DOI: 10.24892/RIJIE/20260307

Автоматизированная система анализа слабоструктурированных данных киберразведки на основе графов знаний*

Луцкович А.И., Вульфин А.М., Кириллова А.Д., Кучкарова Н.В.
Уфимский университет науки и технологий
г. Уфа, Российская Федерация
vulfin.am@ugatu.su

Аннотация. **Рост числа кибератак и усложнение методов их реализации обуславливают необходимость совершенствования инструментов анализа данных киберразведки. В настоящей работе представлена архитектура и программная реализация GraphRAG-системы анализа слабоструктурированных данных киберразведки, интегрирующей национальный банк данных угроз безопасности информации ФСТЭК России с международными базами знаний MITRE ATT&CK, D3FEND, CVE, CWE и CAPEC в единый граф знаний BDU-CTI-KG. Система включает шесть функциональных подсистем: ETL-слой импорта гетерогенных данных, графовую систему управления базами данных Neo4j, векторное хранилище Qdrant с мультиязычными эмбеддингами BGE-M3, унифицированный LLM-слой с поддержкой облачных и локальных моделей, семиэтапный GraphRAG-конвейер обработки запросов и пользовательский интерфейс аналитика центра мониторинга информационной безопасности. Практическая апробация предложенного решения с системой анализа фишинговых ресурсов в условиях центра мониторинга информационной безопасности подтвердила повышение воспринимаемой полезности объяснений с 3,97 до 4,20 балла по пятибалльной шкале при высокой согласованности экспертных оценок (к Флейсса = 0,84, α Кронбаха = 0,96).**

Ключевые слова: **граф знаний, расширенная дополненная генерация, киберразведка, большие языковые модели, MITRE ATT&CK, БДУ ФСТЭК, Neo4j.**

Введение

В последние годы наметился резкий рост числа кибератак на государственные и коммерческие организации, усложнение характера этих атак и масштабов вызываемых ими последствий. По данным Центра мониторинга и реагирования на кибератаки RED Security SOC, общее число инцидентов информационной безопасности (ИБ) в российских компаниях в 2024 году выросло в 2,5 раза по сравнению с 2023 годом и достигло 130 тысяч [1]. Основную угрозу представляли хактивисты – политически мотивированные киберпреступники. Целями атак чаще всего становились объекты критической информационной инфраструктуры (КИИ) – 64% от общего числа инцидентов; наиболее часто атакуемые отрасли – промышленность, IT-компании, финансовый сектор. Число целенаправленных атак (APT) выросло за год на 60%. По прогнозам Positive Technologies [2], более половины кибератак в мире будет совершаться с использованием искусственного интеллекта (ИИ), а появление больших языковых моделей (LLM) ускоряет подготовку злоумышленников к атакам.

Выходом из этой ситуации является организация проактивной защиты, т.е. переход от обнаружения уже свершившихся угроз безопасности информации (УБИ) к их предупреждению. Активную роль играют методы киберразведки угроз (Cyber Threat Intelligence, CTI) – процесс сбора и анализа информации о существующих и потенциальных угрозах, хакерских группировках, способах реализации кибератак [3]. В качестве источников (фидов) используются открытые и коммерческие потоки данных, форумы, данные из DarkNet – как правило, это большие объемы слабоструктурированной информации, из которой специалисты ИБ извлекают индикаторы компрометации (IoC): IP-адреса, доменные имена, хеш-суммы, URL и т.д. [4].

Для обработки данных CTI все чаще привлекаются LLM [5-7], однако их применение сталкивается с ограничениями: генерация ложных утверждений, устаревшие данные и непрозрачность рассуждений [6, 8, 9]. Объяснимый ИИ (XAI) направлен на повышение прозрачности моделей, позволяя экспертам подтверждать аналитические выводы фактами из доменных знаний и доверять автоматизированным рекомендациям при реагировании на инциденты. Одним из подходов к преодолению указанных ограничений является технология RAG (Retrieval Augmented Generation) [10], расширяющая контекст запроса актуальной информацией из внешних источников. Развитием RAG стала концепция GraphRAG, при которой извлечение и генерация дополняются графами знаний (Knowledge Graphs, KGs), отображающими связи между сущностями предметной области. Подробный анализ преимуществ GraphRAG и нерешенных проблем в CTI приведен в [11].

Релевантные работы

Проблема автоматизации построения графов знаний в области ИБ обсуждается во многих публикациях [12, 13], показавших, что графовые модели позволяют визуализировать связи между данными CTI, атрибутировать атаки и прогнозировать угрозы. В [14] предложена двухэтапная процедура: LLM-построение триплетов (“субъект” – “отношение” – “объект”) с последующей верификацией онтологиями. Работа [15] исследует применение open-source LLM (Llama 2-Chat, Mistral 7B) для извлечения знаний из CTI-текстов с оценкой по метрикам ROUGE. В [16] разработан фреймворк KGV для оценки качества данных CTI на основе интеграции графов знаний и LLM.

