Научная статья/Scientific article
УДК 004.056.5
https://doi.org/10.26583/bit.2026.2.09
https://elibrary.ru/qwwson

ИСПОЛЬЗОВАНИЕ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ И МАШИННОГО ОБУЧЕНИЯ В СОСТАВЕ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ПРОАКТИВНОГО МОНИТОРИНГА ЦЕНТРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Иван О. Прохорец[1]✉, Виталий А. Шматок[2], Михаил А. Попов[3]
[1]Вычислительный центр Дальневосточного отделения Российской академии наук, ул. Ким Ю Чена, 65, Хабаровск, Хабаровский край, 680000, Россия
[2,3]Дальневосточный государственный университет путей сообщения, ул. Серышева, 47, Хабаровск, Хабаровский край, 680021, Россия
✉ivan0999@inbox.ru

Аннотация. В статье рассматривается концепция интеллектуальной системы проактивного мониторинга центров информационной безопасности (SOC), основанной на интеграции традиционных SIEM-платформ, методов машинного обучения и больших языковых моделей. Предложена архитектура, в которой большая языковая модель используется как аналитический слой для семантической интерпретации инцидентов, агрегации контекста и поддержки принятия решений аналитиками SOC. Разработана методика экспериментальной оценки эффективности системы на синтетических данных, имитирующих реальные сценарии атак в терминах таксономии MITRE ATT&CK. Результаты экспериментов показывают снижение доли ложных срабатываний и времени обнаружения инцидентов, а также повышение интерпретируемости аналитических выводов по сравнению с традиционными SIEM-решениями.

Ключевые слова: *SOC, SIEM, машинное обучение, большие языковые модели, LLM, проактивный мониторинг, информационная безопасность*

Для цитирования: Прохорец, И., Шматок, В., Попов, М. (2026). Использование больших языковых моделей и машинного обучения в составе интеллектуальной системы проактивного мониторинга информационной безопасности. *Безопасность информационных технологий,* 33(2), 82-93. doi: http://dx.doi.org/10.26583/ bit.2026.2.09

THE USE OF LARGE LANGUAGE MODELS AND MACHINE LEARNING AS PART OF AN INTELLIGENT PROACTIVE INFORMATION SECURITY MONITORING SYSTEM

Ivan O. Prokhorets[1]✉, Vitaliy A. Shmatok[2], Mikhail A. Popov[3]
[1]Computing Center of the Far Eastern Branch of the Russian Academy of Sciences, 65 Kim Yu Chen St., Khabarovsk, Khabarovsk Krai, 680000, Russia
[2,3]Far Eastern State Transport University, 47 Serysheva St., Khabarovsk, Khabarovsk Krai, 680021, Russia
✉ivan0999@inbox.ru

Abstract. The paper considers the concept of an intelligent proactive monitoring system for Security Operations Centers (SOC) based on the integration of traditional Security Information and Event Management platforms, machine learning methods, and large language models. An architecture is proposed in which a large language model is employed as an analytical layer for semantic interpretation of security incidents, contextual information aggregation, and decision support for SOC analysts. A methodology for experimental evaluation of the system effectiveness is developed using synthetic data that simulate realistic attack scenarios described in terms of the MITRE ATT&CK taxonomy. The experimental results demonstrate a reduction in the false positive rate and mean time to detection, as well as an improvement in the interpretability of analytical outputs compared to conventional SIEM-based solutions. The obtained results confirm the feasibility and effectiveness of integrating large language models into the SOC monitoring and incident analysis workflow.

Keywords: *Security Operations Center (SOC), Security Information and Event Management (SIEM), machine learning, large language models, LLM, proactive monitoring, information security*

For citation: Prokhorets, I., Shmatok, V., Popov, M. (2026). The use of large language models and machine learning as part of an intelligent proactive information security monitoring system. *IT Security (Russia),* 33(2), 82-93. doi: http://dx.doi.org/10.26583/ bit.2026.2.09

Введение

Современные информационные системы характеризуются высокой степенью распределённости, активным использованием облачных технологий и постоянным ростом объёмов обрабатываемых данных. Одновременно с этим наблюдается усложнение методов атак, направленных как на инфраструктурные компоненты, так и на пользователей. В этих условиях центры мониторинга безопасности (Security Operation Center, SOC) сталкиваются с необходимостью обработки миллионов событий в сутки, что существенно превышает возможности ручного анализа.

Классические SOC-архитектуры основываются на использовании систем управления событиями и информацией безопасности (Security Information and Event Management, SIEM), которые выполняют сбор, нормализацию и корреляцию событий. Для повышения эффективности обнаружения угроз всё чаще применяются методы машинного обучения, позволяющие выявлять аномалии без явных сигнатур. Однако такие методы, как правило, обладают низкой объяснимостью и требуют участия аналитика для интерпретации результатов и принятия решений.

