УДК 004.056.53
doi:10.31799/1684-8853-2026-5-37-55
EDN: IULELD

Научные статьи
Articles

Модель и алгоритмы анализа данных киберразведки на основе графа знаний

А. М. Вульфин[a], *доктор техн. наук, профессор, orcid.org/0000-0001-5857-2413, vulfin.alexey@yandex.ru*
В. И. Васильев[a], *доктор техн. наук, профессор, orcid.org/0000-0002-6105-5481*
А. И. Луцкович[a], *старший преподаватель, orcid.org/0009-0000-7257-6947*
А. Д. Кириллова[a], *канд. техн. наук, доцент, orcid.org/0009-0000-4164-2526*
[a] *Уфимский университет науки и технологий, К. Маркса ул., 12, Уфа, 450008, РФ*

Введение: *традиционные системы генерации ответов с расширенным поиском, основанные на векторном поиске по текстовым фрагментам, ограниченно эффективны при многошаговом сопоставлении отчетов киберразведки, национальных классификаторов угроз и международных баз знаний.* ***Цель:*** *разработать и экспериментально оценить модель графа знаний, алгоритмов межонтологического выравнивания и двухконтурного извлечения контекста в ходе анализа данных киберразведки.* ***Методы:*** *модель реализована как ориентированный типизированный граф свойств с набором атрибутов, объединяющий национальный банк данных угроз, международные базы знаний о тактиках и техниках атак, защитных мерах, реестры уязвимостей, классификаторы слабостей программного обеспечения, каталоги шаблонов атак и корпус отчетов киберразведки. Достижение цели оценивается количественными метриками при построении межонтологических связей и анализе возможностей вопросно-ответной системы.* ***Результаты:*** *разработан алгоритм построения межонтологических связей с проверкой по семантическому сходству, доменным ограничениям и выравниванием с контролем корректности с помощью больших языковых моделей. Реализован двухконтурный алгоритм извлечения контекста, объединяющий граф знаний и доказательный слой текстовых фрагментов. Предложен метод анализа данных киберразведки на основе модели графа знаний, алгоритмов построения межонтологических связей и извлечения контекста. На тестовой выборке обучаемый классификатор межонтологических связей достиг значения метрики F_1 = 0,83. Вводимые экспертные связи повысили значение метрики EM полного совпадения предсказанного и эталонного множества идентификаторов с 0,34 до 0,63, автоматические связи обеспечили значение метрики EM = 0,56. Получен значимый прирост значения метрики Entity Recall@50 относительно текстового поиска – 0,5225, и после сокрытия идентификаторов тактик и техник прирост составил 0,5467.* ***Практическая значимость:*** *метод предназначен для поддержки принятия решений аналитиками центра мониторинга информационной безопасности при сопоставлении отчетов киберразведки с национальными и международными базами знаний.* ***Обсуждение:*** *межонтологические связи повышают проверяемость ответа за счет выравнивания с контролем корректности, а слой сводных описаний сообществ графа увеличивает согласованность ответа с извлеченным контекстом при умеренном снижении точности.*

Ключевые слова *— граф знаний, графовая генерация с расширенным поиском, данные киберразведки, тактики и техники, сопоставление онтологий, выравнивание сущностей, большие языковые модели, MITRE ATT & CK, MITRE D3FEND, БДУ ФСТЭК.*

Для цитирования: Вульфин А. М., Васильев В. И., Луцкович А. И., Кириллова А. Д. Модель и алгоритмы анализа данных киберразведки на основе графа знаний. *Информационно-управляющие системы*, 2026, № 5, с. 37–55. doi:10.31799/1684-8853-2026-5-37-55, EDN: IULELD

For citation: Vulfin A. M., Vasilyev V. I., Lutskovich A. I., Kirillova A. D. A model and algorithms for cyber threat intelligence data analysis based on a knowledge graph. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 5, pp. 37–55 (In Russian). doi:10.31799/1684-8853-2026-5-37-55, EDN: IULELD

Введение

Действенную роль в реализации проактивной защиты информационных систем играют методы анализа данных отчетов киберразведки (Cyber Threat Intelligence, CTI) о тактиках, техниках и процедурах (Tactics, Techniques and Procedures, TTP), применяемых злоумышленниками в ходе реализации компьютерных атак [1]. CTI-отчеты обычно представляют собой аналитические или технические документы, содержащие сведения о действиях злоумышленников, применяемом вредоносном программном обеспечении, инфраструктуре атак, индикаторах компрометации и мерах противодействия. Извлечение полезной (структурированной) информации из указанных «сырых» данных в форме некоторых признаков — индикаторов компрометации (Indicators of Compromise, IoC) — является актуальной задачей [2]. IoC рассматриваются как формализуемые признаки инцидента информационной безопасности (ИБ), например сетевые адреса, домены, хеш-суммы файлов, адреса электронной почты и другие наблюдаемые артефакты.