* Статья публикуется по рекомендации программного комитета Всероссийской научно-практической конференции Индустрия 4.0", https://smartindustrycon.ru

В [17] представлена среда CyKG-RAG Framework, интегрирующая графы знаний и RAG: граф строится на основе локальных логов и внешних источников (CVE, CWE, CAPEC, MITRE ATT&CK), далее реализуется взаимодействие векторных вложений с узлами графа по метрике семантической близости. На основе GraphRAG развиваются проекты: LightRAG [18] (граф знаний с векторным поиском), fast-GraphRAG [19] (интерпретируемые поисковые процессы с управлением через агентов), HiRAG [20]. В [21] отмечается необходимость баланса между интерпретируемостью через XAI и защитой модели; одним из решений служат онтологические ограничения.

Графы знаний активно применяются для объяснимого анализа угроз. Современные графы кибератак включают узлы “тактики/техники ATT&CK”, “уязвимости CVE”, “индикаторы (IoC)” и “группы угроз”, обеспечивая семантический контекст для LLM [22]. Графы строятся двумя подходами: rule-based (RML-трансформация данных CVE, CWE, CAPEC) и LLM-based (извлечение из неструктурированных CTI-отчетов). Для стандартизации применяются онтологии (STIX, таксономии ATT&CK), обеспечивающие семантическую совместимость и априорные ограничения.

В [23] предложен фреймворк OntoLogX: LLM генерирует описания событий безопасности, определяемые онтологией, с проверкой валидности выхода – подход извлекает информацию из логов точнее, чем LLM со специализированным prompt. В [24] предложен KGV для оценки качества CTI-данных на наборе CTI-200 (1000 отчетов), показавший преимущество интегрированного подхода над изолированным применением LLM или графовых методов.

Анализ работ позволяет констатировать высокий уровень зрелости методов построения графов знаний CTI: CTIKG [25] – 91,89% Precision и 89,39% Recall, CTINexus [26] – адаптация к онтологиям без дообучения, LLM-TIKG [27, 28] – few-shot обучение для минимизации ручной разметки. Архитектурные решения GraphRAG (Microsoft GraphRAG, CyKG-RAG, GraphCyRAG) демонстрируют от 30% до 80% улучшения точности по сравнению с базовыми RAG-системами.

Вместе с тем существующие решения имеют ограничения [11]: ориентация на англоязычные источники без интеграции национальных баз знаний, недостаточная формализация межонтологических связей, фрагментарная проработка мультиязычного поиска. Значительны и вычислительные затраты на построение графов и генерацию суммаризаций. Указанные обстоятельства обуславливают необходимость разработки комплексной программной системы, реализующей предложенные в [11] алгоритмы и обеспечивающей практическую эксплуатацию GraphRAG-подхода в условиях центров мониторинга ИБ.

Проектирование и разработка GraphRAG-системы анализа данных CTI

Описывается архитектура мультиязычной (русский и английский) GraphRAG-системы, объединяющей: БДУ ФСТЭК (угрозы, объекты, компоненты, меры, последствия), MITRE ATT&CK (домены Enterprise, ICS, Cloud) и D3FEND, корпус CTI-отчетов [29], уязвимости CVE, CWE, CAPEC [30]. Целью является формирование единого графа знаний BDU-CTI-KG (Baza Dannih Ugroz-Cyber Threat Intelligence-Knowledge Graph), поверх которого реализуется GraphRAG-конвейер с поддержкой локальных и облачных LLM и эмбеддинговым бэкендом BGE-M3. В отличие от классического RAG, где контекст формируется из фрагментов документов, система приоритизирует графовые факты БДУ и использует текстовые доказательства как дополнительный слой обоснования.

Система сочетает несколько направлений: знание-ориентированное извлечение CTI-фактов (KnowCTI [31]), построение графов атак (AttacKG [32], AttacKG+ [33]), GraphRAG-retrieval [34], мультиязычные эмбеддинги BGE-M3 [35] (поддержка более 100 языков, SOTA в кросс-язычном поиске) и систематическую оценку качества RAG (RAGAS [36]).

Архитектура (рис. 1) включает шесть функциональных подсистем, взаимодействующих в рамках единого GraphRAG-конвейера.

1. Подсистема источников данных интегрирует три категории ресурсов: структурированные базы знаний (БДУ ФСТЭК, MITRE ATT&CK, D3FEND, CVE/CWE/CAPEC), слабоструктурированные данные (CTI-отчеты в форматах PDF и текстовых документов, события и IoC из MISP, STIX-объекты из OpenCTI) и артефакты GraphRAG (иерархические сообщества и резюме).

2. ETL-слой реализует извлечение, преобразование и загрузку данных через шесть специализированных модулей: импорта БДУ (парсинг XML), ATT&CK (формат STIX), D3FEND (OWL-онтология), CVE2CAPEC (уязвимости), обработки CTI (извлечение текста, чанкинг, построение эмбеддингов) и интеграции с CTI-платформами (MISP, OpenCTI через API-коннекторы).