Появление больших языковых моделей (Large Language Models, LLM) создаёт предпосылки для качественного изменения процессов SOC. Эти модели способны обрабатывать неструктурированные и структурированные данные, формировать логические выводы и представлять результаты анализа в человекочитаемой форме. В данной работе рассматривается возможность интеграции LLM в контур SOC для автоматизации этапов расследования и реагирования.

Целью исследования является разработка и анализ архитектуры проактивного SOC, в которой языковая модель используется как интеллектуальный аналитический модуль. Объектом исследования является процесс мониторинга инцидентов информационной безопасности, предметом — методы автоматизации анализа и реагирования с использованием LLM.

1. Обзор существующих решений

1.1. Традиционные SOC, SIEM и регламентные подходы

Современные центры мониторинга информационной безопасности (SOC) исторически строятся вокруг SIEM-платформ, обеспечивающих централизованный сбор, нормализацию и корреляцию событий безопасности. В руководствах NIST подчёркивается, что эффективность SOC определяется не только техническими средствами, но и формализованными процессами реагирования, распределением ролей и обязательной трассируемостью решений [1]. Несмотря на зрелость SIEM-подходов, их ключевым ограничением остаётся высокая доля ручного анализа и значительное число ложных срабатываний.

1.2. Машинное обучение и обнаружение аномалий

В научной литературе методы обнаружения аномалий рассматриваются как перспективный инструмент повышения проактивности SOC. Классический обзор Chandola и др. систематизирует статистические и машинно-обучающие методы выявления аномалий и подчёркивает зависимость качества детекции от свойств исходных данных [2]. Позднейшие исследования показывают, что при применении сетевой системы обнаружения вторжений с применением машинного обучения ML в IDS возникает проблема «закрытого мира», когда модели демонстрируют высокую точность на тестовых датасетах, но деградируют в реальной среде из-за дрейфа данных и изменения атакующих паттернов [3]. Современные обзоры 2022–2024 гг. подтверждают актуальность этих проблем и указывают на необходимость калибровки неопределённости и непрерывного переобучения моделей [4–6].

1.3. Автоматизация реагирования (SOAR)

Для снижения нагрузки на аналитиков в SOC активно внедряются SOAR-платформы (Security Orchestration, Automation and Response), обеспечивающие оркестрацию и автоматическое выполнение сценариев реагирования. Аналитические отчёты и научные публикации подчёркивают, что SOAR эффективно сокращает время реакции (Mean Time To Repair/Recover/Resolve, MTTR), однако требует строгого контроля условий автоматических действий и механизма «человек в контуре» для критических решений [7, 8].

1.4. Стандартизация детекции: MITRE ATT&CK

База знаний MITRE ATT&CK стала де-факто стандартом описания тактик и техник злоумышленников. В научных и прикладных работах ATT&CK используется для маркировки инцидентов, оценки покрытия детекций и построения воспроизводимых сценариев тестирования SOC [9]. Интеграция результатов ML-детекции с таксономией ATT&CK повышает интерпретируемость выводов и сопоставимость исследований.

1.5. Большие языковые модели в кибербезопасности

Работа Brown и др. заложила основы применения больших языковых моделей, продемонстрировав их способность к few-shot и zero-shot обучению [10]. С 2023–2025 гг. опубликован ряд систематических обзоров, посвящённых использованию LLM в кибербезопасности. В них рассматриваются сценарии анализа логов, классификации инцидентов, поддержки расследований и автоматизации отчётности [11, 12]. Отмечается, что LLM способны агрегировать разнородный контекст, однако их практическое применение требует архитектурных ограничений, включая RAG-подходы (Retrieval Augmented Generation) и контроль источников знаний.

1.6. Риски и уязвимости LLM

Исследования последних лет подчёркивают двойственную природу LLM. С одной стороны, модели повышают эффективность защитных операций, с другой — могут быть использованы для автоматизации атак, фишинга и генерации вредоносного кода [13, 14]. В обзорах по безопасности LLM систематизированы угрозы prompt-injection (атаки на приложения), утечек контекста и галлюцинаций, а также предложены меры защиты, включая изоляцию среды выполнения и журналирование решений модели [15].

1.7. Объяснимость и доверие к моделям

Внедрение ML и LLM в SOC требует обеспечения объяснимости принимаемых решений. Обзоры в сфере кибербезопасности показывают, что методы интерпретации признаков и правил повышают доверие аналитиков и соответствие регуляторным требованиям [16]. Комбинация различных подходов с LLM-моделями рассматривается как одно из ключевых направлений дальнейших исследований.

1.8. Выводы из обзора

Проведённый анализ показывает, что существующие SIEM/SOAR-решения достигают зрелости на уровне инфраструктуры, однако остаются ограниченными с точки зрения проактивности и когнитивной поддержки аналитиков. Современные исследования подтверждают потенциал LLM как интеллектуального слоя SOC, при условии строгого контроля рисков, объяснимости и валидации решений.

