УДК 004.056.55
DOI: 10.26102/2310-6018/2025.51.4.040

Оценка эффективности центров мониторинга и реагирования на киберугрозы: ограничения временных метрик и операционные индикаторы качества

В.В. Пахомов✉

Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Москва, Российская Федерация

Резюме. В статье рассматриваются практики оценки эффективности центров мониторинга и реагирования на киберугрозы в условиях роста объемов телеметрии и усложнения атак. Показано, что распространенные показатели среднего времени обнаружения и среднего времени реагирования отражают преимущественно быстроту, но не отвечают на вопросы о достаточности данных для обоснованных выводов, наличии контекста расследования и повторяемости его шагов. Выполнено сопоставление международных руководств и обзорных отчетов с российскими нормативными требованиями и проведен анализ отраслевых публикаций. В качестве результата систематизированы источники данных центра мониторинга, выделены типовые узкие места в цепочке преобразования данных и ограничения классических временных метрик. Предложена простая рамка сравнения по трем направлениям: скорость, контекст, процесс. Новизна состоит во введении трех вычислимых индикаторов: полноты контекста (доля инцидентов, подтвержденных не менее чем тремя независимыми источниками), воспроизводимости расследований (доля шагов, выполненных по утвержденным сценариям с машиночитаемым журналированием) и устойчивости к пиковым нагрузкам (сопоставление соблюдения целевых сроков в пиковом и базовом режимах), а также интегрального показателя управляемости, объединяющего скорость, точность и полноту. Практическая значимость заключается в возможности расчета указанных индикаторов на имеющихся системах управления событиями информационной безопасности и в их включении в дашборды для аудита, планирования ресурсов и сопоставимости команд.

Ключевые слова: SOC, оценка эффективности, MTTD, MTTR, полнота контекста, воспроизводимость расследований, устойчивость под нагрузкой, SIEM, SOAR, XDR.

Для цитирования: Пахомов В.В. Оценка эффективности центров мониторинга и реагирования на киберугрозы: ограничения временных метрик и операционные индикаторы качества. *Моделирование, оптимизация и информационные технологии.* 2025;13(4). URL: https://moitvivt.ru/ru/journal/pdf?id=2092 DOI: 10.26102/2310-6018/2025.51.4.040

Evaluating the effectiveness of cyber-threat monitoring and response centers: limits of time-based metrics and operational quality indicators

V.V. Pakhomov✉

The Russian Presidential Academy of National Economy and Public Administration, Moscow, the Russian Federation

Abstract. The paper examines practices for evaluating the effectiveness of cyber-threat monitoring and response centers under growing telemetry volumes and increasingly complex attacks. It is shown that commonly used indicators such as mean time to detect and mean time to respond mainly capture speed while failing to assess whether available data are sufficient for sound conclusions, whether investigation context is present, and whether investigation steps are reproducible. The study compares international

guidance and landscape reports with Russian regulatory requirements and analyzes industry publications. As a result, data sources used by monitoring centers are systematized, typical bottlenecks in the data value chain are identified, and limitations of classic time-based metrics are highlighted. A simple three-axis comparison framework is proposed: speed, context, and process. The contribution introduces three computable indicators: context completeness (share of incidents corroborated by at least three independent sources), investigation reproducibility (share of steps executed via approved playbooks with machine-readable logging), and resilience to peak loads (comparison of service-level target adherence in peak versus baseline periods), together with an integral manageability index combining speed, accuracy, and completeness. The practical value lies in the feasibility of calculating these indicators using existing security event management systems and incorporating them into monitoring dashboards for audit, resource planning, and cross-team comparability.

Keywords: SOC, effectiveness assessment, MTTD, MTTR, context completeness, investigation reproducibility, load resilience, SIEM, SOAR, XDR.

For citation: Pakhomov V.V. Evaluating the effectiveness of cyber-threat monitoring and response centers: limits of time-based metrics and operational quality indicators. *Modeling, Optimization and Information Technology*. 2025;13(4). (In. Russ.). URL: https://moitvivt.ru/ru/journal/pdf?id=2092 DOI: 10.26102/2310-6018/2025.51.4.040

Введение

Центры мониторинга и реагирования на киберугрозы (SOC) стали ключевым элементом киберустойчивости: на их базе консолидируются события из сети, конечных точек и облака, выстраиваются процедуры выявления и обработки инцидентов, а также обеспечивается прослеживаемость действий[1,2].

Многоуровневая модель работы SOC:

– Tier 1 – фильтрация и нормализация, отсев «шума»;

– Tier 2 – корреляция событий, выявление аномалий, обогащение индикаторами компрометации (IoC);

– Tier 3 – расследование сложных атак, причинно-следственный анализ, рекомендации по развитию защиты.

– Такая последовательность формирует «цепочку ценности информации»: от сигналов – к событиям, затем к контекстным описаниям и управленческим решениям.

– Задачи анализа потоков SOC включают:

– фильтрацию, нормализацию и обогащение данных;

– агрегацию и корреляцию событий, реконструкцию сессий/цепочек;

– контроль качества данных (полнота, целостность, согласованность, задержка доставки) и прослеживаемость происхождения (data lineage);

– приоритизацию и маршрутизацию реагирования, снижение «алерт-шторм»;

– проверку воспроизводимости результатов расследования (плейбуки/скрипты, машинно-читаемое журналирование шагов) и актуализацию плейбуков по итогам инцидентов.

