18. *Trofimenko S.V., Trofimenko S.V., Marshalov A.Ya., Grib N.N., Kolodeznikov I.I.* Modifikatsiya metoda Irvina dlya vyyavleniya anomal'nykh urovney vremennykh ryadov: metodika i chislennye eksperimenty [Modification of the Irwin method for identifying anomalous levels of time series: methodology and numerical experiments], *Sovremennye problemy nauki i obrazovaniya* [Modern problems of science and education], 2014, № 5. Available at: https://science-education.ru/ru/article/view?id=15130 (accessed 15 February 2025).
19. *Gufel'd I.L., Gavrilov V.A., Korol'kov A.V. i Novoselov O.N.* Endogennaya aktivnost' Zemli i dekompressionnaya model' seysmicheskogo shuma [Endogenous activity of the Earth and decompression model of seismic noise], *Doklady Akademii nauk SSSR* [Reports of the USSR Academy of Sciences], 2008, Vol. 423, No. 6, pp. 811-814.
20. *Novoselov O.N.* Identifikatsiya i analiz dinamicheskikh sistem: monografiya [Identification and analysis of dynamic systems: monograph]. 3rd ed. Moscow: GOU VPO MGUL, 2010, 424 p.

Клевцов Сергей Иванович – Южный федеральный университет; e-mail: sergkmps@mail.ru; г. Таганрог, Россия; тел.: 88634328025; к.т.н.; доцент.

Klevtsov Sergey Ivanovich – Southern Federal University; e-mail: sergkmps@mail.ru; Taganrog, Russia; phone: +78634328025; cand. of eng. sc.; associate professor.

УДК 004.89 DOI 10.18522/2311-3103-2025-4-57-69

В.А. Частикова, А.С. Бахтин, П.А. Меркулов

РАЗРАБОТКА МЕТОДИКИ ИНТЕГРАЦИИ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ В ПРОЦЕССЫ ЦЕНТРА МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Показана важность интеграции больших языковых моделей (БЯМ) в процессы центров мониторинга информационной безопасности (SOC) для повышения их эффективности в условиях растущих киберугроз. Цель исследования – разработка методики интеграции БЯМ в SOC, направленной на автоматизацию процессов анализа данных и реагирования на инциденты. Задачи исследования включают теоретическое обоснование и разработку платформы для безопасного внедрения БЯМ, а также оценку существующих процессов и технической инфраструктуры SOC. В статье анализируются ключевые метрики эффективности работы SOC, такие как среднее время обнаружения инцидента и количество нерешенных инцидентов, и предлагается использование подхода GQM (Goal-Question-Metric) для разработки этих метрик. Рассматривается также необходимость оценки рисков, связанных с использованием БЯМ, с учетом уязвимостей и угроз, а также методов их минимизации, включая использование списка критических уязвимостей от OWASP. В статье предложены основные этапы разработки и внедрения системы, включая инвентаризацию существующих ресурсов, анализ сложности интеграции и развертывание системы. Рассматриваются ключевые аспекты, такие как оценка сложности интеграции, эксплуатационные и поддерживающие факторы, а также оценка рисков, связанных с внедрением новых технологий в инфраструктуру SOC. В заключение подчеркивается актуальность использования БЯМ для улучшения оперативности и качества работы SOC, что способствует повышению уровня информационной безопасности и ускорению реакции на киберугрозы. Внедрение таких технологий позволит SOC не только быстрее реагировать на инциденты, но и повысить точность анализа данных, снижая риски, связанные с человеческим фактором.

Автоматизация; инцидент; большая языковая модель; генеративный искусственный интеллект; центр мониторинга информационной безопасности.

V.A. Chastikova, A.S. Bahtin, P.A. Merkulov

DEVELOPMENT OF A METHODOLOGY FOR INTEGRATING LARGE LANGUAGE MODELS INTO THE PROCESSES OF SECURITY OPERATIONS CENTERS

The article discusses the importance of integrating large language models (LLMs) into information security monitoring center processes (SOCs) to increase their effectiveness in dealing with growing cyber threats. The aim of the research is to develop a method for incorporating LLMs into SOCs aimed at automating data analysis and incident response processes. The research goals include the theoretical justifica-

tion for and development of a safe LLM implementation platform, as well as assessing existing SOC processes and technical infrastructure. The article analyses key SOC metrics such as average incident detection times and the number of outstanding incidents, and proposes using the GQM approach to improve these metrics.. It also considers the need to assess the risks associated with the use of LLM, taking into account vulnerabilities and threats, as well as methods for minimizing them, including using the OWASP list of critical vulnerabilities. The article suggests the main stages of system development and implementation, including inventory of existing resources, analysis of integration complexity and system deployment. Key aspects such as assessing the complexity of integration, operational and supporting factors, as well as assessing risks associated with introducing new technologies into SOC infrastructure, are considered. In conclusion, the relevance of LLM use is emphasized to improve efficiency and quality of SOC work, contributing to increased information security level and faster response to cyberthreats. The introduction of such technologies will allow SOC to not only respond faster to incidents, but also improve the accuracy of data analysis and reduce the risks associated with the human factor.

LLM; information security; security operations center; artificial intelligent; automatization.

Введение. Киберугрозы становятся всё более опасными, поэтому информационная безопасность организаций приобретает большое значение. Центры мониторинга информационной безопасности (SOC) играют важную роль, непрерывно отслеживая и анализируя системы для предотвращения угроз [1].