3. Подсистема хранения построена на графовой СУБД Neo4j (единый граф BDU-CTI-KG, объединяющий узлы типов BduThreat, BduObject, BduComponent, BduControl, BduConsequence, AttackTactic, AttackTechnique, AttackGroup, AttackSoftware, AttackMitigation, D3fendTechnique, DigitalArtifact, CVE, CWE, CAPEC, CTIReport, CTIChunk, GraphCommunity, GraphSummaryNode) и векторном хранилище Qdrant с четырьмя коллекциями эмбеддингов: kg_nodes, descriptions, cti_chunks, graph_summaries. Для построения эмбеддингов используется мультиязычная модель BGE-M3 с поддержкой комбинированного плотного, лексического и многовекторного поиска.

4. LLM-слой обеспечивает унифицированный доступ к языковым моделям через абстрактный клиент: облачные модели OpenAI API (GPT-4o) для высококачественной генерации и локальные модели (Gemma3:27B [37]) через Ollama [38] для автономной работы без передачи данных во внешние сервисы.

5. GraphRAG-конвейер реализует цепочку обработки CTI-запросов: извлечение CTI-сущностей (LLM в режиме JSON-генерации), построение контекста (сопоставление с узлами графа, обход на глубину до двух переходов, векторный поиск в Qdrant), генерацию ответа и логирование.

6. Пользовательский интерфейс предоставляет аналитику SOC возможность формулировать запросы на естественном языке и получать контекстуализированные ответы с указанием источников.

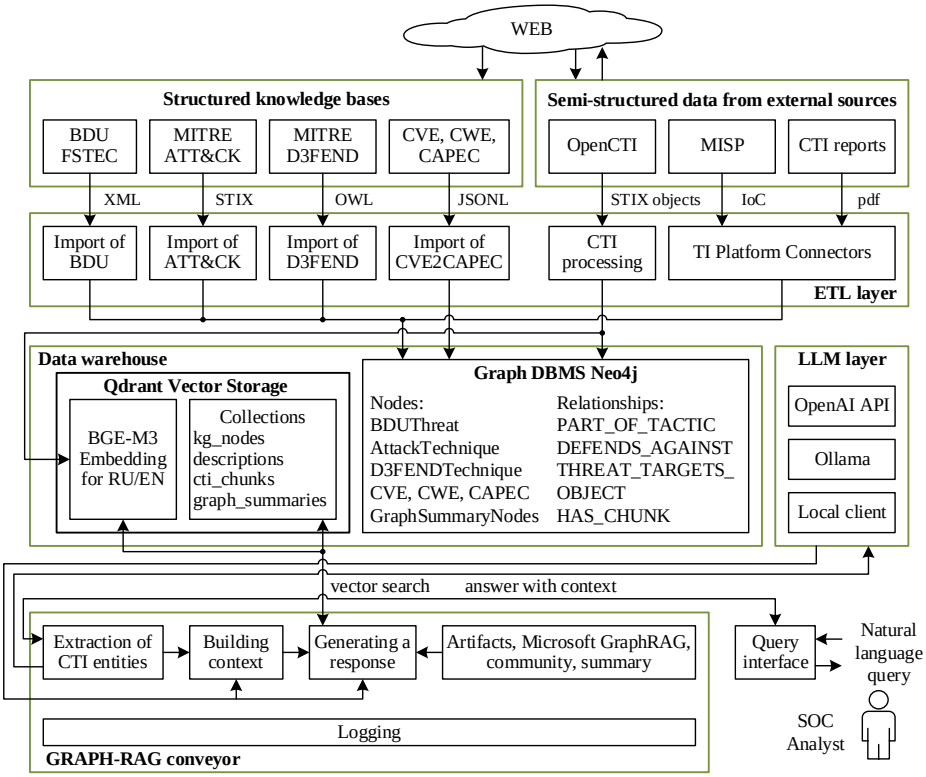

Рис. 1. Архитектура разработанной системы

Программная реализация организована в четыре подсистемы (ingestion, vector, rag, graph), образующие направленный ациклический граф зависимостей. Архитектура обеспечивает независимое развитие компонентов, добавление новых источников и замену LLM-бэкенда. Конвейер может работать полностью локально или в гибридном режиме с использованием облачных API.

Онтологическая модель BDU-CTI-KG, детально описанная в [11], объединяет шесть предметных доменов: БДУ ФСТЭК (угрозы, объекты, компоненты, меры, последствия), MITRE ATT&CK (тактики, техники, группы, ПО), MITRE D3FEND (защитные техники, артефакты), CVE/CWE/CAPEC, CTI-документы и GraphRAG (иерархические сообщества и резюме). Физическая схема (рис. 2) реализована в Neo4j в виде размеченного графа свойств и включает 30 типов узлов и 23 типа связей.

