в таймстемпе);
3. Базовая работа с SIEM: открывать алерты, писать простые запросы, фильтровать шум;
4. Знакомство с EDR и IDS на уровне "нашёл, посмотрел, не убил";
5. Знание что такое инцидент, как его задокументировать, и когда пора эскалировать.

🧠 Soft Skills:

1. Способность не сойти с ума от потока сигналов;
2. Навык писать понятно (а не "что-то произошло, непонятно что");
3. Желание учиться у старших, а не гуглить в TikTok;
4. Внимание к деталям — если инцидент был в 03:14:00, то не 03:15;
5. Инициативность: если видишь лишние алерты — не молчи, предложи фильтр (но не ломай всё сразу).

📦 Middle SOC-аналитик (L2)

📌 Что делает:

1. Получает эскалации от L1 и сам роет глубже;
2. Делает форензику, сопоставляет кучу логов, пишет нормальные отчёты;
3. Понимает MITRE ATT&CK как Библию и находит TTP, даже если они в трёх строчках **логов.**

🛠 Hard Skills:

1. Глубокий анализ инцидентов, работа с SIEM, EDR, NTA, IDS;

2. Написание и тюнинг корреляционных правил, поиск IOC, базовый форензик (память, диск, сети);
3. Использование SOAR для автоматизации рутин;
4. Работа с TI — enrich инцидентов, сопоставление с известными группами;
5. Пост-инцидентные отчёты с выводами и планом защиты.

🧠 **Soft Skills:**

1. Критическое мышление и структурный подход;
2. Умение брать ответственность и вести кейс до конца;
3. Наставничество джунов — проверка тикетов, объяснение, как и зачем;
4. Работа с ИТ: объяснять, что надо поправить, не вызывая вражды;
5. Инициативность: видишь рутину — автоматизируй, предложи плейбук.

🧱 **Senior SOC-аналитик (L3)**

📌 **Что делает:**

1. Берёт на себя тяжёлые кейсы (APT, внутренние инциденты, утечки);
2. Руководит расследованиями, сам проводит глубокую форензику и threat hunting;
3. Координирует ответные действия и улучшает процессы мониторинга.

🛠 **Hard Skills:**

1. Углублённая форензика: память, диск, reverse malware, сетевой анализ;
2. Разработка детектов: YARA, сигнатуры, кастомные корреляции;
3. Threat hunting, UEBA, гипотезы и их проверка в логах;
4. Участие в стратегии SOC, написание IR-планов, взаимодействие с регуляторами (ФСТЭК, ФСБ, ФинЦЕРТ);
5. Настройка и внедрение новых методов мониторинга.

🧠 **Soft Skills:**

1. Спокойствие под давлением, способность принимать решения в условиях нехватки данных;
2. Коммуникация с бизнесом: объяснить сложный кейс не через Wireshark, а через риски;
3. Вдохновлять команду, быть наставником и координатором;
4. Мыслить стратегически: видеть, куда SOC идёт и как туда прийти;
5. Продвигать инновации — от AI-детектов до новых источников логов.

⚙️ SOC-инженер (по автоматизации и работе с СЗИ)

🧱 Junior SOC-инженер

📌 Что делает:

1. Подключает источники логов, настраивает агентов, пишет скрипты "чтобы всё не падало";
2. Работает по шаблонам, учится, старается не сломать прод.

🛠 Hard Skills:

1. Linux, Windows, сети, основные команды, grep и не grepни себя по пальцам;
2. SIEM: базовое подключение, написание парсеров;
3. Скрипты: Python, Bash, PowerShell — если не автоматизирует, то хотя бы не тормозит;
4. Документирование: записал — значит живо.

🧠 Soft Skills:

1. Точность, аккуратность, не пушить в прод ночью без ревью;
2. Коммуникабельность с аналитиками: помочь, выгрузить, настроить алерт;
3. Обучаемость и открытость к фидбэку;
4. Минимум паники, максимум вопросов.

🧱 Middle SOC-инженер

📌 Что делает:

1. Ведёт интеграции, развивает автоматизацию, следит за стабильностью SOC-инструментов;
2. Создаёт плейбуки, тюнингует правила, пишет свои утилиты.

🛠 Hard Skills:

1. Владение SIEM/SOAR/EDR: от настройки до CI/CD пайплайнов;
2. Плотная работа с API: логгинг, enrichment, автоматизация;
3. Проектирование: добавление новых систем, контроль форматов, timezones и фолбэков;
4. Поддержка инфраструктуры мониторинга (retention, перехват логов, корреляции).

🧠 Soft Skills:

1. Тайм-менеджмент и мультизадачность (внедрить, обновить, не забыть);
2. Умение вести диалог с разработкой и не превратиться в их врага;
3. Наставничество, разруливание конфликтов в команде;

4. Ответственность: "на мне — значит работает".

📦 Senior SOC-инженер

📌 Что делает:

1. Строит архитектуру мониторинга, управляет командой инженеров, внедряет новые технологии;
2. Отвечает за отказоустойчивость, масштабирование и техническое развитие SOC.

🛠 Hard Skills:

1. Архитектура SIEM, SOAR, EDR, NTA, NAC, UEBA: от выбора до продакшна;
2. DevSecOps, Terraform/Ansible, GitOps, full pipeline автоматизации безопасности;
3. Глубокая экспертиза в лог-менеджменте, нормализации, масштабировании;
4. Управление метриками SOC (MTTD, MTTR, log coverage).

🧠 Soft Skills:

1. Руководство, планирование, донесение value до бизнеса;
2. Ответственность за инфраструктуру и команду;
3. Работа с вендорами, аудитами, заказчиками;
4. Постоянный апдейт знаний, понимание рынка и трендов.

🎯 **Вывод**

Эта карта не претендует на абсолютную истину, но если ты узнаёшь себя на одном из уровней — отлично. Значит, она работает.

Если читаешь и чувствуешь, что твои задачи давно middle, а ты всё ещё в грейде джуна — стоит идти к тимлиду и обсуждать план развития.

А если уже на уровне senior, но никто не в курсе — пора выйти из тени и навести порядок не только в логах, но и в своей карьере 👊