SOC выполняет централизованный сбор и анализ данных безопасности [1]. Он работает циклично: выводы верхних уровней возвращаются в виде корректировок правил корреляции, плейбуков и политик сенсоров. Эффективность определяется не только технологиями, но и согласованностью операций обработки информации; потеря событий, недостаток контекста или отсутствие журналирования ведут к деградации

[1] ENISA Threat Landscape 2023. European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (дата обращения: 21.09.2025).
[2] Verizon. Data Breach Investigations Report 2023.

качества решений и смещают оценку в сторону формального улучшения времени без реального роста управляемости.

Традиционные метрики (MTTD, MTTR) удобны для отчетности и сравнения во времени, но описывают преимущественно скорость и слабо отражают полноту наблюдаемости, наличие контекста для обоснованных выводов и воспроизводимость расследований [2, 3]. Исследования указывают на риск «формальных улучшений по времени» при росте доли ложноположительных срабатываний и недостатке артефактов, необходимых для передачи дела между сменами [4].

Международные руководства по реагированию на инциденты и отечественные требования для объектов критической информационной инфраструктуры (ФЗ-187[3] (далее – ФЗ-187), документы ФСТЭК[4] (далее – Приказ ФСТЭК № 239), ГОСТ Р 57580.1-2017[5]) подчеркивают необходимость прослеживаемости, достаточности данных и соблюдения SLA[6,7].

С учетом этого проблема формулируется как отсутствие в повседневной практике согласованного набора показателей, дополняющих MTTD/MTTR характеристиками качества данных и управляемости процесса (контекст, воспроизводимость, устойчивость под нагрузкой) [5]. В работе предлагаются операционные индикаторы для восполняющих аспектов и обсуждается их расчет на телеметрии SIEM/XDR и журналах SOAR.

В данной статье рассматривается проблема оценки эффективности SOC с учетом не только скорости обнаружения и реагирования, но и качества обработки информации (контекст, воспроизводимость, устойчивость под нагрузкой), что соответствует тенденциям, описанным в международных рекомендациях и обзорах угроз. Исследование опирается на сопоставление практик NIST, ENISA, MITRE ATT&CK и эмпирики отраслевых отчетов (DBIR) с точки зрения применимости к реальным контурам мониторинга.

Цель исследования – обосновать и формализовать набор дополняющих индикаторов эффективности SOC, отражающих качество данных и управляемость процессов реагирования, а также показать их применимость наряду с MTTD/MTTR [3, 6].

Для достижения цели решаются следующие задачи:

– провести систематизацию потоков данных SOC, указав основные источники (сеть, конечные точки, облако, OT/SCADA, средства защиты), параметры качества и характерные «узкие места»;

– определить, какие методы обработки (сигнатурные, корреляционные, поведенческие, ML-подходы) повышают управляемость процесса и снижают нагрузку на персонал [7, 8];

[3] Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Электронный фонд правовой и нормативно-технической информации. URL: https://docs.cntd.ru/document/436752114 (дата обращения: 21.09.2025).

[4] Приказ ФСТЭК России от 25.12.2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». Электронный фонд правовой и нормативно-технической информации. URL: https://docs.cntd.ru/document/542616931 (дата обращения: 21.09.2025).

[5] ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер: национальный стандарт Российской Федерации: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому ре-гулированию и метрологии от 8 августа 2017 г. № 822-ст: введен впервые: дата введения 2018-01-01. Москва: Стандартинформ, 2017. 61 с.

[6] ISO/IEC 27035-1:2016. Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management. Geneva: ISO/IEC; 2016. 21 p.

[7] Grance T., Kent K., Kim B. NIST SP 800-61. Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology. Gaithersburg: NIST; 2004. 148 p.

– сопоставить используемые метрики эффективности SOC с задачами управления информацией и выявить их ограничения с точки зрения наблюдаемости и интерпретируемости [2, 3];

– проанализировать воспроизводимость процессов расследования и влияние человеческого фактора на обработку событий, учитывая роль плейбуков/скриптов и журналирования (SOAR) [6, 9];

– сформулировать индикаторы полноты контекста, воспроизводимости и устойчивости под нагрузкой и описать правила их расчета на данных SIEM/XDR и журналах SOAR [6, 8];

– предложить направления развития критериев и практические рекомендации по включению новых индикаторов в отчетность и дашборды SOC наряду с MTTD/MTTR.

Ожидаемый результат – рамка «скорость – контекст – процесс – устойчивость», три вычислимых индикатора и интегральный индекс, а также рекомендации по внедрению в условиях российских и международных требований.

Материалы и методы

Работа включает две связанные части:

1) обзорно-аналитическую (отбор и структурирование источников по рамке «скорость – контекст – процесс»);

2) методическую (расчет индикаторов поверх MTTD/MTTR на данных SOC).

Цель – получить воспроизводимый набор метрик, который можно внедрить в отчетность SOC без изменения существующей инфраструктуры.

Источники данных:

– Потоки событий и телеметрии: SIEM/XDR (сеть, конечные точки, приложения, облако/OT), журналы систем учётных записей (IdP/AD), инвентарь/CMDB.

– Журналы оркестрации и реагирования: SOAR.