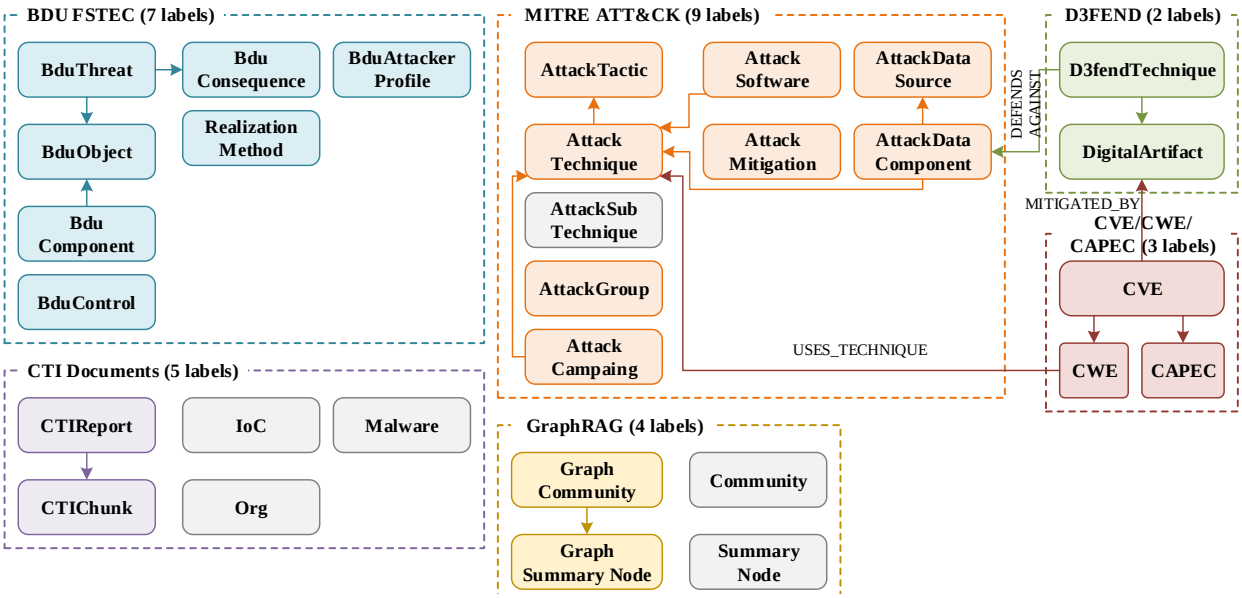

Рис. 2. Физическая схема графа знаний BDU-CTI-KG

Межонтологические связи между доменами (БДУ–ATT&CK–D3FEND) строятся алгоритмом верифицируемого межонтологического выравнивания [11], реализующим трехэтапную процедуру: генерацию кандидатов по векторному сходству, проверку доменными ограничениями и ограниченную LLM-верификацию. В системе предусмотрены два варианта построения связей: M_1 (экспертные таблицы соответствий) и M_2 (автоматизированное выравнивание с LLM-верификацией).

Конвейер обработки запросов реализует гибридный подход, объединяющий графовый поиск в Neo4j с векторным поиском в Qdrant. Обработка запроса аналитика SOC выполняется в семь последовательных этапов (рис. 3).

На первом этапе модуль extraction идентифицирует в тексте запроса сущности: идентификаторы CVE, техники ATT&CK (по коду и описанию), защитные техники D3FEND, фразы, соответствующие угрозам БДУ, и IoC. На втором этапе извлеченные фрагменты преобразуются в эмбеддинги для поиска семантически близких узлов графа по коллекциям kg_nodes и descriptions с фильтрацией по типам (AttackTechnique, D3fendTechnique, BduThreat). Третий этап расширяет подграф в Neo4j: точное сопоставление с узлами и извлечение окрестности на глубину до двух переходов с фильтрацией по разрешенному списку типов.

Четвертый и пятый этапы обогащают контекст иерархическими резюме сообществ GraphRAG (агрегированные резюме тематических кластеров) и преобразуют подграф в структурированный формат: триплеты, свойства узлов и текстовые карточки с механизмом отсечения (приоритет – узлам БДУ как наиболее релевантным для российского нормативного контекста). На шестом этапе формируется запрос к LLM (облачной или локальной) с температурой 0,2. Седьмой этап обеспечивает формирование ответа с метаданными и протоколирование в формате JSONL.

Ключевые достоинства: (1) интеграция национального (БДУ ФСТЭК) и международного (ATT&CK, D3FEND) знания; (2) мультиязычность на основе моделей BGE-M3 и Gemma3:27B; (3) графо-ориентированный RAG со структурным обходом по шаблонам “Угроза – Объекты – Компоненты – Меры – Последствия” и “ATT&CK – D3FEND – CVE”, снижающий галлюцинации и повышающий интерпретируемость за счет трассировки фактов; (4) гибридный LLM-бэкенд (облако/локальный).

Основные ограничения: неполная экспертная валидация ребер БДУ и DEFENDS_AGAINST в D3FEND; необходимость дополнительной валидации интеграции GraphRAG-community; сложная многоуровневая архитектура, усложняющая воспроизводимость и требующая отдельной инфраструктуры.