Для решения задач обработки данных CTI-отчетов о TTP злоумышленников все чаще применяются методы искусственного интеллекта, связанные с использованием больших языковых моделей (Large Language Models, LLM) [3, 4]. На практике применение LLM для анализа данных TTP может сталкиваться с рядом ограничений [4, 5]:

— LLM дает ложные сведения, если не знает правильного ответа («галлюцинации»);

— сообщает пользователю устаревшую информацию, в то время как от нее ждут актуальных данных;

— неправильно или неточно обрабатывает запрос из-за нарушения терминологии.

Одним из подходов к уменьшению числа необоснованных ответов LLM является генерация с расширенным поиском (Retrieval-Augmented Generation, RAG) [6]. В RAG-системе перед генерацией ответа выполняется извлечение релевантных фрагментов из внешнего хранилища знаний, далее эти фрагменты передаются в генеративную модель как контекст. Архитектура RAG-системы в общем виде включает модуль извлечения контекста (retriever) и модуль генерации ответа (generator). Примеры применения RAG-систем в задачах обработки слабоструктурированных данных в домене ИБ приводятся в публикациях (см., например, [7, 8]), а также в работе авторов [9].

В то же время, как отмечается, например, в [9], стандартный RAG также не лишен определенных недостатков, таких как:

— потеря контекста (при увеличении фрагментов информации может быть потеряна важная взаимосвязь между ними, что приводит к неполным или неточным ответам);

— сложность работы с многошаговыми вопросами (в случаях, когда требуется объединение информации из нескольких источников или выполнение логических выводов);

— неэффективность при работе с неструктурированными данными (извлечение релевантной информации из неструктурированных данных может быть сложным и неточным).

Для преодоления указанных ограничений развивается направление GraphRAG — графовая генерация ответов с расширенным поиском, при которой извлечение контекста опирается на граф сущностей и отношений. Граф знаний в настоящей работе рассматривается как ориентированный типизированный граф с заданием атрибутов, позволяющий явно представлять угрозы, тактики и техники атак, уязвимости, меры защиты и доказательные фрагменты CTI-отчетов. Графовое представление может повысить связность контекста и обеспечить прослеживаемость использованных фактов, однако эффект зависит от качества исходных данных, формируемых междоменных связей и правил извлечения [10, 11]. Анализ современного состояния исследований позволяет выделить следующие нерешенные проблемы.

Во-первых, существующие GraphRAG-системы для анализа данных CTI-отчетов ориентированы преимущественно на англоязычные источники и международные базы знаний. Интеграция национальных баз знаний, в частности банка данных угроз безопасности информации (БДУ) ФСТЭК России, в графовые структуры RAG-систем исследована недостаточно. Это ограничивает применимость существующих решений для организаций, деятельность которых регулируется российским законодательством в области ИБ и требует соответствия национальным классификаторам угроз.

Во-вторых, методология построения межонтологических связей между гетерогенными базами знаний в области ИБ остается недостаточно формализованной. Базы знаний используют различные таксономии, уровни абстракции и языки описания. Отсутствуют систематизированные подходы к установлению семантических соответствий между угрозами национального классификатора и техниками международных фреймворков, что препятствует формированию единого пространства знаний для комплексного анализа.

В-третьих, вопросы мультиязычного поиска и генерации в GraphRAG-системах для анализа CTI-отчетов исследованы фрагментарно. В рассматриваемом корпусе преобладают англоязычные документы, БДУ ФСТЭК России и запросы аналитиков отечественных центров мониторинга ИБ (Security Operations Center, SOC) представлены преимущественно на русском языке. Используемые многоязычные векторные представления (embeddings) обеспечивают техническую возможность кросс-язычного поиска, однако отдельная оценка режимов RU-RU, EN-EN, RU-EN и EN-RU в настоящем исследовании не проводилась.