– Календарь SLA (рабочие/нерабочие интервалы, пороги для классов инцидентов). Аналитическое окно – не менее 6 последовательных месяцев для отделения «базы» от «пиков».

– Программное обеспечение (ПО) и форматы.

– Хранилище выгрузок в текстовых форматах (JSON/CSV) с последующей нормализацией к унифицированной схеме (ECS/OCSF).

– Скрипты обработки и расчета индикаторов реализуемы в любом современном стеке (Python/R) – методика не привязана к вендору. Все шаги ниже описаны так, чтобы компетентный специалист мог воспроизвести их по одному тексту статьи.

Модульная архитектура конвейера:

1. Унификация событий – приведение полей к общей схеме (ECS/OCSF), нормализация часовых поясов и форматов времени, дедупликация (ключи: источник/хэш/окно схлопывания).

2. Реконструкция инцидентов – агрегация событий в дела/кейсы (правила корреляции SIEM + связи ITSM).

3. Обогащение контекстом – присоединение атрибутов из CMDB/IdP/TI (критичность актива, принадлежность сегменту, IoC).

4. Разметка процессов – извлечение из журналов SOAR шагов расследования, сопоставление с утвержденными плейбуками/скриптами.

5. Разметка режимов нагрузки – определение «пиков» по верхнему децилю объема алертов/событий SIEM на интервалах; остальное – «база».

Операционные определения:

– Единица учета – инцидент (не отдельное срабатывание).

– Независимый источник – отличающийся домен телеметрии: сеть; журналы приложений; конечные точки; облако/OT (перечень фиксируется в регламенте).

– Полнота контекста – доля инцидентов, где задействованы ≥ 3 независимых домена.

– Воспроизводимость расследований – доля шагов, выполненных по утвержденным плейбукам/скриптам с машинно-читаемым журналированием в SOAR [5, 9].

– Устойчивость под нагрузкой – отношение доли инцидентов, закрытых в пределах SLA, в «пиковые» интервалы к той же доле в «базовых».

Процедура расчета индикаторов (поверх MTTD/MTTR):

1. Контекст. Для каждого инцидента фиксировать перечень реально использованных доменов данных; проставить признак «контекст ≥ 3». На отчетный период – доля таких инцидентов (в целом и по типам).

2. Воспроизводимость. По журналам SOAR для каждого инцидента извлечь последовательность шагов; посчитать долю шагов, прошедших по утвержденным плейбукам/скриптам (ID плейбука + запись в журнале).

3. Устойчивость. По меткам «пик/база» и календарю SLA рассчитать долю инцидентов, закрытых в SLA, отдельно для «пика» и «базы»; получить коэффициент «пик/база».

4. Интегральный показатель (для управленческой витрины): нормировать компоненты и агрегировать в сводный индекс с разложением по компонентам (скорость/точность, контекст, воспроизводимость, устойчивость) [3].

5. Представление. Рядом с MTTD/MTTR выводить: полноту контекста (доля, тренд, теплокарта по доменам); воспроизводимость (доля, разрез по типам); устойчивость («пик/база» и коэффициент, месячный тренд) [6].

Контроль качества и сопоставимость:

– Качество телеметрии. В каждом цикле отчетности фиксировать причины недобора источников (пробелы наблюдаемости, недоступные логи, технический долг) и план закрытия «слепых зон».

– Справочники и версии. Единые справочники типов инцидентов и плейбуков; версионирование методики расчетов; неизменяемые машинно-читаемые журналы действий для аудита и повторных пересчетов.

– Малые контуры. Допускается временный порог «≥ 2 источников» при явной пометке в методике и отдельной интерпретации результатов.

Ограничения: зависимость от качества журналирования, неполнота телеметрии в отдельных доменах и различия в трактовке SLA между организациями; эти факторы учитываются при обсуждении результатов [3, 4].

Результаты

Сформирован сводный обзор источников по международным и российским нормам/практикам инцидент-менеджмента. Зафиксированы ключевые элементы жизненного цикла в документах NIST SP 800-61 (rev. 3), ISO/IEC 27035 и в таксономии MITRE ATT&CK; дополнительно использованы агрегированные статистические сводки ENISA Threat Landscape и Verizon DBIR. MITRE предлагает стратегические рекомендации для SOC и таксономию ATT&CK, позволяющую соотносить наблюдения с тактиками и техниками противника и строить воспроизводимые цепочки реагирования[8]. Обзоры ENISA Threat Landscape и отчеты Verizon DBIR дают статистическую базу для метрик процесса (включая среднее время обнаружения/реагирования и долю ложноположительных

[8] MITRE. 2022 MITRE ATT&CK®. Knowledge Base of Adversary Tactics and Techniques.

срабатываний, FPR – False Positive Rate). Отдельные исследования рассматривают производительность аналитиков и влияние автоматизации на устойчивость процесса [6, 4].

Для российской практики отмечены требования ФЗ-187, подзаконных актов ФСТЭК и взаимодействие с инфраструктурой ГосСОПКА[7]. В отличие от зарубежных моделей, где ключевые метрики – скорость реакции, в России главным критерием является соответствие нормам. В научных публикациях (например, в «Трудах СПИИРАН») акцент делается на архитектуру SOC и автоматизацию обработки [10, 11]. Однако остается нерешенным вопрос разработки критериев управляемости потоков в условиях нормативных ограничений.