Ручной анализ больших объёмов данных требует много времени и усилий, что замедляет обнаружение и реакцию на угрозы.

Автоматизация процессов в SOC значительно повышает их эффективность, охватывая сбор и анализ данных, а также реагирование на инциденты. Это позволяет улучшить работу аналитиков, ускорить выявление угроз и снизить затраты на безопасность [2].

Обоснование необходимости интеграции больших языковых моделей в SOC. Современные центры мониторинга и реагирования на инциденты (SOC) испытывают трудности из-за увеличения количества и сложности киберугроз [3]. Аналитики прогнозируют рост использования искусственного интеллекта для атак в ближайшие годы. В этих условиях автоматизация процессов в SOC становится критически важной для повышения эффективности работы и ускорения реакции на угрозы.

Ключевым элементом такой автоматизации являются модели генеративного ИИ, однако их внедрение связано с рисками, требующими тщательного контроля. Поэтому необходимо разработать методику интеграции больших языковых моделей в процессы SOC, которая будет учитывать основные принципы разработки и эксплуатации таких систем, а также предложит соответствующую архитектуру решения.

Обзор современных научных исследований. Обзор современных исследований показывает, что LLM применяется в сфере кибербезопасности для генерации политик безопасности и автоматизации реагирования на инциденты [4]. Некоторые исследования посвящены автоматизации первичного анализа оповещений (triage), снижению когнитивной нагрузки на аналитиков SOC и снижению частоты ложных срабатываний на 87% [5, 6]. Статья Arthur Hermann показывает, что большие языковые модели могут быть использованы для классификации логов безопасности на безопасные (benign) и вредоносные (malicious), но пока что это неприменимо для мультиклассовой классификации, а только для бинарной [7].

Предложенный фреймворк Rule-ATT&CK Mapper (RAM) использует большие языковые модели для сопоставления правил SIEM с техниками MITRE ATT&CK [8]. А в сочетании с RuleGenie правила для SIEM можно оптимизировать с помощью векторизации правил и поиску похожих по косинусной близости [9].

Возможна также интеграция LLM с блокчейном и квантовой криптографией, необходима разработка нормативных документов для ИИ [10].

Также HuntGPT – прототип для обнаружения сетевых аномалий, имеет высокий потенциал благодаря сочетанию машинного обучения (ML), объяснимого искусственного интеллекта (xAI) и больших языковых моделей (LLM). Инструмент может оказаться полезным для малых или средних SOC-команд [11].

Исследование Openime Oniagbi рекомендует использовать LLM как «копилотов» для аналитиков SOC, а не полностью автономных агентов так как при использовании БЯМ часто возникают галлюцинации [12].

LLM применяются в различных доменах кибербезопасности – в анализе кода, анализе сетевого трафика, обнаружении фишинга, а также в блокчейне [13].

Основные подходы и концепции, используемых при разработке методики. Методика предназначена для разработки подхода к интеграции больших языковых моделей (БЯМ) в инфраструктуру SOC (Security Operations Center), обеспечивая безопасное и эффективное взаимодействие с уже существующими системами [14].

Основные принципы интеграции:

- платформенный подход – интеграция больших языковых моделей должна осуществляться через гибкую программную платформу;
- использование моделей в SOC – предпочтение должно отдаваться локальным экземплярам моделей для лучшего контроля данных;
- поддержка стандартных API и форматов – система должна поддерживать общепринятые механизмы взаимодействия и протоколы для совместимости с другими системами;
- асинхронность – система не должна блокировать работу при ожидании обработки запросов;
- масштабируемость – возможность горизонтального масштабирования;
- отказоустойчивость – система должна эффективно перераспределять нагрузку при отказах.

Кроме того, для обеспечения безопасности взаимодействия с моделями должны быть выполнены следующие условия:

- защищенные каналы передачи данных с шифрованием;
- аутентификация и авторизация для защиты доступа к платформе и её данным;
- ролевая модель доступа для ограничения доступа к моделям;
- интеграция с существующими системами аутентификации.

Эти принципы обеспечивают качество и безопасность взаимодействия, создавая основу для интеграции моделей в процессы SOC.

Также важны принципы взаимодействия с моделями:

- интерактивность – система на базе генеративного ИИ должна уметь обрабатывать запросы в реальном времени;
- актуальность – учет контекста запросов и предыдущих взаимодействий для предоставления актуальных данных;
- гибкость – система должна обеспечивать заменяемость моделей без зависимости от конкретных реализаций.

Применение этих принципов создаст эффективную платформу для интеграции больших языковых моделей в процессы SOC.

Описание методики интеграции больших языковых моделей. Предлагаемая методика ориентирована на теоретическое обоснование интеграции больших языковых моделей для автоматизации процессов SOC. Её цель – разработка и внедрение платформы, обеспечивающей безопасное и организованное взаимодействие с такими моделями в рамках SOC.

Методика включает следующие этапы:

1. Анализ текущих процессов SOC, определение целей и задач интеграции.
2. Оценка существующей инфраструктуры, выявление точек интеграции и разработка сценариев развертывания.
3. Оценка рисков, связанных с использованием больших языковых моделей.
4. Разработка и развертывание системы.
5. Введение в эксплуатацию.
6. Корректировка системы на основе анализа метрик.