Цель работы состоит в разработке и экспериментальной оценке модели графа знаний BDU-KG, алгоритма построения межонтологических связей и алгоритма двухконтурного извлечения контекста. Проверяется гипотеза о том, что включение типизированных графовых фактов и межонтологических связей повышает точное совпадение ответа с эталоном и полноту извлечения сущностей по сравнению с текстовым поиском в многошаговых сценариях. Практическим критерием достижения цели является повышение полноты контекста при контролируемом изменении метрики оценки релевантности извлеченного контекста с учетом его ранжирования (Context Precision) и снижении доли утверждений, не поддержанных переданным контекстом.

Анализ применения графов знаний в области ИБ с помощью GraphRAG-систем

Проблема автоматизации построения графов знаний в области ИБ, предназначенных для анализа и защиты сетевой инфраструктуры, обсуждается во многих публикациях (например, [12, 13]).

Оригинальная двухэтапная процедура генерации графов знаний из текстов домена знаний, где на первом этапе с помощью LLM осуществляется построение непосредственно графов знаний в виде совокупности взаимосвязанных триплетов («субъект» — «отношение» — «объект»), а на втором этапе производится проверка достоверности полученных графовых моделей с использованием онтологий, предложена в [14].

В [15] исследуются вопросы применения LLM с открытым исходным кодом (и весовыми коэффициентами) для извлечения и структурирования знаний в форме триплетов из текстов в области ИБ. Полученные триплеты используются при построении графов знаний, интегрированных с LLM для решения задач перевода, суммаризации текстов и извлечения сущностей. Качество решений оценивалось с помощью метрик ROUGE, предназначенных для сравнения сгенерированного текста с эталонным текстом.

В [16] разработана программная среда Knowledge Graph Verifier для оценки качества данных о TTP, основанная на объединении интерпретируемых графов знаний и LLM как носителей контекстных априорных знаний. В работе предложены критерии, позволяющие автоматически извлекать ключевые утверждения из открытых баз данных о TTP и проверять достоверность этих утверждений.

Общие вопросы архитектуры и применения GraphRAG-систем рассмотрены в [17]. Графовое расширение позволяет учитывать связи между фрагментами и повышать связность контекста, однако само по себе не гарантирует устранения необоснованных ответов или снижения вычислительных затрат.

В [18] обсуждается подход к интеграции графов знаний и RAG-технологии в области кибербезопасности, названный авторами средой CyKG-RAG Framework. Рассмотрены основные этапы проектирования проблемно-ориентированной Graph-RAG-системы. Вначале осуществляется построение графа знаний с использованием двух типов источников: локальных данных логов и событий ИБ, отражающих специфику обеспечения ИБ конкретной организации, и внешних данных из публичных источников и предметных баз знаний.

Графы знаний для предметной области TTP часто строятся путем автоматического извлечения знаний из специализированных текстов на основе правил (rule-based approach) и LLM-ориентированных подходов (LLM-based approach). Однако необработанные знания, извлеченные из CTI-документов, могут быть неточными и неполными. Для минимизации таких ошибок применяются онтологии: они обеспечивают семантическую совместимость данных из разных источников и задают априорные ограничения, повышающие надежность анализа.

Интеграция гетерогенных источников данных предметной области приводит к задаче сопоставления онтологий и выравнивания сущностей (ontology matching / entity alignment, OM/EA). Эта задача заключается в установлении соответствий между концептами, атрибутами и отношениями в разных схемах представления знаний. В отличие от построения графа знаний только на основе текстов, построение межонтологических связей предполагает наличие как минимум двух уже существующих онтологий и необходимость контролировать семантическую корректность связей.

Сущности типа «уязвимости» (CVE), «слабости» (CWE), «шаблоны атак» (CAPEC) и «тактики» злоумышленника могут быть представлены как узлы графа знаний. Каждая сущность ассоциируется со специфическими свойствами, описывающими ее атрибуты, такие как идентификатор, описание, оценка воздействия и возможность эксплуатации. Подобная интеграция позволяет создавать комплексные системы анализа угроз безопасности информации (УБИ).

Извлечение сведений о действиях злоумышленников из CTI-текстов рассмотрено в [19], применение графов знаний при формировании гипотез о реализуемых атаках — в [20]. База MITRE D3FEND представляет граф знаний защитных техник (репозиторий онтологии: https://github.com/d3fend/d3fend-ontology). База CVE2CAPEC используется как источник соответствий между записями CVE, CWE, CAPEC и техниками ATT & CK/D3FEND (https://github.com/Galeax/CVE2CAPEC).