Сводное сопоставление ключевых этапов приведено в Таблице 1.

Таблица 1 – Сравнение этапов управления инцидентами в международных и российских подходах
Table 1 – Comparison of incident-handling stages in international and Russian approaches

Этап	Международная практика (NIST, ENISA, MITRE)	Российская нормативная база (ФЗ-187, ФСТЭК, ГОСТ Р 57580)
Выявление	Мониторинг событий, использование SIEM/XDR, корреляция по ATT&CK	Обязательное фиксирование события в системе учёта
Регистрация	Рекомендуется ведение журнала инцидентов	Обязательная регистрация в установленной форме
Классификация	По типам атак и их тактикам (ATT&CK, ENISA)	По уровням значимости и критичности (ФСТЭК)
Анализ	Корреляция событий, использование TI, реконструкция сценариев	Расследование в соответствии с методическими рекомендациями
Реагирование	Устранение последствий, блокировка атакующих техник	Ликвидация последствий и восстановление работоспособности
Постинцидентное расследование	Обязательный разбор и совершенствование процессов	Документирование и отчётность в адрес ФСТЭК/ГосСОПКА

Представленное сопоставление показывает, что международные документы уделяют больше внимания скорости и автоматизации процесса, тогда как российская нормативная база обеспечивает полноту регистрации и доказуемость действий. Однако обе линии недостаточно формализуют требования к качеству исходных данных и воспроизводимости расследований, что затрудняет управление потоками информации при росте телеметрии и нагрузки.

Выводы по рамке «скорость – контекст – процесс»:

– Скорость. В международных подходах доминируют MTTD/MTTR и соблюдение SLA; российские нормы фиксируют регламенты и контроль сроков, но не учитывают время на сбор контекста и верификацию гипотез.

– Контекст. ENISA/NIST/ISO подчеркивают достаточность артефактов; российские документы требуют полноты журналирования и трассируемости, но не определяют минимально достаточное покрытие источниками.

– Процесс. Международные практики требуют воспроизводимости (плейбуки, SOAR, машинно-читаемое логирование); российские – наличие формальных регламентов и отчетности, при этом степень автоматизации и измеримость воспроизводимости остаются открытыми.

Эти различия мотивируют введение индикаторов, дополняющих MTTD/MTTR: полноты контекста, воспроизводимости расследований и устойчивости под нагрузкой.

Далее рассматриваются показатели эффективности SOC и способы их расчета по телеметрии SIEM/XDR и журналам SOAR.

Собран и структурирован набор применяемых метрик: среднее время обнаружения (MTTD), среднее время реагирования (MTTR), доля ложноположительных срабатываний (FPR), а также показатели информационного поиска precision и recall[7] [3].

В международной практике доминируют временные показатели – среднее время обнаружения (MTTD) и среднее время реагирования (MTTR). Доля ложноположительных срабатываний (FPR, False Positive Rate) применяется для оценки избыточности сигналов (часто в обзорах ENISA), однако затрагивает лишь «шум» детектов и не отражает полноту наблюдаемости и полезность данных для расследования.

Для баланса чувствительности и точности используют показатели информационного поиска – precision и recall; в практиках с применением методов ML рост полноты часто сопровождается увеличением ложноположительных тревог, а повышение точности – потерей части истинных инцидентов [7, 12].

Сводные характеристики базовых метрик приведены в Таблице 2.

Таблица 2 – Характеристика основных метрик эффективности SOC
Table 2 – Characteristics of core SOC effectiveness metrics

Метрика	Смысл	Ограничения
MTTD	Время от начала инцидента до его обнаружения	Не учитывает качество данных, может искажаться при большом числе несущественных событий
MTTR	Время от обнаружения до устранения последствий	Отражает скорость, но не полноту устранения или глубину анализа
FPR	Доля оповещений, не подтвердившихся как инциденты	Фокусируется только на избыточности
Precision	Доля корректно классифицированных инцидентов среди всех срабатываний	Может снижаться при максимизации полноты
Recall	Доля обнаруженных инцидентов от их общего числа	Рост Recall часто ведёт к росту ложноположительных тревог

Временные и классические качественные метрики описывают «скорость» и частично «точность» детектов, но практически не затрагивают контекст, воспроизводимость и устойчивость под нагрузкой.

Дополняющие индикаторы эффективности (к MTTD/MTTR):

– Полнота контекста. Доля инцидентов, для которых задействовано ≥ 3 независимых источника данных (например, сеть, журналы приложений, телеметрия конечных точек). Источники расчета: SIEM/XDR, инвентарь/CMDB. Представление: процент по периодам; теплокарта по доменам.

– Воспроизводимость расследований. Доля шагов, выполненных по утверждённым плейбукам/скриптам с машинно-читаемым журналированием в SOAR. Источники: журналы SOAR, репозиторий плейбуков. Представление: процент по периодам; разрез по типам инцидентов.

– Устойчивость под нагрузкой. Отношение доли инцидентов, закрытых в пределах SLA, в пиковые периоды к той же доле в базовом режиме. Источники: SIEM/XDR (объём событий), SOAR/ITSM, календарь SLA. Представление: пара «пик/база» и коэффициент; месячный тренд.