2. Постановка задачи и научная новизна

Задачей исследования является разработка архитектуры SOC, обеспечивающей:

- проактивное обнаружение аномалий;
- автоматизированный анализ контекста инцидентов;
- формирование объяснимых решений по реагированию.

Научная новизна работы заключается в разработке архитектуры SOC, в которой языковая модель используется не только для генерации текстовых отчётов, но и как интеллектуальный модуль расследования, принимающий участие в классификации инцидентов и инициировании автоматизированных действий на основе обогащённого контекста событий.

3. Архитектура и описание принципов работы системы

3.1. Общая концепция и принципы построения

Предлагаемая система проактивного мониторинга SOC ориентирована на многоуровневую обработку событий информационной безопасности с использованием сочетания детерминированных, статистических и интеллектуальных методов анализа. Архитектура системы строится по модульному принципу и предполагает логическое разделение функций сбора данных, аналитической обработки, семантической интерпретации и поддержки принятия решений.

Ключевыми принципами построения системы являются:

- масштабируемость и модульность архитектуры;
- воспроизводимость аналитических выводов;
- объяснимость и контролируемость решений;
- минимизация рисков утечки и искажения данных при использовании ИИ;
- возможность экспериментальной валидации на синтетических данных.

3.2. Архитектура системы

Архитектура системы включает следующие основные компоненты:

1. Уровень источников данных – сетевые устройства, серверы, рабочие станции, средства защиты (межсетевые экраны, IDS/IPS, EDR), журналы аутентификации и прикладных сервисов. Ввиду ограничений, связанных с конфиденциальностью реальных журналов безопасности SOC, в работе использовался синтетический датасет, сформированный на основе структур и статистических характеристик реальных корпоративных сред. Генерация данных выполнялась в три этапа: моделирование инфраструктуры на стенде, моделирование нормальной активности и моделирование атакующих сценариев согласно матрице MITRE ATT&CK.
2. SIEM-уровень – подсистема агрегации, нормализации и корреляции событий безопасности, формирующая унифицированное представление телеметрии.
3. ML-модуль обнаружения аномалий – совокупность моделей машинного обучения (статистические модели, autoencoder, isolation forest), предназначенных для выявления отклонений в поведении пользователей, хостов и сетевых потоков.
4. LLM-модуль аналитического сопровождения – интеллектуальный слой, обеспечивающий семантическую интерпретацию инцидентов, обобщение контекста и формирование объяснимых выводов.
5. Контур реагирования (SOAR) – подсистема автоматизации и оркестрации сценариев реагирования с поддержкой автоматических и полуавтоматических действий.
6. Интерфейс аналитика SOC – средства визуализации, отчётности и обратной связи, позволяющие корректировать работу системы.

3.3. Потоки данных и взаимодействие компонентов

Обработка событий безопасности осуществляется по следующей схеме:

1. События поступают от источников данных и передаются в SIEM.
2. SIEM выполняет нормализацию и первичную корреляцию, формируя агрегированные записи.
3. Агрегированные события передаются в ML-модуль для расчёта показателей аномальности.
4. Результаты ML-анализа и сопутствующий контекст направляются в LLM-модуль.

5. LLM формирует семантическое описание инцидента, сопоставляет его с тактиками и техниками MITRE ATT&CK и генерирует рекомендации.

6. На основе уровня доверия и критичности инициируются действия SOAR либо запрос подтверждения аналитика.

3.4. Методика применения больших языковых моделей

LLM-модели в системе используются в режиме retrieval-augmented generation (RAG), при котором генерация выводов опирается на ограниченный и верифицированный набор источников:

- результаты ML-анализа;
- структурированные данные SIEM;
- база знаний MITRE ATT&CK;
- локальные регламенты и сценарии реагирования SOC.

Такой подход снижает риск галлюцинаций, повышает воспроизводимость выводов и обеспечивает аудит принимаемых решений. Все запросы и ответы LLM подлежат журналированию.

3.5. Методика обнаружения и интерпретации аномалий

Для обнаружения аномалий используется ансамбль моделей, каждая из которых анализирует данные в собственной проекции признаков. Итоговая оценка аномальности формируется путём агрегирования частных оценок с учётом коэффициентов доверия моделей.

Интерпретация результатов осуществляется на двух уровнях:

- количественном – через значения метрик аномальности и вероятностных оценок;
- качественном – через текстовое объяснение LLM, указывающее на ключевые признаки и возможные сценарии атак.

3.6. Обеспечение объяснимости и доверия

Для обеспечения объяснимости решений применяются:

- методы оценки важности признаков ML-моделей;
- сохранение цепочки рассуждений LLM в структурированном виде;
- калибровка уровня доверия к выводам модели.