Методы автоматического построения графов знаний предметной области ИБ достигли высокой зрелости. CTIKG [21] демонстрирует 91,89 % точности и 89,39 % полноты при извлечении триплетов, CTINexus [22] обеспечивает гибкую адаптацию к различным онтологиям без обширного дообучения моделей, LLM-TIKG [23] эффективно использует обучение на ограниченном количестве примеров для минимизации ручной разметки.

При переходе от единственного доменного графа знаний к составному графу знаний критическим становится вопрос корректного построения межонтологических связей (мостов). В существующих работах задача сквозного сопоставления между разнородными онтологиями часто решается либо вручную, либо эвристически по текстовому/векторному сходству, либо через LLM-сопоставление. Сопоставление рассмотренных работ по источникам знаний, поддержке национальных классификаторов, русскому языку, механизму происхождения данных, экспертной проверке и прямой оценке межонтологических связей показывает, что существующие решения преимущественно решают одну из трех задач: извлечение графа из англоязычного CTI-корпуса, вопросно-ответный

(Question Answering, QA) поиск по готовому графу либо проверку отдельных утверждений. В них, как правило, отсутствует одновременно реализованный переход от БДУ ФСТЭК России к международным базам знаний ATT & CK и D3FEND, разделение нормативного и доказательного контекста, а также отдельная оценка качества автоматически построенных межонтологических связей. Указанное сочетание признаков определяет научную задачу и границы заявляемой новизны.

Для решения данных проблем предлагается метод анализа данных киберразведки на основе модели графа знаний, алгоритмов построения межонтологических связей и извлечения контекста.

Разработка метода анализа данных киберразведки на основе модели графа знаний, алгоритмов построения межонтологических связей и извлечения контекста

Предлагаемый метод объединяет модель графа знаний, алгоритм построения межонтологических связей и алгоритм двухконтурного извлечения контекста. Далее под термином «проверяемое выравнивание» понимается свойство, при котором для каждой сформированной связи сохраняются источник, версия, компонентные оценки, примененные правила и подтверждающий путь (формальная верификация как метод анализа онтологий не применяется).

Модель предметной области BDU-KG

BDU-KG является концептуальной и логической моделью предметной области, физически реализованной как размеченный граф свойств (Labeled Property Graph). Модель объединяет нормативный слой БДУ ФСТЭК России, базы знаний MITRE ATT & CK и MITRE D3FEND, слои CVE/CWE/CAPEC и доказательные фрагменты CTI-отчетов. Модель BDU-KG не является формальной OWL-онтологией, так как аксиоматический вывод и автоматическая проверка непротиворечивости не применяются.

Модель отличается строгой типизацией сущностей: угрозы, объекты воздействия, компоненты, способы реализации угроз, меры защиты, техники атак, защитные техники, уязвимости, слабости и паттерны атак представлены как типизированные узлы. Отношения между ними разделяются на нормативные связи, заимствованные из исходных баз знаний, и межонтологические связи. Мультиязычные текстовые атрибуты используются как унифицированный носитель семантики для поиска и сопоставления. Это позволяет обеспечить семантическую совместимость русско- и англоязычных источников о TTP, прослеживаемость фактов и корректное структурное расширение подграфа в задачах многошагового анализа.

Граф свойств задается кортежем

$$G = (V, E, \lambda_V, \lambda_E, A_V, A_E, \Pi),$$

где V и E — множества узлов и ориентированных ребер; λ_V и λ_E — функции типизации узлов и отношений; A_V и A_E — их атрибуты; Π — сведения о происхождении данных.

Пусть имеются два графа знаний: $G_B = (V_B, E_B)$ — граф БДУ и $G_M = (V_M, E_M)$ — граф международного фреймворка, например ATT & CK или D3FEND. Здесь V_B и V_M обозначают множества узлов, а E_B и E_M — множества отношений внутри соответствующих графов.

Входом метода являются исходные графы БДУ (G_B) и графы международных фреймворков ATT & CK или D3FEND (G_M), корпус документов D, запрос пользователя q, набор доменных правил R и параметры Θ.

Выход включает множество межонтологических связей B, контекст ответа $C(q)$, ответ y и связанный с ним набор происхождения Π_y.

Критерии достижения цели определяются на двух уровнях: качество межонтологических связей оценивается количественными метриками Precision, Recall, F_1, AUC-ROC и Accuracy; качество QA-системы — количественными метриками Exact Match, F_1, Entity Recall@50, Context Precision, Answer Relevancy и Faithfulness.