Анализ и оценка процессов SOC. Этот этап включает оценку текущих процессов SOC, определение целей интеграции и выбор задач для автоматизации. Анализируются метрики эффективности, такие как среднее время обнаружения инцидента (MTTD) и ко-

личество нерешенных инцидентов. Метрики могут разрабатываться с использованием подхода GQM (Goal-Question-Metric), который помогает формулировать цели, вопросы и соответствующие показатели для оценки процессов SOC [15].

Таблица 1

Подход GQM для определения метрик

Цель	Вопрос	Метрика
Эффективное реагирование на инциденты	Насколько быстро происходит реагирование на инцидент?	Среднее время реагирования на инцидент или медианное время реагирования на инцидент
Увеличение автономности SOC	Сколько процессов автоматизировано?	Количество автоматизированных процессов или коэффициент автоматизированных процессов

При разработке метрик необходимо учитывать следующие факторы:

- метрики должны соответствовать целям и задачам SOC;
- метрики должны помогать в принятии решений;
- их цель и ценность должны быть очевидны как для внутренних сотрудников, так и для внешних потребителей, услуг и сервисов;
- метрики должны быть реалистичными с точки зрения сбора и точности данных;
- сбор и анализ метрик должны по возможности происходить автоматически.

Для этого можно использовать модель SMART (Specific, Measurable, Achievable, Relevant, Time-based; конкретность, измеримость, достижимость, актуальность и привязанность ко времени). Также важно учитывать зрелость процессов, для чего можно применить модель оценки процессов PAM из методологии COBIT 5 (с учетом ГОСТ Р ИСО/МЭК 15504-2-2009 Информационная технология (ИТ). Оценка процесса. Часть 2. Проведение оценки), которая оценивает вероятность достижения ожидаемых результатов процессов. В соответствии с указанной моделью выделяются уровни зрелости, указанные в табл. 2.

Таблица 2

Уровни зрелости процесса

Уровень	Обозначение уровня зрелости	Описание уровня зрелости
0	Неполный процесс	Такой процесс еще не внедрен или не способен соответствовать своему назначению. Например, основные процессы SOC отсутствуют
1	Осуществленный процесс	Осуществленный процесс достиг своего назначения. Например, процесс обработки инцидентов информационной безопасности реализован, но не документирован
2	Управляемый процесс	Процесс выполняется управляемым образом (планируется, регулируется и проводится его мониторинг), а его рабочие продукты соответствующим образом установлены, контролируются и поддерживаются. Например, имеются метрики инцидентов информационной безопасности

Окончание табл. 2

Уровень	Обозначение уровня зрелости	Описание уровня зрелости
3	Установленный процесс	Управляемый процесс на данном уровне осуществляется с использованием определенного процесса, который способен достичь выходов этого процесса. Например, есть документированный процесс обработки инцидентов информационной безопасности, метрики инцидентов документированы
4	Предсказуемый процесс	Процесс на данном уровне осуществляется в определенных пределах для достижения выходов этого процесса. Например, целевые показатели по выявлению и обработке инцидентов задокументированы и выполняются
5	Оптимизирующий процесс	Предсказуемый процесс на данном уровне непрерывно улучшается для достижения соответствующих текущих и планируемых бизнес-целей. Например, проводится регулярная оценка эффективности SOC, производится выстраивание процессов для достижения максимальных ключевых показателей эффективности

Для определения процессов, подлежащих автоматизации, необходимо оценить основные метрики SOC и зрелость процессов, чтобы выявить те, которые требуют улучшения. Время для расчета метрик определяется в зависимости от специфики SOC. Пример оценки типовых метрик за определенный промежуток времени приведен в табл. 3.

Таблица 3

Оценка метрик за условный временной промежуток

Метрика	Оценка за текущий период	Оценка за предыдущий период	Изменение в процентах
Среднее время обнаружения (MTTD)	54 минуты	48 минут	11.11%
Среднее время расследования (MTTI)	600 минут	570 минут	5.00%
Среднее время сдерживания (MTTC)	480 минут	420 минут	-12.50%
Среднее время восстановления (MTTR)	330 минут	360 минут	-8.33%
Количество инцидентов	200	150	33.33%
Коэффициент закрытых инцидентов	0.85	0.80	6.25%
Количество ложноположительных оповещений	55	60	-8.33%
Количество инцидентов на аналитика	11	10	10.00%

Необходимо составить матрицу влияния процессов на метрики, где влияние и сложность оцениваются по шкале от 0 до 3 (отсутствует – 0, низкое – 1, среднее – 2, высокое – 3). Аналогичным образом оценивается степень автоматизации. Система баллов может быть расширена, если потребуется. Пример для временных метрик приведен в табл. 4.

Таблица 4

Влияние процессов на ключевые метрики SOC

Процесс SOC	Среднее время обнаружения (MTTD)	Среднее время расследования (MTTI)	Среднее время сдерживания (MTTC)	Среднее время восстановления (MTTR)
Сбор информации об инцидентах	Высокое	Высокое	Среднее	Среднее
Сбор данных о киберугрозах	Высокое	Высокое	Высокое	Среднее
Повышение квалификации персонала	Низкое	Среднее	Среднее	Среднее
Составление планов реагирования на инциденты	Низкое	Высокое	Высокое	Высокое
Расследование инцидентов	Низкое	Высокое	Высокое	Высокое

На основе перечня процессов и уровней зрелости необходимо определить сценарии автоматизации с помощью ИИ, оценить их влияние на процессы, степень автоматизации и сложность реализации. Влияние рассчитывается как среднее арифметическое значений влияния процесса на метрики, округленное до ближайшего целого. Пример оценки процессов и сценариев автоматизации приведен в табл. 5.