Оценка эффективности предложенной системы

В ходе внедрения прототипа в SOC проведен эксперимент по оценке влияния интеграции GraphRAG-системы на воспринимаемую полезность объяснений результатов классификации фишинговых веб-ресурсов.

Для оценки было случайно отобрано 30 уникальных URL, по каждому из которых система формировала текстовое объяснение с указанием ключевых признаков классификации. Три действующих SOC-аналитика первой линии оценивали ответ по пятибалльной шкале полезности: 1 – бесполезно; 2 – почти не помогает; 3 – скорее полезно, но требует доработок; 4 – полезно для принятия решения; 5 – полностью покрывает потребности аналитика.

Эксперимент проводился в два этапа. На первом этапе эксперты оценивали объяснения в базовом режиме (без GraphRAG). На втором этапе для тех же 30 URL объяснения генерировались с использованием GraphRAG-контекста: система дополняла вывод ссылками на техники фишинга по матрице MITRE ATT&CK, примерами схожих кампаний и рекомендациями по мерам защиты. Средняя оценка полезности возросла с 3,97 (базовый режим) до 4,20 (режим с GraphRAG). Распределение оценок (табл. 1) сместилось в сторону высоких значений: доля оценок 5 баллов увеличилась с 12 до 27, оценки 1 и 2 балла полностью исчезли.

Таблица 1

Распределение оценок для двух сценариев

Параметр	Без RAG	С RAG
Распределение	2 б.–3; 3 б.–9; 4 б.–66; 5 б.–12	2 б.–0; 3 б.–9; 4 б.–54; 5 б.–27
Средний балл	3,97	4,20
к Флейсса	0,82	0,84
α Кронбаха	0,90	0,96

Подключение GraphRAG-системы не только повышает средний балл полезности объяснений, но и делает оценки экспертов более однородными.

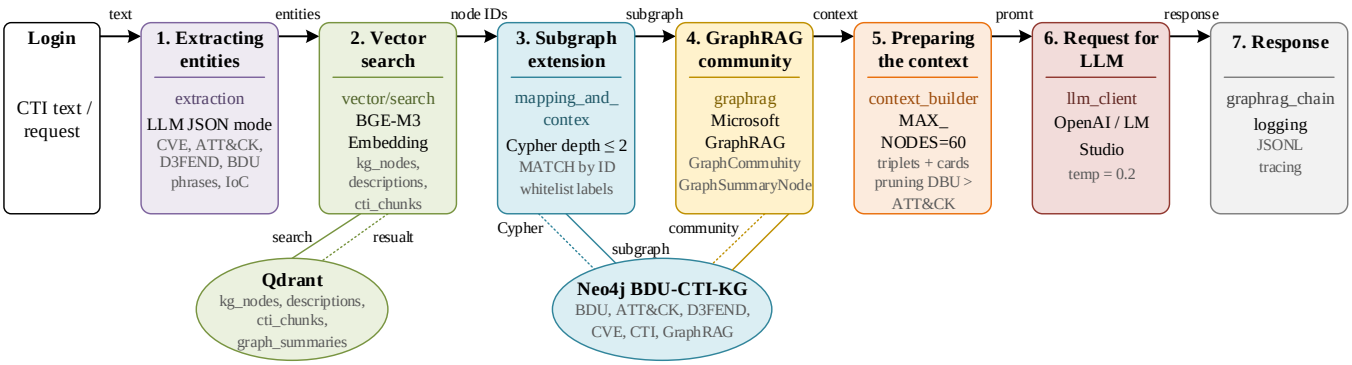

Рис. 3. Схема GraphRAG-конвейера обработки запросов CTI

Анализ результатов и перспективные направления

Проведенные эксперименты подтверждают эффективность предложенной GraphRAG-системы. Переход от текстового к гибридному GraphRAG принципиально повышает полноту и проверяемость ответов. Автоматизированное построение связей (M2) показало результаты, отличающиеся от экспертных менее чем на 10%, что свидетельствует о практической применимости в условиях ограниченных ресурсов на разметку. Интеграция с системой анализа фишинговых ресурсов подтвердила повышение полезности объяснений (с 3,97 до 4,20) при высокой согласованности оценок (κ Флейсса = 0,84, α Кронбаха = 0,96).

Факторы, ограничивающие обобщаемость: экспертная оценка проводилась тремя специалистами одной организации; использовалась единственная локальная модель Gemma3:27B; межонтологические связи БДУ–ATT&CK прошли лишь частичную валидацию.

Перспективные направления развития: (1) автоматизация построения графов атак на основе CVE; (2) оптимизация вычислительных затрат через подходы LightRAG и LazyGraphRAG (модели с 3-8 млрд параметров при настройке достигают результатов, сопоставимых с крупными); (3) интеграция темпоральных аспектов (ChronoCTI [39]) для моделирования эволюции угроз; (4) создание агентных систем [40, 41], способных автономно инициировать запросы к внешним источникам при обнаружении подозрительных индикаторов. По прогнозам Gartner [42], к 2027 году агентные системы на основе ИИ будут участвовать в автоматизации более половины бизнес-решений в области кибербезопасности.