Алгоритм построения межонтологических связей с контролем корректности

Предлагаемый алгоритм предназначен для построения межонтологических связей между сущностями БДУ и сущностями ATT & CK/D3FEND с учетом формальных доменных ограничений. Эти связи далее используются в двухконтурном алгоритме извлечения контекста для GraphRAG: нормативные факты БДУ включаются в контекст обязательно, а фрагменты CTI-отчетов используются как доказательный слой.

Алгоритм строит только два типа межонтологических связей: MAPS_TO_TECHNIQUE от способа реализации угрозы RealizationMethod к технике ATT & CK AttackTechnique и IMPLEMENTED_BY от меры защиты BduControl к защитной технике D3fendTechnique. Отношения MITIGATED_BY_CONTROL и DEFENDS_AGAINST являются предметными отношениями, импортируемыми соответственно из БДУ и MITRE D3FEND, и не оцениваются как результат сопоставления сущностей. Прямое отношение BduThreat к AttackTechnique не вводится, угроза связывается с техникой через нормативное отношение REALIZED_BY и узел RealizationMethod.

Каждый узел v из объединения V_B и V_M описывается следующими характеристиками:

— тип type(v) (например, “RealizationMethod”, “AttackTechnique”, “D3fendTechnique”, “BduControl”);

— мультиязычные текстовые поля text(v) = = {*title*, *description*, *synonyms*};

— набор атрибутов attr(v).

Межонтологическая связь задается кортежем

$$b = (u, v, r, s, \varepsilon),$$

где u и v — сущности разрешенных типов; r — тип отношения; $s \in [0, 1]$ — итоговая оценка уверенности в корректности связи; ε — набор проверяемых сведений. Структура ε включает идентификаторы и версии источников, идентификатор документа или записи, подтверждающий текстовый диапазон либо путь в графе, результаты доменных правил, компонентные оценки, итоговый статус и отметку экспертной проверки.

Построение выполняется каскадно. Сначала для каждой исходной сущности формируется не более k кандидатов по косинусному сходству многоязычных векторных представлений и лексическому перекрытию. Затем применяются критические ограничения совместимости типов, допустимого направления отношения и структурной согласованности. Кандидаты, не прошедшие ограничения, исключаются до обращения к языковой модели.

Оставшиеся кандидаты проверяются локальной LLM. Модель получает только описания двух сущностей, результаты правил и доступные доказательства и возвращает метку “match”, “partial” или “no”, числовую оценку и краткое обоснование. В последующей реализации метки отображались на интервалы: “no” — [0; 0,34], “partial” — [0,35; 0,74], “match” — [0,75; 1].

Оценка уверенности может задаваться обучаемым классификатором либо линейной агрегацией компонентных оценок

$$s(u, v) = \alpha \times s_{vec}(u, v) + \beta \times s_{rule}(u, v) + \\ + \gamma \times s_{LLM}(u, v), \quad (1)$$

где $s_{vec}(u, v)$ — косинусное сходство векторных представлений описаний сущностей; $s_{rule}(u, v)$ — оценка прохождения доменных правил; $s_{LLM}(u, v)$ — оценка LLM поддержки связи переданными фактами; α, β и γ ($\alpha + \beta + \gamma = 1$) — веса компонент, задаваемые экспертно или калибруемые на проверочной выборке.

В исходном сравнении использовались веса $\alpha = 0{,}4$, $\beta = 0{,}3$, $\gamma = 0{,}3$ и порог $\tau = 0{,}6$, выбранные на проверочной выборке. В последующей реализации применялись раздельные параметры: для отношений MAPS_TO_TECHNIQUE — 0,50/0,30/0,20 и $\tau = 0{,}65$; для IMPLEMENTED_BY — 0,40/0,40/0,20 и $\tau = 0{,}68$. Значения $0{,}55 \le s < \tau$ направлялись на экспертную проверку; значения ниже 0,55 отклонялись.

Альтернативный вариант построения использует обучаемый классификатор f_θ по 12 признакам: сходству описаний и заголовков, коэффициенту Жаккара для ключевых слов, совместимости типов, наличию и длине подтверждающего пути, общим тактикам и платформам, результату LLM-проверки, соотношению длин описаний и языковому признаку.

Завершаемость алгоритма обеспечивается конечностью множеств исходных сущностей и ограничением k. При индексированном поиске кандидатов вычислительно дорогостоящая LLM-проверка выполняется для не более чем $k|V_B|$ кандидатов, прошедших критические ограничения (вместо полного декартова произведения $|V_B| \times |V_M|$).