Таблица 5

Оценка процессов

Процесс	Уровень зрелости	Сценарий автоматизации с помощью ИИ	Влияние на процессы	Сложность автоматизации	Степень автоматизации
Сбор информации об инцидентах	3	Генерация отчетов на основе логов инцидентов	Высокое	Низкая	Полная
Сбор данных о киберугрозах	2	Предоставление и интерпретация информации относительно запроса специалиста	Высокое	Средняя	Частичная
Повышение квалификации персонала	3	Предоставление и интерпретация информации относительно запроса специалиста	Среднее	Низкая	Частичная
Составление планов реагирования на инциденты	3	Составление «плейбуков» для инцидентов на основе уже существующих	Высокое	Высокая	Частичная
Расследование инцидентов	3	Ассистирование с помощью поиска релевантной информации	Высокое	Высокая	Частичная

На основе данных из таблицы необходимо приоритизировать процессы по принципу «от простого к сложному» с учетом следующих критериев сортировки:

1. Возрастание сложности автоматизации.
2. Возрастание степени автоматизации.
3. Убывание влияния на процессы.
4. Убывание уровня зрелости.

При совпадении значений приоритет определяется произвольно.

Таблица 6

Приоритет автоматизации процессов

Приоритет	Процесс	Сценарий автоматизации с помощью ИИ	Уровень зрелости	Влияние на процессы	Сложность автоматизации	Степень автоматизации
1	Повышение квалификации персонала	Предоставление и интерпретация информации относительно запроса специалиста	3	Среднее	Низкая	Частичная
2	Сбор данных о киберугрозах	Предоставление и интерпретация информации относительно запроса специалиста	2	Высокое	Средняя	Частичная
3	Сбор информации об инцидентах	Генерация отчетов на основе логов инцидентов	3	Высокое	Средняя	Полная
4	Составление планов реагирования на инциденты	Составление «плейбуков» для инцидентов на основе уже существующих	3	Высокое	Высокая	Частичная
5	Расследование инцидентов	Ассистирование с помощью поиска релевантной информации	3	Высокое	Высокая	Частичная

Полученный список используется для определения целей и задач интеграции. Например, для процесса повышения квалификации персонала целью автоматизации с помощью ИИ является улучшение осведомленности специалистов SOC. Задачи автоматизации включают:

- предоставление интерфейса для запросов по информационной безопасности;
- обеспечение эффективности взаимодействия с платформой;
- поддержание актуальности данных для работы с большими языковыми моделями.

Оценка существующей технической инфраструктуры и составление сценариев интеграции. На этом этапе необходимо провести инвентаризацию существующих систем и аппаратных ресурсов в SOC. Затем следует проанализировать их возможность интеграции с новой системой, оценив сложность интеграции, эксплуатации и поддержки каждой из них.

Таблица 7

Пример оценки существующих систем

Система	Тип системы	Механизмы интеграции	Сценарии интеграции	Сложность поддержки и эксплуатации	Сложность интеграции
Security Vision	SOAR	Коннекторы	Разработка коннектора и сценариев применения в no-code/low-code платформе	Низкая	Средняя
MaxPatrol SIEM	SIEM	REST API	Разработка логики взаимодействия в коде интегрируемой платформы; разработка интеграционного скрипта	Высокая	Высокая
MaxPatrol EDR	EDR	Разработка интеграционного модуля	Разработка модуля с помощью Lua-кода	Высокая	Высокая

Исходя из таблицы видно, что наибольшую способность к интеграции демонстрируют SOAR системы, которые являются не только инструментами реагирования на инциденты, но и платформами для интеграции. Для SOC предпочтительнее выбирать такие интеграционные платформы. Если SOAR-система отсутствует, следует рассмотреть её добавление. В случае невозможности внедрения SOAR или аналогичных систем, можно изучить возможность интеграции с текущими решениями через скрипты или разработку интеграционных модулей. Рис. 1 иллюстрирует пример точки интеграции с инфраструктурой SOC [16].

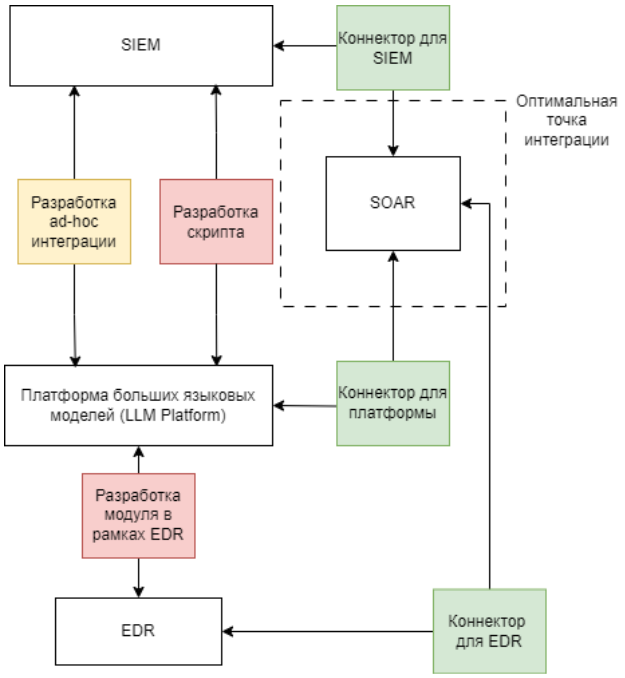

Рис. 1. Пример определения точки интеграции в рамках SOC

На рис. 2 изображено схематическое расположение интегрируемой системы в инфраструктуре SOC.