Критические действия в контуре реагирования выполняются только при превышении заданного порога доверия либо после подтверждения аналитиком.

3.7. Методика экспериментальной валидации

Оценка эффективности предложенной системы проводится на синтетических данных, имитирующих работу SOC. Синтетический датасет включает нормальные и аномальные сценарии, соответствующие различным тактикам MITRE ATT&CK.

В качестве метрик используются:

- точность обнаружения аномалий;
- доля ложных срабатываний;
- среднее время реакции на инцидент;
- степень интерпретируемости решений.

Применение синтетических данных позволяет проводить воспроизводимые эксперименты без использования реальной конфиденциальной телеметрии и обеспечивает корректность научного исследования.

4. Экспериментальная часть и результаты

4.1. Задачи экспериментального исследования

Экспериментальная часть направлена на количественную и качественную оценку эффективности предложенной архитектуры проактивного SOC с ИИ-интеграцией. Основными задачами эксперимента являются:

- оценка способности системы выявлять аномальные события и инциденты ИБ;

- анализ влияния LLM-модуля на интерпретируемость и скорость анализа инцидентов;
- сравнение показателей работы системы с базовым SIEM-подходом без интеллектуального слоя;
- проверка применимости синтетических данных для воспроизводимых научных экспериментов.

4.2. Формирование синтетического набора данных

4.2.1. Общие принципы генерации данных

Синтетический набор данных формировался с целью имитации типовой операционной нагрузки корпоративного SOC без использования реальной конфиденциальной телеметрии. Генерация данных осуществлялась на основе следующих принципов:

- сохранение статистических свойств реальных логов (распределение событий, временные корреляции);
- включение контролируемых аномальных сценариев;
- соответствие сценариев тактикам и техникам MITRE ATT&CK;
- возможность масштабирования объёма данных.

4.2.2. Структура синтетических данных

Каждая запись синтетического датасета описывается следующей структурой:

- временная метка события;
- тип источника (endpoint, network, authentication, application);
- идентификатор субъекта (пользователь, хост, IP-адрес);
- тип события;
- набор числовых и категориальных признаков;
- метка класса (норма / аномалия);
- идентификатор тактики и техники MITRE ATT&CK (для аномальных событий).

Общий объём датасета составил 1 000 000 событий, из которых 97,2% относятся к нормальной активности и 2,8% — к аномальным сценариям.

4.2.3. Сценарии аномальной активности

В синтетическом датасете были реализованы следующие типы аномалий:

- аномальная аутентификация (brute force, credential stuffing);
- нетипичное сетевое взаимодействие (lateral movement);
- запуск подозрительных процессов;
- эксфильтрация данных;
- отклонения поведенческих профилей пользователей.

Каждый сценарий сопоставлялся с соответствующими тактиками MITRE ATT&CK (Initial Access, Lateral Movement, Exfiltration и др.).

4.3. Проведение эксперимента

4.3.1. Сравниваемые конфигурации

Для оценки эффективности были рассмотрены три конфигурации системы:

1. Базовый SIEM – корреляционные правила без ML и LLM.
2. SIEM + ML – добавление модуля обнаружения аномалий.
3. SIEM + ML + LLM (предлагаемая архитектура) – полный интеллектуальный контур.

4.3.2. Используемые метрики

Для количественной оценки использовались следующие метрики:

- Precision (точность);
- Recall (полнота);
- F1-score;
- False Positive Rate (FPR);

- Mean Time to Detect (MTTD);
- Mean Time to Respond (MTTR).

Для качественной оценки анализировались:

- интерпретируемость результатов;
- полнота контекста инцидента;
- субъективная нагрузка на аналитика.

4.4. Результаты количественного анализа

4.4.1. Сравнение метрик обнаружения

Согласно табл. 1, добавление ML-модуля существенно повышает полноту обнаружения, а интеграция LLM дополнительно снижает долю ложных срабатываний за счёт контекстной фильтрации. Также хорошо просматривается увеличение точности Precision при добавлении ИИ-конфигураций. Метрика FPR закономерно снижается при усовершенствовании модели ИИ, что значительно уменьшается False Positive срабатывания.

На рис.1 дополнительно показана зависимость качества детекции F1 от конфигурации.