Алгоритм 1. BridgeBuild: построение межонтологических связей с контролем корректности

Вход: Базовый граф $G_B = (V_B, E_B)$, объединяемый граф $G_M = (V_M, E_M)$, набор правил **R**, параметр k — максимальное число кандидатов на исходную сущность, пороговое значение τ

Ensure: Набор межонтологических связей B

1: $B \leftarrow \varnothing$
2: **for all** $u \in V_B$ **such that** Eligible(u) **do**
3: C ← TopK(VectorCandidates(u, V_M), k)
4: **for all** $v \in C$ **do**
5: ($pass$, s_{rule}, e_{rule}) ← RuleVerify(u, v, R)
6: **if not** $pass$ **then**
7: **continue**
8: **end if**
9: ($label$, s_{LLM}, e_{LLM}) ← LLMVerify(u, v, e_{rule})
10: s ← $\alpha \cdot s_{vec}(u, v) + \beta \cdot s_{rule} + \gamma \cdot s_{LLM}$
11: **if** $s \ge \tau$ and $label \in \{match, partial\}$ **then**
12: r ← SelectRelation($type(u)$, $type(v)$, $label$, R)
13: $B \leftarrow B \cup \{(u, v, r, s, \varepsilon)\}$
14: **end if**
15: **end for**
16: **end for**
17: **return** B

Шаблон запроса к LLM ограничивает ответ переданным JSON, запрещает использование внешних знаний и требует машиночитаемый формат. Невалидный ответ отклоняется либо повторно запрашивается; автоматическое принятие невозможно при нарушении критического доменного правила. На шаге 13 объект ε объединяет сведения об источниках пары, результаты e_{rule} и e_{LLM} и итоговый статус проверки.

Таким образом, алгоритм построения межонтологических связей основан на алгоритмах OM/EA, отличается процедурой создания связей и их оценки. Использование независимых подтверждающих путей в графе знаний и порогового принятия связи по оценке $s(u, v)$ позволяет снизить долю ложноположительных соответствий и повысить воспроизводимость сопоставлений.

Алгоритм двухконтурного извлечения контекста

Для запроса q контекст формируется как $C(q) = P_{ack}(C_{norm}(q), C_{evid}(q), B_{tok})$, где C_{norm} — нормативное ядро, C_{evid} — доказательный слой, B_{tok} — токенный бюджет. В первом контуре извлекаются стартовые узлы БДУ, после чего выполняется ограниченное расширение по разрешенным типам ребер. Карточки узлов и типизированные триплеты нормативного подграфа включаются в итоговый контекст независимо от наличия внешних текстовых свидетельств.

Во втором контуре сущности нормативного подграфа используются для расширения запроса к векторному хранилищу. CTI-фрагменты и сводные описания сообществ ранжируются по покрытию сущностей нормативного подграфа G_{norm}, близости к запросу, разнообразию источников и избыточности. Дубликаты удаляются по идентификатору источника и нормализованному тексту. При $k = 50$ средний объем сформированного контекста в основной серии составлял около 3000 токенов.

Каждое утверждение ответа связывается с используемыми карточками, отношениями и фрагментами. Такой механизм обеспечивает проверяемость происхождения и уменьшает избыточность контекста.

Алгоритм 2. DualLoopContext: двухконтурное извлечение контекста
Вход: запрос q, токенный бюджет B_{tok}
Выход: упакованный контекст C

1: $S_0 \leftarrow \text{RetrieveBDUNodes}(q, k_1)$
2: $G_{norm} \leftarrow \text{GraphExpand}(S_0, \text{depth} = d_1, \text{edge_allowlist} = \text{NormEdges})$
3: $C_{norm} \leftarrow \text{SummarizeFacts}(G_{norm}, \text{budget} = b_1)$
4: $q' \leftarrow \text{AugmentQuery}(q, \text{Entities}(G_{norm}))$
5: $T \leftarrow \text{RetrieveCTITexts}(q', k_2)$
6: $C_{evid} \leftarrow \text{SelectAndLinkEvidence}(T, G_{norm}, \text{budget} = b_2)$
7: **return** $P_{ack}(C_{norm}, C_{evid}, B_{tok})$

Таким образом, LLM используется как генератор ответа поверх явно извлеченного и проверяемого контекста. Это важно для задач SOC-аналитики: пользователь должен видеть, какие угрозы БДУ, техники ATT & CK, защитные техники D3FEND и фрагменты CTI-отчетов использованы при формировании вывода.