– Интегральный показатель управляемости. Агрегирование нормированных компонент: скорость (время), качество/точность данных, полнота наблюдаемости,

воспроизводимость. Источники: все перечисленные. Представление: индекс 0–1, тренд и разложение по компонентам.

Эти индикаторы закрывают пробелы временных метрик и позволяют оценивать качество данных и управляемость процесса. В следующем разделе уместно кратко показать, как они компенсируют ограничения традиционных показателей.

Сводный разбор метрик показывает: MTTD/MTTR и качественные показатели детектов описывают скорость и частично точность, но оставляют за кадром полноту контекста и воспроизводимость процесса. Это приводит к расхождениям между «красивыми» цифрами и реальным качеством расследований, особенно при всплесках телеметрии. Ниже систематизируем ключевые ограничения традиционных показателей и показываем, как их компенсируют дополнительные индикаторы.

Сформирован перечень часто встречающихся типов инцидентов и контекстных факторов их обработки (по международным и российским источникам):

1. Фишинг и социальная инженерия. Существенная доля инцидентов связана с человеческим фактором; критично обеспечить быструю верификацию сигналов и накопление контекста (почтовые заголовки, поведение пользователей).

2. Вредоносное ПО и эксплойты. Продолжается рост ransomware и эксплуатации уязвимостей нулевого дня; исторические кампании (например, WannaCry, 2017) подчеркивают важность базовой гигиены и сегментации.

3. Атаки на цепочки поставок. Случай SolarWinds (2020) демонстрирует масштабы риска при компрометации обновлений вендоров.

4. DDoS-атаки. Массовые и дестабилизирующие; требуют стыковки сетевой и прикладной аналитики.

5. Инсайдерские угрозы. Намеренные и ошибочные действия сотрудников; по оценкам отраслевых исследований совокупные издержки сопоставимы и нередко выше, чем при части внешних инцидентов[9].

Российская специфика. Для объектов критической информационной инфраструктуры обязательны регистрация, классификация и отчетность в соответствии с ФЗ-187 и ФСТЭК, а также взаимодействие с инфраструктурой ГосСОПКА. Высокая формализация обеспечивает полноту регистрации и трассируемость, но повышает нагрузку на SOC и снижает гибкость: к учету подлежат даже малозначимые события, что усиливает требования к приоритизации и автоматизации процессов[10,11].

Системные вызовы SOC:

1. Перегрузка оповещениями («alert fatigue») [13]. Десятки тысяч событий в сутки при высокой доле ложноположительных сигналов затрудняют выделение критически важных инцидентов [4].

2. Кадровый дефицит. По прогнозам Gartner (2022), нехватка квалифицированных специалистов сохраняется; время подготовки аналитика велико[12].

3. Фрагментарность данных. Разнородность источников (сеть, конечные точки, облака, OT/SCADA) требует унификации форматов и повышает риск пропусков при корреляции [8].

4. Рост сложности атак. Многостадийные кампании и «living-off-the-land» хуже детектируются правилами общего вида.

5. Нормативные ограничения. Необходимость строгой отчетности и соблюдения регламентов снижает гибкость и создает издержки на формальные процедуры.

[9] Ponemon Institute. 2022 Cost of Insider Threats: Global Report.
[10] Cybersecurity Threatscape: Q4 2023. Positive Technologies. URL: https://global.ptsecurity.com/en/research/analytics/cybersecurity-threatscape-2023-q4/ (дата обращения: 21.09.2025).
[11] Group-IB. Hi-Tech Crime Trends 2023/2024.
[12] 2022 Gartner® Market Guide for Operational Technology Security.

Примеры значимых инцидентов (иллюстрация масштаба вызовов): Colonial Pipeline (2021) – остановка операций из-за ransomware; кампании против энергосетей Украины (2015–2022) – влияние на критическую инфраструктуру; крупнейшие DDoS-атаки на российские ресурсы (в т. ч. «Яндекс», 2021) – потребовали межорганизационной координации.

Перечисленные вызовы непосредственно задают требования к:

– полноте контекста – подтверждение наблюдений независимыми источниками при алерт-шторме и многостадийных атаках;

– воспроизводимости расследований – минимизация влияния человеческого фактора через плейбуки/скрипты и машинно-читаемое журналирование;

– устойчивости под нагрузкой – поддержание доли инцидентов, закрытых в пределах SLA, в пиковые периоды.

Тем самым обосновывается включение соответствующих индикаторов в оценку эффективности SOC наряду с MTTD/MTTR. Они позволяют отличать формальные улучшения по времени от реального повышения управляемости процесса, подсвечивая «слепые зоны» наблюдаемости и точки для автоматизации.

Собраны практики и зафиксированные в источниках эффекты внедрения.

Автоматизация процессов реагирования (SOAR). Внедрение платформ SOAR позволяет автоматизировать типовые сценарии: изоляцию узлов, блокировку параметров на периметре, сбор артефактов и тикетинг. По оценкам Gartner (2022), применение SOAR сокращает среднее время обработки инцидента и снижает долю ручных операций; экспериментальные сравнения и разборы рабочих кейсов подтверждают эффект за счет стандартизации процедур [6]. Связь с индикаторами: рост воспроизводимости (плейбуки/скрипты с машинно-читаемым журналированием) и вклад в устойчивость под нагрузкой за счет разгрузки Tier 1–2.