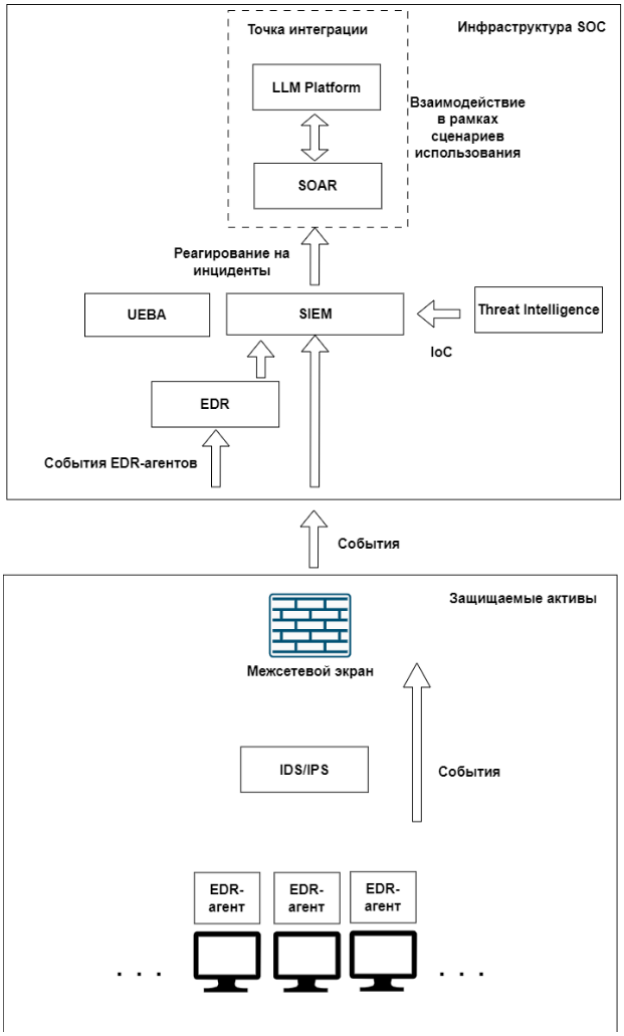

Рис. 2. Расположение интегрированной системы в инфраструктуре SOC

Следующий шаг – описание потоков данных в инфраструктуре SOC для автоматизации с использованием больших языковых моделей. Пример диаграммы данных приведен на рис. 3.

Описание данных позволяют понимать каким образом данные двигаются в рамках процессов, а также позволяют оценить потенциал интеграции.

Для ответственных задач следует рассматривать развертывание на физических, выделенных или облачных серверах с GPU [17]. Наиболее безопасным вариантом является использование физического GPU-сервера в инфраструктуре SOC, но это увеличивает затраты на интеграцию [18]. Альтернативой может быть подключение моделей через API официальных поставщиков, однако это сопряжено с риском утечки чувствительных данных, поэтому такой подход допустим только при отсутствии конфиденциальной информации в автоматизируемых процессах. Характеристики пяти возможных сценариев развертывания приведены в табл. 8.

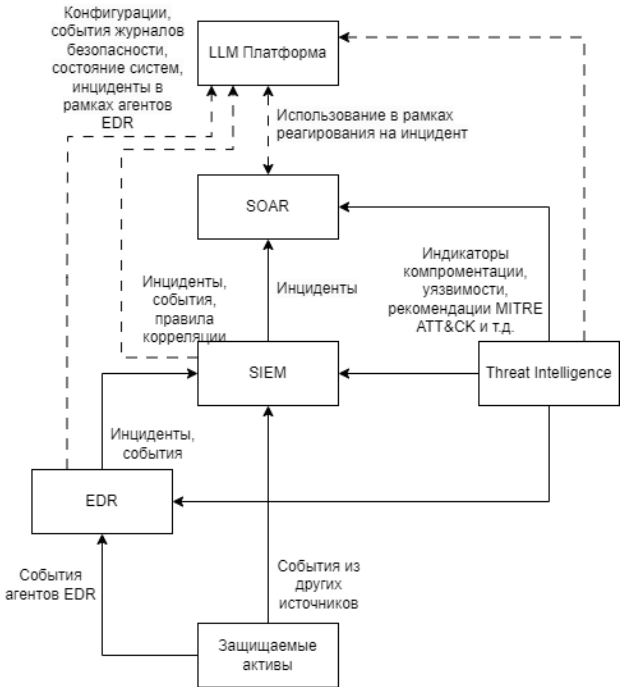

Рис. 3. Пример диаграммы описания данных в инфраструктуре SOC

Таблица 8

Сценарии развертывания моделей

Сценарий развертывания	Эффективность	Затраты	Контроль данных
Локально на центральном процессоре	Низкая	Низкие	Высокий
Локально на GPU-сервере	Высокая	Высокие	Высокий
На выделенном сервере	Высокая	Высокие	Средний
На облачном сервере	Высокая	Средние	Средний
С помощью поставщика моделей	Высокая	Низкие	Низкий

Поскольку автоматизаций процессов может быть много, для каждого процесса выбирается свой сценарий развертывания. Это обеспечивает гибкость и масштабируемость использования ресурсов без привязки к одному конкретному сценарию.