Заключение

В настоящей работе представлена архитектура и программная реализация GraphRAG-системы анализа слабоструктурированных данных киберразведки, интегрирующей национальный банк данных угроз ФСТЭК России с международными базами знаний MITRE ATT&CK, D3FEND, CVE, CWE и CAPEC в единый граф знаний BDU-CTI-KG.

Разработана модульная программная архитектура, включающая шесть функциональных подсистем: источники данных, ETL-слой с шестью модулями импорта, двухкомпонентное хранилище (Neo4j + Qdrant), унифицированный LLM-слой с поддержкой облачных и локальных моделей, семиэтапный GraphRAG-конвейер обработки запросов и пользовательский интерфейс аналитика SOC. Архитектура обеспечивает независимое развитие компонентов и работу в полностью локальном или гибридном режиме.

Интеграция с системой анализа фишинговых ресурсов в условиях центра мониторинга информационной безопасности подтвердила повышение воспринимаемой полезности объяснений с 3,97 до 4,20 балла по пятибалльной экспертной шкале при высокой согласованности оценок (κ Флейсса = 0,84, α Кронбаха = 0,96).

К ограничениям работы относятся неполная экспертная валидация межонтологических связей БДУ-ATT&CK и ограниченный объем экспертной выборки. Дальнейшие исследования предполагают автоматизацию построения графов атак, оптимизацию вычислительных затрат, интеграцию темпоральных аспектов и разработку агентных систем проактивного обнаружения угроз.

Предложенная система может применяться для поддержки принятия решений аналитиками SOC при разборе CTI-отчетов, формировании рекомендаций по мерам защиты и атрибуции инцидентов.

Литература

1. Число кибератак в России и мире. TAdviser. – URL: https://www.tadviser.ru/ (дата обращения 13.01.2026).
2. Резников Р. Positive Technologies: хакеры способны использовать ИИ более чем в половине техник кибератак. – URL: https://ptsecurity.com/ru-ru/about/news/positive-technologies-hakery-sposobny-ispolzovat-ii-bolee-chem-v-polovine-tehnik-kiberatak/ (дата обращения 13.01.2026).
3. Сдобникова И. Threat Intelligence: как опередить атакующих и защитить компанию с помощью киберразведки. – URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Threat-Intelligence-AMLive-2025 (дата обращения 13.01.2026).
4. Мещеряков Р.В. Исследование индикаторов компрометации для средств защиты информационных и киберфизических систем / Р.В. Мещеряков, С.Ю. Исхаков // Вопросы кибербезопасности. – 2022. – № 5. – С. 82-99.
5. Alturkistani H. Artificial Intelligence and Large Language Models in Advancing Cyber Threat Intelligence: A Systematic Literature Review / H. Alturkistani, S. Chuprat. – URL: https://assets-eu.researchsquare.com/files/rs-5423193/v1/0ff16810-f9d8-488d-92dc-e4d8bed0052f.pdf?c=1734046706 (дата обращения 13.01.2026).
6. Котенко И.В. Использование больших языковых моделей для поиска угроз кибербезопасности на основе методов глубокого обучения: анализ современных исследований / И.В. Котенко, Г.Т. Абраменко // Правовая информатика. – 2024. – № 3. – С. 32-42.
7. Clarioux-Trepanier V. The Use of Large Language Models (LLM) for Cyber Threat Intelligence (CTI) in Cybercrime Forums / V. Clairoux-Trepanier, I.M. Beauchamp, E. Ruellan, M. Paquet-Clouston, S.O. Paquette, E. Clay // arXiv:2408.03354v3. – DOI: 10.48550/arXiv.2408.03354.
8. Würsch M. LLM-based entity extraction is not for cybersecurity / M. Würsch, A. Kucharavy, D. Percia David, A. Mermoud // Extraction and Evaluation of Knowledge Entities from Scientific Documents (EEKE2023). – 2023. – Vol. 3451. – P. 26-32.
9. Поляков С.В. Проблема когнитивной непрозрачности искусственного интеллекта как фактор риска в условиях цифровой трансформации // Искусственный интеллект и духовная культура: сб. тр. Междунар. науч.-практ. конф. – СПб.: Сциентиа, 2025. – С. 94-97.
10. Lewis P. Retrieval-augmented generation for knowledge-intensive NLP tasks / P. Lewis, E. Perez, A. Piktus, F. Petroni, V. Karpukhin, N. Goyal, D. Kiela // Advances in Neural Information Processing Systems. – 2020. – Vol. 33. – P. 9459-9474.
11. Луцкович А.И. Автоматизированная система анализа слабоструктурированных данных киберразведки с использованием больших языковых моделей / А.И. Луцкович, В.И. Васильев, А.М. Вульфин, А.Д. Кириллова, А.Е. Сулавко // Информационно-управляющие системы. – 2025. – № 2(135). – С. 50-67. – DOI: 10.31799/1684-8853-2025-2-50-67.