Машинное обучение и искусственный интеллект (ML/AI, UEBA). SOC применяют ML/AI для выявления аномалий и поведенческих отклонений (UEBA): анализ сетевой статистики, событий аутентификации, файловых операций и др. [7]. Такие модели помогают отсеивать «шум» и подсвечивать редкие цепочки. Эффект: снижение FPR за счет контекстуализации и приоритизации сигналов, поддержка перехода от реактивного к проактивному анализу [7]. Связь с индикаторами: улучшение контекста (обогащение признаками) и вклад в устойчивость за счет автоматизированной фильтрации и ранжирования.

Интеграция платформ и консолидация данных (XDR). Фрагментарность источников остается ключевым вызовом. Решения класса XDR объединяют телеметрию сетевых сенсоров, EDR и облачных платформ, повышая точность детектирования за счет расширенного контекста[13]. В России сопоставимые задачи решаются интеграцией SIEM с отраслевыми платформами (в т. ч. при взаимодействии с ГосСОПКА); это одновременно закрывает нормативные требования. Связь с индикаторами: прямое повышение полноты контекста (подтверждение инцидента независимыми источниками) и опосредованный вклад в устойчивость (меньше ручных запросов к внешним системам).

Приоритизация и интеллектуальная фильтрация. Механизмы приоритизации ранжируют оповещения по критичности с учетом типа атаки, важности активов, подтвержденных IoC, частоты и истории аналогичных событий, что снижает «alert fatigue» и повышает концентрацию на действительно важных кейсах [8]. Связь с индикаторами: опора на расширенный контекст; стабилизация выполнения SLA в пике (устойчивость).

[13] Forrester. The Security Analytics Platform Landscape, Q3 2022.

Организационные меры и развитие кадров. Ключевые направления: многоуровневая модель реагирования (Tier 1–3), централизация SOC на уровне холдингов/отраслей, обучение и симуляции (Cyber Range). Эти меры смягчают кадровый дефицит и повышают предсказуемость процессов. Связь с индикаторами: стандартизация ролей и плейбуков повышает воспроизводимость; централизация упрощает консолидацию источников (контекст).

Обсуждение

Полученные результаты демонстрируют, что базовые метрики SOC (MTTD, MTTR, FPR, precision, recall) охватывают преимущественно скорость и частично точность детектов, но не отражают полноту контекста, воспроизводимость расследований и устойчивость процесса при всплесках нагрузки. Это согласуется с наблюдениями отраслевых обзоров и практик инцидент-менеджмента, где рост телеметрии и усложнение сценариев атак приводят к перегрузке аналитиков и к разрыву между «красивыми» временными метриками и реальным качеством расследований.

Соотнесение результатов с предложенными индикаторами:

1. Полнота контекста. Сопоставление международных и российских подходов (Таблица 1) показывает: нормативные режимы обеспечивают полноту регистрации, тогда как практики NIST/ISO/ENISA сильнее акцентируют оперативность и автоматизацию. В обоих случаях не до конца определен минимум независимых источников, достаточный для обоснованных выводов. Введенный индикатор «≥ 3 домена телеметрии на инцидент» закрывает эту лакуну и делает требование наблюдаемости измеримым на уровне отчетности SOC.

2. Воспроизводимость расследований. Результаты по базовым метрикам (Таблица 2) не фиксируют, насколько шаги расследования выполнялись по утвержденным плейбукам, а значит – не отражают стандартизацию процесса. Связка журналов SOAR с каталогом плейбуков позволяет считать долю «скриптуемых» шагов и выводить ее в составе регулярных отчетов, что напрямую снижает вариативность человеческого фактора и облегчает аудит [6, 9].

3. Устойчивость под нагрузкой. Эмпирические данные о «пиках» (алерт-шторм, DDoS, крупные кампании) и «базе» свидетельствуют: даже при стабильных MTTD/MTTR качество закрытия инцидентов по SLA может проседать. Отношение «SLA-пик/база» позволяет контролировать именно устойчивость процесса расследования к скачкам входящего потока, а не только средние временные показатели.

4. Интегральный показатель управляемости. Нормированная агрегация компонент «скорость – точность/качество данных – полнота наблюдаемости – воспроизводимость» решает проблему несопоставимости отдельных частных метрик между командами и периодами. Индекс удобен для управленческой витрины, а его разложение – для операционных улучшений [3].

Сопоставление с практиками оптимизации (интерпретация эффекта):

– SOAR. Факты использования SOAR, указанные в «Результатах», интерпретируются как прямой рост индикатора воспроизводимости за счет выполнения шагов по плейбукам и фиксации машинно-читаемых журналов. Дополнительно SOAR разгружает Tier 1–2 в пики, косвенно повышая «SLA-пик/база» и тем самым устойчивость процесса [6].

– ML/AI (включая UEBA). По данным источников, ML/AI снижает FPR за счет контекстуализации и приоритизации, что уменьшает «шум» и высвобождает ресурс на сбор артефактов. Это ведет к росту полноты контекста и стабилизации соблюдения SLA в периоды повышенной нагрузки [7].

– Интеграция/XDR. Консолидация сетевой, конечной и облачной телеметрии увеличивает вероятность подтверждения инцидента независимыми источниками и сокращает долю ручного обогащения. Таким образом, улучшается индикатор «полнота контекста» и опосредованно улучшается «SLA-пик/база» благодаря снижению операционных задержек на запросы к внешним системам.