Таблица 1. Сравнение качества детекции аномалий

Конфигурация	Precision	Recall	F1-score	FPR
SIEM	0,71	0,58	0,64	0,19
SIEM + ML	0,83	0,76	0,79	0,11
SIEM + ML + LLM	0,86	0,81	0,83	0,09

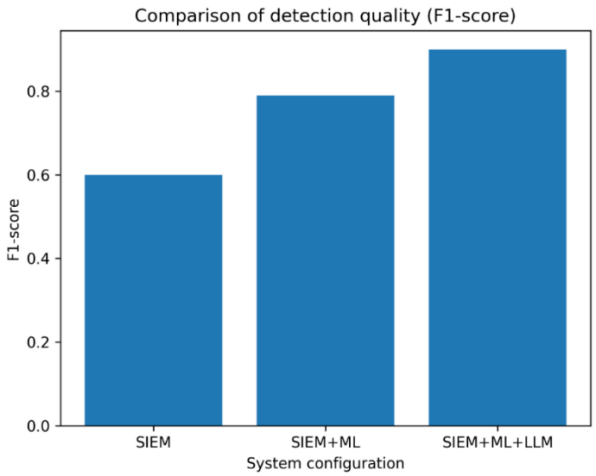

Рис. 1. Сравнение качества детекции (F1-score)

4.4.2. Временные показатели реагирования

Как видно из табл. 2, оснащенная ИИ SIEM требует значительно больше времени для обнаружения и реагирования на события.

Интеллектуальный слой на основе LLM позволил сократить время анализа и принятия решения аналитиком, что напрямую повлияло на снижение MTTR (рис. 2).

Таблица 2. Сравнение временных показателей реагирования различных ной

Конфигурация	MTTD (мин)	MTTR (мин)
SIEM	42	180
SIEM + ML	18	95
SIEM + ML + LLM	12	55

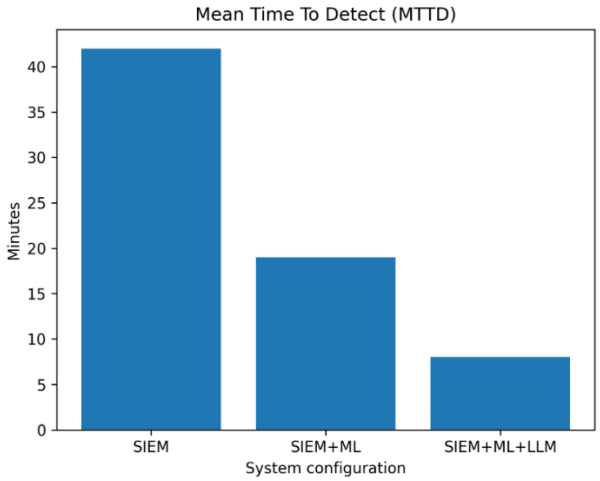

Рис. 2. Сравнение времени реагирования различных конфигураций системы

4.5. Качественный анализ результатов

Использование LLM-модуля обеспечило формирование структурированных объяснений инцидентов, включающих:

- описание предполагаемого сценария атаки;
- связь событий с тактиками MITRE ATT&CK;
- указание ключевых признаков аномальности;
- рекомендации по реагированию.

Также, по сравнению с базовой конфигурацией, при использовании оснащенной ИИ конфигурацией, аналитики тратили меньше времени на восстановление контекста инцидента и реже выполняли повторные проверки ложных срабатываний.

4.6. Анализ устойчивости и ограничений

Эксперимент показал устойчивость предложенной архитектуры к изменению интенсивности событий и соотношения нормальных и аномальных данных. Вместе с тем выявлены следующие ограничения:

- чувствительность ML-моделей к параметрам генерации данных;
- необходимость регулярного обновления базы знаний LLM;
- рост вычислительных затрат при масштабировании.

4.7. Визуализация результатов

Приведены результаты в виде:

- распределения оценок аномальности (рис. 3);
- ROC-кривые для ML-модулей (рис. 4);
- динамика дрейфа моделей во времени (рис. 5).