Оценка и учет рисков связанных с большими языковыми моделями. При интеграции больших языковых моделей необходимо учитывать их уязвимости и связанные угрозы. Для оценки, необходимо обратиться к ресурсу OWASP, который описывает 10 самых распространённых уязвимостей БЯМ [19].

Данные уязвимости необходимо учитывать при разработке платформы.

Разработка и развертывание системы. На данном этапе проводится разработка, проверка, конфигурация и развертывание системы. Несмотря на отсутствие специализированных LLM-платформ для SOC, наблюдается активное развитие данной области. Предполагается, что решение уже разработано или разрабатывается в рамках компании. Архитектура решения описана в следующем разделе.

Перед развертыванием необходимо убедиться в соблюдении ряда требований безопасности:

♦ секреты и аутентификационные данные должны храниться в безопасных хранилищах;

♦ файлы моделей и актуальные данные должны быть защищены от несанкционированного доступа;

♦ доступ к моделям должен быть ограничен на уровне сети, а сами модели должны поступать из надежных источников.

После этого следует развертывание системы, настройка интеграции, составление сценариев использования и первичное тестирование. Оцениваются метрики эффективности, на основе которых выполняется дополнительная настройка конфигураций и скриптов. Важным шагом является настройка механизмов актуализации данных. При необходимости проводится дообучение моделей под конкретный контекст SOC.

После успешного развертывания система вводится в эксплуатацию. На этом этапе оцениваются метрики эффективности работы системы, такие как медианное время ответа, время импорта данных, коэффициенты "галлюцинаций" и неверных ответов, коэффициент выполненных процессов автоматизации, среднее время простоя. На основе полученных данных проводятся доработки и планируются улучшения.

В процессе эксплуатации оцениваются ключевые метрики SOC и интегрированного решения, и на основе их анализа производится корректировка функционирования системы [20].

Заключение. В данной статье показана актуальность и необходимость разработки методики интеграции больших языковых моделей в процессы центра мониторинга информационной безопасности, описаны основные принципы и этапы интеграции.

По результату внедрения БЯМ в инфраструктуру SOC достигается не только повышение оперативности реакции, но и улучшение качества анализа данных. Так же интеграция, проведенная по правильной методике, позволяет вносить в систему изменения без необходимости вмешательства в основные рабочие процессы, что способствует минимизации сбоев и повышению общей отказоустойчивости системы.

Рассмотренный сценарий применения доказывает эффективность технологий ИИ в роли средства автоматизации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Центр мониторинга информационной безопасности (Security Operations Center, SOC). – URL: https://encyclopedia.kaspersky.ru/glossary/security-operations-center-soc.
2. *Частикова В.А., Митюгов А.И.* Методика построения системы анализа инцидентов информационной безопасности на основе нейроиммунного подхода // Электронный сетевой политематический журнал "Научные труды КубГТУ". – 2022. – № 1. – С. 98-105.
3. Национальная база данных уязвимостей. – URL: https://nvd.nist.gov/vuln.
4. *Hasanov I., Virtanen S., Hakkala A., Isoaho J.* Application of Large Language Models in Cybersecurity: A Systematic Literature Review // IEEE Access. – 2024. – Vol. 12. – P. 176751-176778. – DOI: 10.1109/ACCESS.2024.3505983.
5. *Singh Y., Patel N.D., Shandilya S.K.* Enhancing Security Operations Center Efficiency through Multi-Model Integration of Large Language Models and SIEM Systems // Preprints. – 2024. – DOI: 10.21203/rs.3.rs-5615639/v1.
6. *Kotilingala S.* Leveraging large language models for enhanced threat detection in security operations centers // World Journal of Advanced Engineering Technology and Sciences. – 2025. – Vol. 15, No. 1. – P. 579-591. – URL: https://doi.org/10.30574/wjaets.2025.15.1.0241 – DOI: 10.30574/wjaets.2025.15.1.0241.
7. *Hermann A.* GPT Powered Log Analysis: Enhancing SOC Decision Making for Malicious and Benign Security Log Classification // Twente Student Conference on IT (TSeIT 41). – Enschede, Netherlands, 2024. – P. 1-6.
8. *Wudali P.N., Kravchik M., Malul E., Gandhi P.A., Elovici Y.* A. Shabtai Rule-ATT&CK Mapper (RAM): Mapping SIEM Rules to TTPs Using LLMs // arXiv preprint. – 2024. – URL: https://arxiv.org/abs/2502.02337v1.
9. *Shukla A., Gandhi P.A., Elovici Y., Shabtai A.* RuleGenie: SIEM Detection Rule Set Optimization // arXiv. – 2024. – URL: https://arxiv.org/abs/2505.06701v1.
10. *Zangana H.M., Mohammed H.S., Husain M.M.* The Role of Large Language Models in Enhancing Cybersecurity Measures: Empirical Evidence from Regional Banking Institutions // Sistemasi: Jurnal Sistem Informasi. – 2025. – Vol. 14, No. 5. – P. 2018–2027. – URL: https://sistemasi.ftik.unisi.ac.id/index.php/stmsi/article/download/5144/1029.