– Приоритизация и интеллектуальная фильтрация. Ранжирование по критичности активов и наличию подтвержденных IoC повышает концентрированность внимания на значимых инцидентах, что отражается в росте доли закрытий в рамках SLA в «пики» и в уменьшении влияния «alert-fatigue» на процесс [8].

– Организационные меры. Многоуровневая модель (Tier 1–3), централизация SOC, тренировки и симуляции обеспечивают повторяемость действий и переносимость практик между командами, что выражается в индикаторе воспроизводимости. Централизация также облегчает достижение порога наблюдаемости по доменам телеметрии.

В сумме это подтверждает целесообразность добавления к MTTD/MTTR трех индикаторов, непосредственно отражающих управляемость информационных потоков в SOC, и интегрального показателя для управленческой витрины [3].

Сравнение с другими работами. Результаты согласуются с выводами о необходимости расширения набора производственных метрик SOC, затрагивающих не только скорость, но и организационно-процессные аспекты. Работы по измерению эффективности SOC и производительности аналитиков подчеркивают влияние стандартизации и автоматизации на устойчивость и предсказуемость процесса, что коррелирует с ростом наших индикаторов воспроизводимости и «SLA-пик/база» [3, 4]. Отдельные исследования по оценке SOAR и XDR эмпирически подтверждают вклад автоматизации и консолидации данных в снижение ручных операций и улучшение качества детектирования, что интерпретируется как рост полноты контекста и устойчивости под нагрузкой [6].

Практические следствия и рекомендации:

1. Отчетность. Рядом с MTTD/MTTR выводить: долю инцидентов с «≥ 3 доменами», долю «шагов по плейбукам», пару значений «SLA-пик/база» и соответствующий коэффициент; для управленцев – интегральный индекс и его разложение по компонентам [3].

2. Управление качеством данных. В каждом цикле фиксировать причины недобора источников (пробелы наблюдаемости, отказоустойчивость логов, технический долг) и план закрытия «слепых зон»; вести чек-лист качества (полнота, целостность, задержки доставки, корректность тайм-стампов).

3. Внедрение по шагам. Пилот на одном типе инцидентов; маркировка «пик/база»; включение индикаторов в еженедельные обзоры; корректировка плейбуков и план устранения пробелов наблюдаемости [6].

Ограничения интерпретации. Интерпретации зависят от качества телеметрии и от полноты журналов SOAR; для малых контуров правомерна временная адаптация порога «не менее трех источников» с явной пометкой в методике. Сопоставимость между организациями ограничивают различия в SLA и в политике корреляции/дедупликации; при межорганизационных сравнениях требуется нормализация [3, 4].

Введенные индикаторы и интегральный показатель позволяют перевести оценку SOC из плоскости «только скорость» в плоскость управляемости информационных потоков и устойчивости процесса.

Заключение

Проведенный анализ показал, что оценивать эффективность SOC только временными и классическими качественными метриками (MTTD, MTTR, FPR, precision, recall) недостаточно: они не отражают полноту контекста, требования прослеживаемости и устойчивость процесса при всплесках нагрузки [3]. Практика и обзоры инцидентов дополнительно указывают на перегрузку оповещениями, дефицит кадров и фрагментарность данных, что обостряет разрыв между «скоростью на отчете» и реальным качеством расследований.

В работе предложены три дополняющих индикатора – полнота контекста (подтверждение инцидента независимыми источниками), воспроизводимость расследований (доля шагов по плейбукам/скриптам с машинно-читаемым журналированием) и устойчивость под нагрузкой (сопоставление соблюдения SLA «пик/база») – а также интегральный показатель управляемости, агрегирующий нормированные компоненты «скорость – качество/точность – полнота наблюдаемости – воспроизводимость».

Выводы.

– Добавление трех индикаторов к MTTD/MTTR повышает объяснимость и сопоставимость отчетности, позволяя отличать формальные улучшения по времени от реального роста управляемости процесса [3].

– Индикаторы технологически реализуемы на имеющейся телеметрии SIEM/XDR и журналах SOAR без замены инфраструктуры: требуется унификация событий, разметка доменов контекста и фиксация шагов расследований.

– На типовых классах инцидентов индикаторы подсвечивают «слепые зоны» наблюдаемости и вариативность ручных действий, что напрямую связано с риском «alert-fatigue» и потерей качества при пиковых нагрузках.

Практические рекомендации.

– Включать рядом с MTTD/MTTR: долю инцидентов с ≥ 3 независимыми доменами (контекст), долю шагов по плейбукам/скриптам (воспроизводимость), пару значений SLA «пик/база» и коэффициент устойчивости; для управленческой витрины – интегральный индекс с разложением по компонентам.

– В каждом цикле отчетности фиксировать причины недобора источников (пробелы наблюдаемости, недоступные логи, технический долг) и план их закрытия; вести чек-лист качества (полнота, целостность, задержки доставки, корректность тайм-стампов).

– Опираться на SOAR для машинно-читаемого журналирования и исполнения плейбуков; поддерживать версионирование сценариев и их соответствие фактической практике расследований [6, 9].