12. Манжосов А.В. Метод автоматизированного построения графа знаний связности формальных моделей норм и требований в области информационной безопасности / А.В. Манжосов, И.П. Болодурина // Вестник УрФО. Безопасность в информационной сфере. – 2022. – № 2 (44). – С. 49-56.

13. Sikos L.F. Cybersecurity knowledge graphs // Knowledge and Information Systems. – 2023. – Vol. 65, no. 9. – P. 3511-3531.

14. Chepurova A. Prompt Me One More Time: A Two-Step Knowledge Extraction Pipeline with Ontology-Based Verification / A. Chepurova, Y. Kuratov, A. Bulatov, M. Burtsev // Proceedings of TextGraphs-17. – 2024. – P. 61-77.

15. Fieblinger R. Actionable cyber threat intelligence using knowledge graphs and large language models / R. Fieblinger, M.T. Alam, N. Rastogi // 2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). – IEEE, 2024. – P. 100-111.

16. Wu Z. KGV: Integrating large language models with knowledge graphs for cyber threat intelligence credibility assessment / Z. Wu, F. Tang, M. Zhao, Y. Li // arXiv preprint arXiv:2408.08088v1. – 2024. – DOI: 10.48550/arXiv.2408.08088.

17. Kurniawan K. CyKG-RAG: Towards knowledge-graph enhanced retrieval augmented generation for cybersecurity / K. Kurniawan, E. Kiesling, A. Ekelhart // CEUR Workshop Proceedings (CEUR-WS.org), vol-3950, ISWC, November 2024, Baltimore, USA.

18. Guo Z. LightRAG: Simple and fast retrieval-augmented generation / Z. Guo, L. Xia, Y. Yu, T. Ao, C. Huang // arXiv preprint arXiv:2410.05779. – 2024.

19. Zhao Y. GraphRAG: Streamlining Graph-based RAG for High Efficiency and Effectiveness / Y. Zhao, J Zhu, Y. Guo, K. He, X. Li // arXiv preprint arXiv:2505.24226. – 2025.

20. Jiao Y.H. HiRAG: Hierarchical-thought instruction-tuning retrieval-augmented generation / Y.H. Jiao, Z.H. Tan, D. Yang, D.L. Sun, J. Feng, Y. Shen, J. Wang, P. Wei // arXiv preprint arXiv:2507.05714. – 2025. – DOI: 10.48550/arXiv.2507.05714.

21. Oriaro S. Improving cybersecurity through explainable artificial intelligence: a systematic literature review / S. Oriaro, S. Mishra // Issues in Information Systems. – 2025. – Vol. 26. – No. 3.

22. F6 (Group-IB). Графовый анализ кибератак. – URL: https://www.f6.ru/media-center/press-releases/graph/ (дата обращения 13.01.2026).

23. Cotti L. Enabling Transparent Cyber Threat Intelligence Combining Large Language Models and Domain Ontologies / L. Cotti, A. Rula, D. Bianchini, F. Cerutti // arXiv preprint arXiv:2509.00081. – 2025.

24. Boylan J. KGValidator: a framework for automatic validation of knowledge graph construction / J. Boylan, S. Mangla, D. Thorn, D.G. Ghalandari, P. Ghaffari, C. Hokamp // arXiv preprint arXiv:2404.15923. – 2024.

25. Huang L. CTIKG: LLM-powered knowledge graph construction from cyber threat intelligence / L. Huang, X. Xiao // First Conference on Language Modeling. – 2024.

26. Cheng Y. CTINexus: Automatic cyber threat intelligence knowledge graph construction using large language models / Y. Cheng, O. Bajaber, S.A. Tsegai, D. Song, P. Gao // 2025 IEEE 10th European Symposium on Security and Privacy (EuroS&P). – IEEE, 2025. – P. 923-938.

27. Hu Y. LLM-TIKG: Threat intelligence knowledge graph construction utilizing large language model / Y. Hu, F. Zou, J. Han, X. Sun, Y. Wang // Computers & Security. – 2024. – Vol. 145. – Art. 103999.

28. Balasubramanian P. Generative AI for cyber threat intelligence: applications, challenges, and analysis of real-world case studies / P. Balasubramanian, S. Liyana, H. Sankaran, S. Sivaramakrishnan, S. Pusuluri, S. Pirttikangas, E. Peltonen // Artificial Intelligence Review. – 2025. – Vol. 58, no. 11. – P. 1-134.

29. CTI-reports-dataset. – URL: https://github.com/nlpai-lab/CTI-reports-dataset (дата обращения 13.01.2026).

30. CVE2CAPEC. – URL: https://github.com/Galeax/CVE2CAPEC (дата обращения 13.01.2026).

31. Wang G. KnowCTI: Knowledge-based cyber threat intelligence entity and relation extraction / G. Wang, P. Liu, J. Huang, H. Bin, X. Wang, H. Zhu // Computers & Security. – 2024. – Vol. 141. – Art. 103824.