11. *Ali T., Kostakos P.* HuntGPT: Integrating Machine Learning-Based Anomaly Detection and Explainable AI with Large Language Models (LLMs) // arXiv. – 2023. – URL: https://arxiv.org/abs/2309.16021v1. – DOI: 10.48550/arXiv.2309.16021.
12. *Oniagbi O., Hakkala A., Hasanov I.* Evaluation of LLM Agents for the SOC Tier 1 Analyst Triage Process // University of Turku. – 2024. – 62 p. – URL: https://www.utupub.fi/bitstream/handle/10024/178601/Oniagbi_Openime_Thesis.pdf?sequence=1.
13. *Ali A., Ghanem M.C.* Beyond Detection: Large Language Models and Next-Generation Cybersecurity // SHIFRA. – 2025. – Vol. (2025). – P. 81-97. – ISSN: 3078-3186. – URL: https://www.researchgate.net/publication/390931574_Beyond_Detection_Large_Language_Models_and_Next-Generation_Cybersecurity.
14. *Частикова В.А., Гуляй В.Г.* Подход к построению систем анализа инцидентов информационной безопасности на основе гибридизации методов машинного обучения // Электронный сетевой политематический журнал "Научные труды КубГТУ". – 2023. – № 6. – С. 107-117.
15. Key SOC metrics and KPIs: How to define and use them. – URL: https://www.techtarget.com/searchsecurity/tip/How-SOC-metrics-improve-security-operation-centers-performance.
16. *Селезнёв В.М., Боровская О.Е.* Встраивание инструментов SOAR-платформ в экосистему SOC для автоматизации процесса реагирования на инциденты ИБ // Международный научно-исследовательский журнал. – 2022. – № 10 (124). – URL: https://research-journal.org/archive/10-124-2022-october/10.23670/IRJ.2022.124.8. – DOI: 10.23670/IRJ.2022.124.8.
17. Running Local LLMs, CPU vs. GPU - a Quick Speed Test. – URL: https://dev.to/maximsaplin/running-local-llms-cpu-vs-gpu-a-quick-speed-test-2cjn.
18. CPU vs GPU for Running LLMs Locally. – URL: https://www.marktechpost.com/2024/03/23/cpu-vs-gpu-for-running-llms-locally/.
19. OWASP Top 10 for LLM Applications. – URL: https://owasp.org/www-project-top-10-for-large-language-model-applications/assets/PDF/OWASP-Top-10-for-LLMs-2023-v1_1.pdf.
20. *Бахтин А.С.* Разработка методики интеграции больших языковых моделей в процессы центра мониторинга информационной безопасности: дипломная работа по специальности 10.05.03 «Информационная безопасность автоматизированных систем». – Краснодар: Кубанский государственный технологический университет, 2024. – 93 с.

REFERENCES

1. Tsentr monitoringa informatsionnoy bezopasnosti (Security Operations Center, SOC) [Information Security Monitoring Center (Security Operations Center, SOC)]. Available at: https://encyclopedia.kaspersky.ru/glossary/security-operations-center-soc.
2. *Chastikova V.A., Mityugov A.I.* Metodika postroeniya sistemy analiza intsidentov informatsionnoy bezopasnosti na osnove neyroimmunnogo podkhoda [Methodology for building a system for analyzing information security incidents based on a neuroimmune approach], *Elektronnyy setevoy politematicheskiy zhurnal "Nauchnye trudy KubGTU"* [Electronic network political journal "Scientific Works of KubSTU"], 2022, No. 1, pp. 98-105.
3. Natsional'naya baza dannykh uyazvimostey [National Vulnerability Database]. Available at: https://nvd.nist.gov/vuln.
4. *Hasanov I., Virtanen S., Hakkala A., Isoaho J.* Application of Large Language Models in Cybersecurity: A Systematic Literature Review, *IEEE Access*, 2024, Vol. 12, pp. 176751-176778. DOI: 10.1109/ACCESS.2024.3505983.
5. *Singh Y., Patel N.D., Shandilya S.K.* Enhancing Security Operations Center Efficiency through Multi-Model Integration of Large Language Models and SIEM Systems, *Preprints*, 2024. DOI: 10.21203/rs.3.rs-5615639/v1.
6. *Kotilingala S.* Leveraging large language models for enhanced threat detection in security operations centers, *World Journal of Advanced Engineering Technology and Sciences*, 2025, Vol. 15, No. 1, pp. 579-591. Available at: https://doi.org/10.30574/wjaets.2025.15.1.0241 DOI: 10.30574/wjaets.2025.15.1.0241.
7. *Hermann A.* GPT Powered Log Analysis: Enhancing SOC Decision Making for Malicious and Benign Security Log Classification, *Twente Student Conference on IT (TSeIT 41)*. Enschede, Netherlands, 2024, pp. 1-6.
8. *Wudali P.N., Kravchik M., Malul E., Gandhi P.A., Elovici Y.* A. Shabtai Rule-ATT&CK Mapper (RAM): Mapping SIEM Rules to TTPs Using LLMs, *arXiv preprint*, 2024. Available at: https://arxiv.org/abs/2502.02337v1.
9. *Shukla A., Gandhi P.A., Elovici Y., Shabtai A.* RuleGenie: SIEM Detection Rule Set Optimization, *arXiv*, 2024. Available at: https://arxiv.org/abs/2505.06701v1.