– Для малых контуров временно допускать порог ≥ 2 источников с явной пометкой в методике и отдельной интерпретацией результатов.

Направления дальнейших исследований.

– Межотраслевая валидация индикаторов и чувствительность к качеству телеметрии и настройкам SLA; формирование эталонных порогов и доверительных интервалов для сравнения разных SOC [3].

– Автоматизация расчетов и визуализации в реальном времени (pipeline поверх SIEM/XDR/SOAR) и оценка влияния обновлений плейбуков на динамику индексов.

– Исследование применения больших языковых моделей для суммаризации инцидентов и извлечения шагов расследований из неструктурированных логов (с контролем воспроизводимости и аудируемости) [14].

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Шабловский Я.К., Гельфанд А.М. Обзор технологии SOC (Security Operations Center). *Инновации. Наука. Образование*. 2021;(33):1316–1321.
2. Кузнецов А.В. Организация раздельного хранения данных о событиях безопасности. *Вопросы кибербезопасности.* 2024;(2):22–28. https://doi.org/10.21681/2311-3456-2024-2-22-28
   Kuznetsov A.V. The Organization of Separate Security Event Data Storage. *Voprosy kiberbezopasnosti.* 2024;(2):22–28. (In Russ.). https://doi.org/10.21681/2311-3456-2024-2-22-28
3. Forsberg J., Frantti T. Technical Performance Metrics of a Security Operations Center. *Computers & Security*. 2023;135. https://doi.org/10.1016/j.cose.2023.103529
4. Agyepong E., Cherdantseva Yu., Reinecke Ph., Burnap P. A Systematic Method for Measuring the Performance of a Cyber Security Operations Centre Analyst. *Computers & Security*. 2023;124. https://doi.org/10.1016/j.cose.2022.102959
5. Шилова А.Д. Критерий безопасности сетевой инфраструктуры. *Научно-технический вестник информационных технологий, механики и оптики.* 2023;23(3):530–537. https://doi.org/10.17586/2226-1494-2023-23-3-530-537
   Shilova A.D. Criterion of the Network Infrastructure Security. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics.* 2023;23(3):530–537. (In Russ.). https://doi.org/10.17586/2226-1494-2023-23-3-530-537
6. Bridges R.A., Rice A.E., Oesch S., et al. Testing SOAR Tools in Use. *Computers & Security*. 2023;129. https://doi.org/10.1016/j.cose.2023.103201
7. Islam M.A. Application of Artificial Intelligence and Machine Learning in a Security Operations Center. *Issues in Information Systems*. 2023;24(4):311–327. https://doi.org/10.48009/4_iis_2023_124
8. González-Granadillo G., González-Zarzosa S., Diaz R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*. 2021;21(14). https://doi.org/10.3390/s21144759
9. Shaked A., Cherdantseva Yu., Burnap P., Maynard P. Operations-Informed Incident Response Playbooks. *Computers & Security*. 2023;134. https://doi.org/10.1016/j.cose.2023.103454
10. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 1. *Труды СПИИРАН*. 2016;(4):5–27. https://doi.org/10.15622/sp.47.1
    Fedorchenko A., Levshun D., Chechulin A., Kotenko I. An Analysis of Security Event Correlation Techniques in SIEM-Systems. Part 1. *SPIIRAS Proceedings.* 2016;(4):5–27. (In Russ.). https://doi.org/10.15622/sp.47.1
11. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 2. *Труды СПИИРАН*. 2016;(6):208–225. https://doi.org/10.15622/sp.49.11
    Fedorchenko A., Levshun D., Chechulin A., Kotenko I. An Analysis of Security Event Correlation Techniques in SIEM-Systems. Part 2. *SPIIRAS Proceedings*. 2016;(6):208–225. (In Russ.). https://doi.org/10.15622/sp.49.11
12. Mahboubi A., Luong Kh., Aboutorab H., et al. Evolving Techniques in Cyber Threat Hunting: A Systematic Review. *Journal of Network and Computer Applications*. 2024;232. https://doi.org/10.1016/j.jnca.2024.104004
13. Афанасьева С.В., Кузьмина У.В. Основные проблемы при работе с центрами мониторинга информационной безопасности. *Вестник УрФО. Безопасность в информационной сфере.* 2023;(1):51–58. https://doi.org/10.14529/secur230105

Afanaseva S.V., Kuzmina U.V. Main Problems Working with Security Operation Center. *Journal of the Ural Federal District. Information Security.* 2023;(1):51–58. (In Russ.). https://doi.org/10.14529/secur230105

14. Feng W., Cao Yu, Chen Y. Multi-Granularity User Anomalous Behavior Detection. *Applied Sciences*. 2025;15(1). https://doi.org/10.3390/app15010128

ИНФОРМАЦИЯ ОБ АВТОРЕ / INFORMATION ABOUT THE AUTHOR

Пахомов Валерий Владиславович, аспирант, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Москва, Российская Федерация.
e-mail: pedobiric@gmail.com

Valeriy V. Pakhomov, Postgraduate, The Russian Presidential Academy of National Economy and Public Administration, Moscow, the Russian Federation.

Статья поступила в редакцию 11.10.2025; одобрена после рецензирования 07.11.2025; принята к публикации 17.11.2025.

The article was submitted 11.10.2025; approved after reviewing 07.11.2025; accepted for publication 17.11.2025.