Разработка GraphRAG-системы анализа данных киберразведки

Программная система реализует модель BDU-KG и конвейер генерации ответов с расширенным поиском с поддержкой русско- и англоязычных текстовых представлений. Многоязычность обеспечивается моделью векторных представлений и нормализацией терминов (отдельная экспериментальная оценка всех четырех кросс-язычных направлений в основной серии не проводилась).

В отличие от классического RAG, где контекст формируется исключительно из фрагментов документов, система приоритизирует графовые факты БДУ (объекты, последствия, способы реализации, меры) и использует текстовые доказательства как дополнительный слой обоснования.

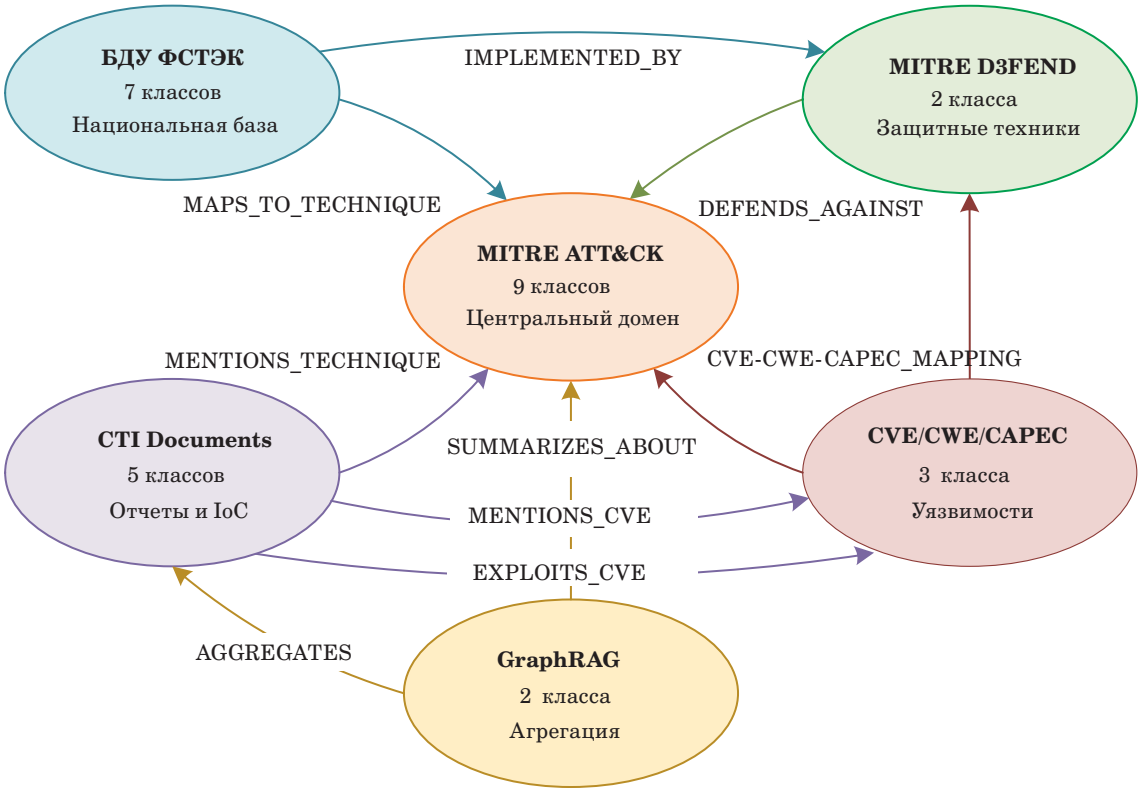
Граф знаний BDU-KG объединяет шесть взаимосвязанных доменов (рис. 1, табл. 1). На концептуальном уровне задаются типы сущностей и отношений; на логическом уровне — ограничения допустимых направлений и атрибуты происхождения; физическая реализация выполнена в Neo4j как размеченный граф свойств.

Проектная физическая схема графа (рис. 2) содержит 30 меток узлов и 23 типа отношений. В экспериментальном снимке экземпляры присутствовали для 24 меток; шесть резервных меток, относящихся к необязательным CTI-сущностям и вспомогательным слоям агрегации, не участвовали в расчете метрик. Междоменные отношения MAPS_TO_TECHNIQUE и IMPLEMENTED_BY формирует алгоритм BridgeBuild.