32. Li Z. AttacKG: Constructing technique knowledge graph from cyber threat intelligence reports / Z. Li, J. Zeng, Y. Chen, Z. Liang // European Symposium on Research in Computer Security. – Cham: Springer, 2022. – P. 589-609.

33. Zhang Y. AttacKG+: Boosting attack knowledge graph construction with large language models / Y. Zhang, T. Du, Y. Ma, X. Wang, Y. Xie, G. Yang, Y. Lu, E.C. Chang // arXiv preprint arXiv:2405.04753. – 2024.

34. Edge D. et al. From local to global: A graph RAG approach to query-focused summarization // arXiv preprint arXiv:2404.16130v2. – 2025. – DOI: 10.48550/arXiv.2404.16130.

35. Chen J. BGE M3-embedding: Multi-lingual, multi-functionality, multi-granularity text embeddings through self-knowledge distillation / J. Chen, S. Xiao, P. Zhang, K. Luo, D. Lian, Z. Liu // arXiv preprint arXiv:2402.03216. – 2024.

36. Es S. RAGAS: Automated evaluation of retrieval augmented generation / S. Es, J. James, L.E. Anke, S. Schockaert // Proceedings of the 18th Conference of the European Chapter of the Association for Computational Linguistics: System Demonstrations. – 2024. – P. 150-158.

37. Team G. et al. Gemma 3 technical report // arXiv preprint arXiv:2503.19786. – 2025.

38. Ollama. – URL: https://ollama.com/ (дата обращения 13.01.2026).

39. Rahman M.R. ChronoCTI: Mining Knowledge Graph of Temporal Relations Among Cyberattack Actions / M.R. Rahman, B. Wroblewski, Q. Matthews, B. Morgan, T. Menzies, L. Williams // 2024 IEEE International Conference on Data Mining (ICDM). – IEEE, 2024. – P. 420-429.

40. Liu Z. AutoBnB-RAG: Enhancing Multi-Agent Incident Response with Retrieval-Augmented Generation / Z. Liu, A. Anwar // arXiv preprint arXiv:2508.13118. – 2025.

41. Cotti L. OntoLogX: Ontology-Guided Knowledge Graph Extraction from Cybersecurity Logs with Large Language Models / L. Cotti, I. Drago, A. Rula, D. Bianchini, F. Cerutti // arXiv preprint arXiv:2510.01409. – 2025.

42. Gartner Predicts Over 40 Percent of Agentic AI Projects Will Be Canceled by End of 2027. – URL: https://www.gartner.com/en/newsroom/press-releases/2025-06-25-gartner-predicts-over-40-percent-of-agentic-ai-projects-will-be-canceled-by-end-of-2027 (дата обращения 13.01.2026).

DOI: 10.24892/RIJIE/20260307

Automated System for Analyzing Semi-structured Cyber threat Intelligence Data Based on Knowledge Graphs

Lutskovich A.I., Vulfin A.M., Kirillova A.D., Kuchkarova N.V.
Ufa University of Science and Technology
Ufa, Russian Federation
vulfin.am@ugatu.su

Abstract. **The growing number of cyber attacks and the increasing complexity of their implementation methods necessitate the improvement of cyber threat intelligence data analysis tools. This paper presents the architecture and software implementation of the GraphRAG system for analyzing semi-structured cyber threat intelligence data, which integrates the national database of information security threats of the FSTEC of Russia with the international knowledge bases MITRE ATT&CK, D3FEND, CVE, CWE and CAPEC into a single knowledge graph BDU-CTI-KG. The system includes six functional subsystems: an ETL layer for importing heterogeneous data, a Neo4j graph database management system, a Qdrant vector storage with BGE-M3 multilingual embeddings, a unified LLM layer with support for cloud and local models, a seven-stage GraphRAG query processing pipeline, and a user interface for an analyst of the security operations center. Practical testing of the proposed solution with a system for analyzing phishing resources in the conditions of the security operations center confirmed an increase in the perceived usefulness of explanations from 3.97 to 4.20 points on a five-point scale with high agreement between expert assessments (Fleiss κ = 0.84, Cronbach's α = 0.96).**

Keywords: **knowledge graph, retrieval augmented generation, cyber threat intelligence, large language models, MITRE ATT&CK, BDU FSTEC, Neo4j.**

Библиографическое описание статьи

Луцкович А.И. Автоматизированная система анализа слабоструктурированных данных киберразведки на основе графов знаний / А.И. Луцкович, А.М. Вульфин, А.Д. Кириллова, Н.В. Кучкарова // Машиностроение: сетевой электронный научный журнал. – 2026. – Т.13, №3. – С. 42-48. DOI: 10.24892/RIJIE/20260307

Reference to article

Lutskovich A.I., Vulfin A.M., Kirillova A.D., Kuchkarova N.V. Automated system for analyzing semi-structured cyber threat intelligence data based on knowledge graphs, *Russian Internet Journal of Industrial Engineering*, 2026, vol.13, no.3, pp. 42-48. DOI: 10.24892/RIJIE/20260307