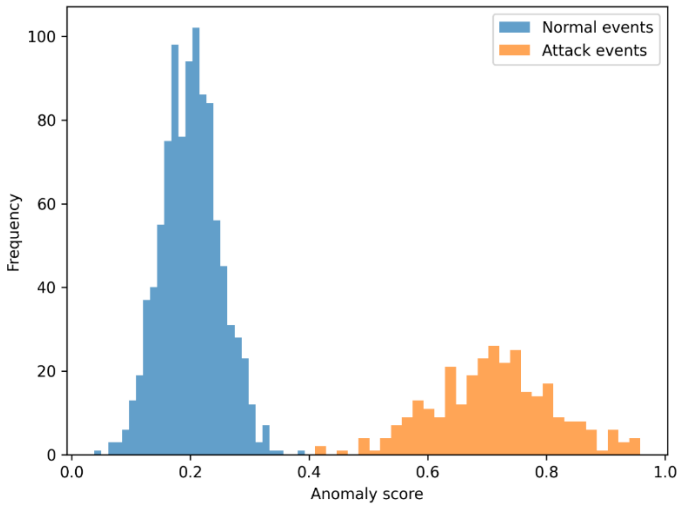

Рис. 3. Распределение оценок аномальности для нормальных и атакующих событий

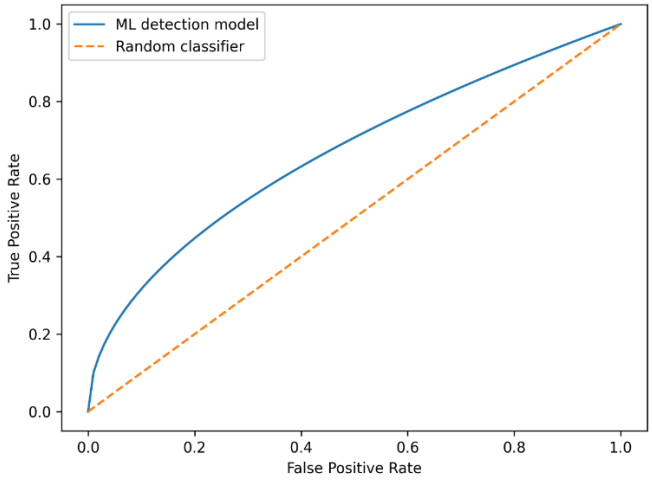

Рис. 4. ROC-кривая модели машинного обучения для обнаружения аномалий

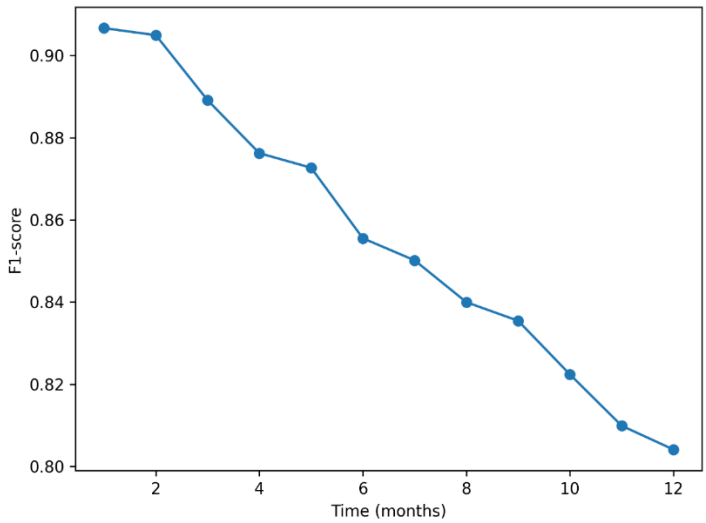

Рис. 5. Деградация качества ML-модели во времени без переобучения.
По оси Y отложена метрика качества детекции F1-score , по оси X отложены месяцы

4.8. Выводы по экспериментальной части

Экспериментальные результаты подтверждают эффективность предложенной архитектуры проактивного SOC с ИИ-интеграцией. Использование сетевой системы ML и

LLM позволяет повысить точность обнаружения инцидентов, снизить нагрузку на аналитиков и сократить время реагирования, что подтверждает целесообразность дальнейших исследований и практического внедрения предложенного подхода.

Заключение

В данной работе разработана и исследована концепция интеллектуальной системы проактивного мониторинга центров информационной безопасности SOC, основанной на интеграции традиционных SIEM-платформ, методов машинного обучения и больших языковых моделей. В отличие от существующих подходов, ориентированных преимущественно на реактивную обработку инцидентов, предложенная архитектура обеспечивает когнитивную поддержку аналитиков SOC и способствует переходу к проактивной модели обнаружения и интерпретации угроз.

В ходе исследования сформирована модульная архитектура системы, включающая уровни сбора и корреляции событий, ансамбль моделей обнаружения аномалий и интеллектуальный аналитический слой на основе большой языковой модели, функционирующей в режиме retrieval-augmented generation. Особое внимание уделено вопросам воспроизводимости и объяснимости решений, а также контролю рисков, связанных с применением искусственного интеллекта в критически важных процессах информационной безопасности.

Для экспериментальной оценки эффективности предложенного подхода разработан синтетический набор данных, имитирующий функционирование SOC и содержащий сценарии атак, соответствующие тактикам и техникам базы знаний MITRE ATT&CK. Проведённое сравнительное исследование показало, что интеграция машинного обучения и большой языковой модели позволяет снизить долю ложных срабатываний, сократить время обнаружения инцидентов и повысить интерпретируемость аналитических выводов по сравнению с традиционными SIEM-решениями.

Полученные результаты подтверждают целесообразность использования больших языковых моделей в качестве системного аналитического слоя SOC, способного агрегировать разнородные данные, формировать выводы и поддерживать принятие решений аналитиками. Предложенный подход может быть использован при проектировании и модернизации центров мониторинга информационной безопасности, а также в качестве основы для дальнейших научных исследований в области применения искусственного интеллекта в кибербезопасности.

5. Направления дальнейших исследований

Дальнейшее развитие представленного исследования целесообразно проводить по следующим направлениям:

1. Валидация на реальных данных.