10. *Zangana H.M., Mohammed H.S., Husain M.M.* The Role of Large Language Models in Enhancing Cybersecurity Measures: Empirical Evidence from Regional Banking Institutions, *Sistemasi: Jurnal Sistem Informasi,* 2025, Vol. 14, No. 5, pp. 2018–2027. Available at: https://sistemasi.ftik.unisi.ac.id/index.php/stmsi/article/download/5144/1029.
11. *Ali T., Kostakos P.* HuntGPT: Integrating Machine Learning-Based Anomaly Detection and Explainable AI with Large Language Models (LLMs), *arXiv,* 2023. Available at: https://arxiv.org/abs/2309.16021v1. – DOI: 10.48550/arXiv.2309.16021.
12. *Oniagbi O., Hakkala A., Hasanov I.* Evaluation of LLM Agents for the SOC Tier 1 Analyst Triage Process, *University of Turku,* 2024, 62 p. Available at: https://www.utupub.fi/bitstream/handle/10024/178601/Oniagbi_Openime_Thesis.pdf?sequence=1.
13. *Ali A., Ghanem M.C.* Beyond Detection: Large Language Models and Next-Generation Cybersecurity, *SHIFRA,* 2025, Vol. (2025), pp. 81-97. ISSN: 3078-3186. Available at: https://www.researchgate.net/publication/390931574_Beyond_Detection_Large_Language_Models_and_Next-Generation_Cybersecurity.
14. *Chastikova V.A., Gulyay V.G.* Podkhod k postroeniyu sistem analiza intsidentov informatsionnoy bezopasnosti na osnove gibridizatsii metodov mashinnogo obucheniya [An approach to building systems for analyzing information security incidents based on the hybridization of machine learning methods], *Elektronnyy setevoy politematicheskiy zhurnal "Nauchnye trudy KubGTU"* [The electronic network political journal "Scientific works of KubSTU"], 2023, No. 6, pp. 107-117.
15. Key SOC metrics and KPIs: How to define and use them. Available at: https://www.techtarget.com/searchsecurity/tip/How-SOC-metrics-improve-security-operation-centers-performance.
16. *Seleznev V.M., Borovskaya O.E.* Vstraivanie instrumentov SOAR-platform v ekosistemu SOC dlya avtomatizatsii protsessa reagirovaniya na intsidenty IB [Embedding SOAR platform tools into the SOC ecosystem to automate the process of responding to information security incidents], *Mezhdunarodnyy nauchno-issledovatel'skiy zhurnal* [International Scientific Research Journal], 2022, No. 10 (124). Available at: https://research-journal.org/archive/10-124-2022-october/10.23670/IRJ.2022.124.8. – DOI: 10.23670/IRJ.2022.124.8.
17. Running Local LLMs, CPU vs. GPU - a Quick Speed Test. Available at: https://dev.to/maximsaplin/running-local-llms-cpu-vs-gpu-a-quick-speed-test-2cjn.
18. CPU vs GPU for Running LLMs Locally. Available at: https://www.marktechpost.com/2024/03/23/cpu-vs-gpu-for-running-llms-locally/.
19. OWASP Top 10 for LLM Applications. Available at: https://owasp.org/www-project-top-10-for-large-language-model-applications/assets/PDF/OWASP-Top-10-for-LLMs-2023-v1_1.pdf.
20. *Bakhtin A.S.* Razrabotka metodiki integratsii bol'shikh yazykovykh modeley v protsessy tsentra monitoringa informatsionnoy bezopasnosti: diplomnaya rabota po spetsial'nosti 10.05.03 «Informatsionnaya bezopasnost' avtomatizirovannykh sistem» [Development of a methodology for integrating large language models into the processes of the Information security Monitoring Center: thesis on specialty 05/10/03 "Information security of automated systems"]. Krasnodar: Kubanskiy gosudarstvennyy tekhnologicheskiy universitet, 2024, 93 p.

Частикова Вера Аркадьевна – Кубанский государственный технологический университет; e-mail: chastikova_va@mail.ru; г. Краснодар, Россия; тел.: 89184635536; кафедра кибербезопасности и защиты информации; к.т.н.; доцент.

Бахтин Антон Сергеевич – Кубанский государственный технологический университет; e-mail: bahtin_.anton@mail.ru; г. Краснодар, Россия; тел.: 89180149890; кафедра кибербезопасности и защиты информации, студент.

Меркулов Павел Алексеевич – Кубанский государственный технологический университет; e-mail: merkulov.pashka444@gmail.com; г. Краснодар, Россия; тел.: 89182951008; кафедра кибербезопасности и защиты информации; аспирант.

Chastikova Vera Arkadyevna – Kuban State Technological University; e-mail: chastikova_va@mail.ru; Krasnodar, Russia; phone: +79184635536; the Department of Cybersecurity and Information Protection; cand. of eng. sc.; associate professor.

Bahtin Anton Sergeevich – Kuban State Technological University; e-mail: bahtin_.anton@mail.ru; Krasnodar, Russia; phone: +79180149890; the Department of Cybersecurity and Information Protection; student.

Merkulov Pavel Alekseevich – Kuban State Technological University; e-mail: merkulov.pashka444@gmail.com; Krasnodar, Russia; phone: +79182951008; the Department of Cybersecurity and Information Protection; graduate student.