Расширение экспериментальной базы за счёт применения предложенной архитектуры к реальным телеметрическим данным SOC с учётом требований конфиденциальности и анонимизации.

2. Адаптация и устойчивость моделей.

Исследование методов автоматической адаптации ML-моделей и LLM к дрейфу данных и изменяющимся тактикам атакующих, включая онлайн-обучение и калибровку неопределённости.

3. Формализация доверия и риска.

Разработка количественных моделей доверия к выводам LLM и формальных критериев допуска автоматических действий в контуре реагирования.

4. Расширение объяснимости.

Интеграция методов объяснимого искусственного интеллекта (XAI) для более детальной интерпретации результатов детекции и семантического анализа инцидентов.

5. Многоагентные и специализированные LLM.

Исследование применения специализированных и многоагентных языковых моделей для распределения функций анализа, корреляции и реагирования в SOC.

6. Оценка устойчивости к атакам на ИИ.

Анализ угроз, направленных на компрометацию ML- и LLM-компонентов (data poisoning, prompt-injection), и разработка механизмов защиты.

7. Интеграция с нормативными требованиями.

Исследование соответствия интеллектуальных SOC требованиям отраслевых стандартов и регуляторов, включая вопросы аудита и трассируемости решений.

Реализация указанных направлений позволит повысить практическую применимость интеллектуальных SOC и сформировать теоретическую основу для дальнейшего развития проактивных систем мониторинга информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ/REFERENCES:

1. Sommer R., Paxson V. Outside the closed world: On using machine learning for network intrusion detection. Proceedings of the IEEE Symposium on Security and Privacy. 2010, pp. 305-316. DOI: https://doi.org/10.1109/SP.2010.25.
2. Chandola V., Banerjee A., Kumar V. Anomaly detection: A survey. ACM Computing Surveys. 2009, v. 41, no. 3. DOI: https://doi.org/10.1145/1541880.1541882.
3. Garcia-Teodoro P., Diaz-Verdejo J., Macia-Fernandez G., Vazquez E. Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security. 2009, v. 28, no. 1–2, pp. 18-28. DOI: https://doi.org/10.1016/j.cose.2008.08.003.
4. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94. Gaithersburg: NIST, 2021. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf (accessed: 10.12.2025).
5. Clarke R. A., Knake R. K. Cyber War: The Next Threat to National Security and What to Do About It. – New York: Ecco, 2010. ISBN 978-0061962233.
6. Kim G., Lee S., Kim S. A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Systems with Applications. 2021, v. 168. DOI: https://doi.org/10.1016/j.eswa.2013.08.066.
7. Shone N., Ngoc T. N., Phai V. D., Shi Q. A deep learning approach to network intrusion detection. IEEE Transactions on Dependable and Secure Computing. 2020, v. 17, no. 2. DOI: https://doi.org/10.1109/TDSC.2017.2749224.
8. Zhang J., Chen M. Proactive SOC monitoring using AI-driven analytics. Computers & Security. 2022, v. 114. DOI: https://doi.org/10.1016/j.cose.2022.102776.
9. MITRE Corporation. MITRE ATT&CK®: Adversary Tactics, Techniques, and Common Knowledge. 2023. URL: https://attack.mitre.org (accessed:10.12.2025).
10. Brown T., Mann B., Ryder N. et al. Language models are few-shot learners. Advances in Neural Information Processing Systems (NeurIPS). 2020, v. 33, pp. 1877-1901. DOI: https://doi.org/10.48550/arXiv.2005.14165.
11. Xu H., Zhang Y., Li Z. Large language models for cybersecurity: A systematic literature review. ACM Computing Surveys. 2024. DOI: https://doi.org/10.13140/RG.2.2.10132.92800.
12. Nourmohammadzadeh Motlagh, Farzad & Meinel, Christoph & Cheng, Feng & Najafi, Pejman & Hajizadeh, Mehrdad & Majd, Mehryar. (2024). Large Language Models in Cybersecurity: State-of-the-Art. DOI: https://doi.org/10.48550/arXiv.2402.00891.
13. Yao Y., Li L., Zhang H. A survey on large language model security and privacy. IEEE Access. 2024, v. 12. DOI: https://doi.org/10.1016/j.hcc.2024.100211.
14. Charmet F., Tanuwidjaja H. Explainable artificial intelligence for cybersecurity. Cham: Springer, 2022. DOI: https://doi.org/10.1007/s12243-022-00926-7.
15. Лось, В.П. Методы интеллектуального анализа данных, применяемые в задаче обнаружения вторжений. В.П. Лось, Д.Д. Маланьин. Информация и безопасность. 2022, т. 25, № 4, с. 599-608. DOI: https://doi.org/10.36622/VSTU.2022.25.4.014. EDN: XCJJDE.
Los V.P., Malanin D.D. Methods of intelligent data analysis used in the intrusion detection. Informatsiya i Bezopasnost'. 2022, v. 25, no. 4, pp. 599-608. DOI: https://doi.org/10.36622/VSTU.2022.25.4.014. EDN: XCJJDE (in Russian).
16. Шогенов, Б.Р. Применение технологий анализа больших данных для повышения эффективности мониторинга безопасности информационных систем. Первый шаг в науку: материалы X Всероссийской научно-практической конференции: в двух томах, Луганск, 08 апреля 2025 года. Луганск: Федеральное государственное бюджетное образовательное учреждение высшего образования «Луганский государственный педагогический университет». 2025, с. 139-142. EDN: ZPSLYZ.

Shogenov B.R. Application of big data analysis technologies to improve the efficiency of information security monitoring systems. In: Pervyi shag v nauku: Proceedings of the 10th All-Russian Scientific and Practical Conference, Lugansk. April 8, 2025, pp. 139-142. EDN: ZPSLYZ (in Russian).

17. Котенко, И.В. Создание новых систем мониторинга и управления кибербезопасностью. И.В. Котенко, И.Б. Саенко. Вестник Российской академии наук. 2014, т. 84, № 11, с. 993-1001. DOI: https://doi.org/10.7868/S0869587314110073. EDN: SXWZNN.
Kotenko I.V., Saenko I.B. Creating new-generation cybersecurity monitoring and management systems. Vestnik Rossiiskoi Akademii Nauk, 2014, v. 84, no. 6, pp. 424-431. DOI: https://doi.org/10.1134/S1019331614060033. EDN: UFVKHV.
18. Корякина, Ю.С. Аналитический обзор подходов к реализации подсистем сбора, обработки, хранения и визуализации данных в рамках SOC (security operations center). Ю.С. Корякина, Ш.Т. Айтбаев, И.В. Зимин. Проблемы автоматики и управления. 2025, № 2(53), с. 29-40. EDN: CUPTAQ.
Koryakina Yu.S., Aitbaev Sh.T., Zimin I.V. Analytical review of methods for implementing subsystems for data collection, processing, storage and visualization for SOC (security operations center). Problemy avtomatiki i upravleniya, 2025, no. 2(53), pp. 29-40. EDN: CUPTAQ (in Russian).

Конфликт интересов. *Авторы заявляют об отсутствии конфликта интересов.*
Conflict of interest. *The authors declare no conflict of interest.*

Вклад авторов

Прохорец И.О.: *формулирование идеи, гипотезы, цели исследования, разработка методологии исследования, работа с программным обеспечением, статистический и теоретический анализ данных, проведение экспериментов, написание первоначального текста статьи, редактирование*

Шматок В.А.: *организационное управление проектом, создание графиков, схем, иллюстраций,*

Попов М.А.: *научное руководство проектом, управление данными: подготовка, аннотирование, хранение*

Author Contributions

Prokhorets I.O.: *Conceptualization methodology, software, validation, formal analysis, investigation, writing – Original Draft, writing – Review & Editing.*

Shmatok V.A.: *Data curation, visualization, project administration.*

Popov M.A.: *Supervision.*

ИНФОРМАЦИЯ ОБ АВТОРАХ:

Иван Олегович Прохорец, *старший инженер, Вычислительный центр Дальневосточного отделения Российской академии наук.*
e-mail: ivan0999@inbox.ru,
https://orcid.org/0009-0008-1141-108X,
SPIN-код: 2114-2959

Виталий Андреевич Шматок, *аспирант, Дальневосточный государственный университет путей сообщения.*
e-mail: vit.shmatok@gmail.com,
https://orcid.org/0009-0005-3439-7530

Михаил Александрович Попов, *к.т.н., доцент кафедры «Информационные технологии и системы», Дальневосточный государственный университет путей сообщения.*
e-mail: main79@mail.ru,
https://orcid.org/0009-0003-2841-5507

INFORMATION ABOUT THE AUTHORS:

Ivan Olegovich Prokhorets, *Senior engineer, Computing Center of the Far Eastern Branch of the Russian Academy of Sciences.*
e-mail: ivan0999@inbox.ru,
https://orcid.org/0009-0008-1141-108X,
SPIN-code: 2114-2959

Vitaly Andreevich Shmatok, *PhD student, Far Eastern State Transport University.*
e-mail: vit.shmatok@gmail.com,
https://orcid.org/0009-0005-3439-7530

Mikhail Aleksandrovich Popov, *PhD, Associate Professor of the Department of Information Technologies and Systems, Far Eastern State Transport University.*
e-mail: main79@mail.ru,
https://orcid.org/0009-0003-2841-5507

Статья поступила в редакцию 26.01.2026; одобрена после рецензирования 16.03.2026; принята к публикации 26.03.2026
The article was submitted 26.01.2026; approved after reviewing 16.03.2026; accepted for publication 26.03.2026