В экспериментальном дизайне предусмотрены две альтернативные реализации связей между графами, дающие разные компромиссы по трудоемкости и качеству.

1. Вариант M_1. Строится таблица соответствий, подготовленная экспертами в полуавтоматическом режиме.

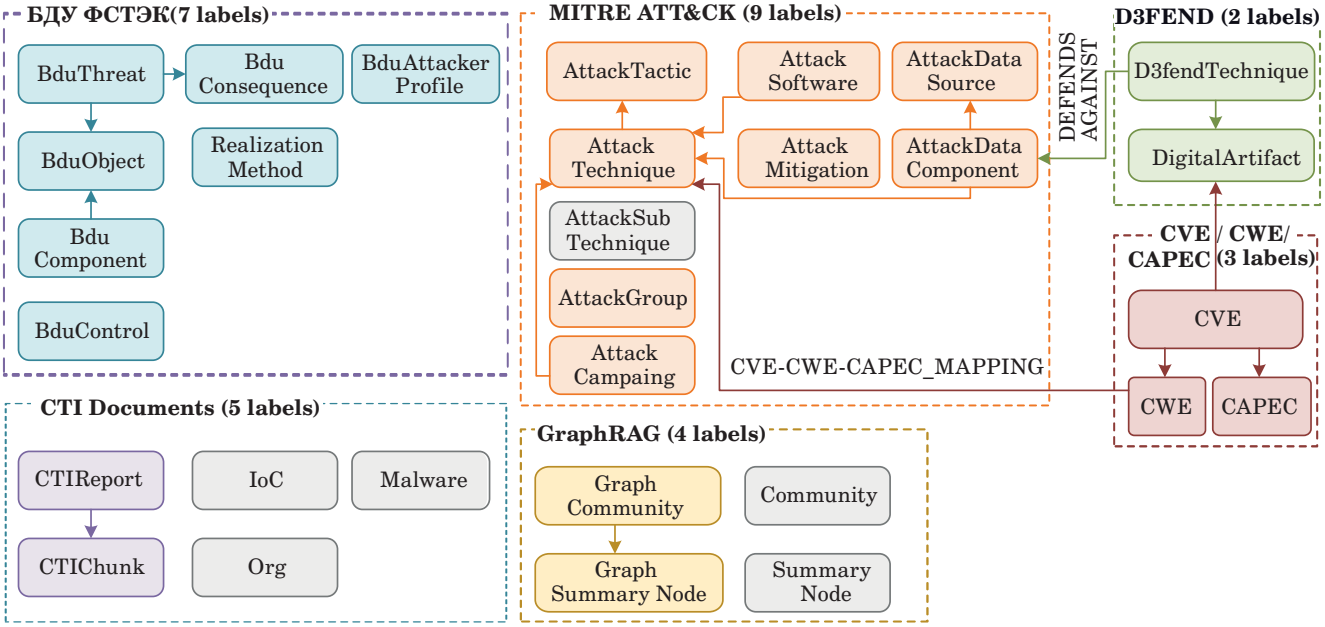
2. Вариант M_2. С помощью предложенного алгоритма построения межонтологических связей между национальным каталогом угроз и международными фреймворками вариант M_2 реализует полуавтоматическое построение межонтологических связей на основе комбинирования: семантической близости текстовых описаний, доменных ограничений/правил согласованности и ограниченной LLM-верификации, выполняемой только после прохождения критических фильтров.



■ ***Рис. 1.*** Концептуальная модель графа знаний BDU-KG
■ ***Fig. 1.*** Conceptual model of the BDU-KG knowledge graph

■ ***Таблица 1.*** Объединяемые домены
■ ***Table 1.*** Interrelated domains

Домен	Описание
БДУ ФСТЭК	Содержит классы для представления УБИ (BduThreat), объектов воздействия (BduObject), компонентов информационных систем (BduComponent), мер защиты (BduControl), негативных последствий (BduConsequence) и способов реализации угроз (RealizationMethod). Связи между классами отражают семантику отношений: угроза направлена на объект, реализуется определенным способом и приводит к последствиям
MITRE ATT & CK	Представлен классами тактик (AttackTactic), техник (AttackTechnique), групп злоумышленников (AttackGroup), кампаний (AttackCampaign), вредоносного программного обеспечения (AttackSoftware), мер противодействия (AttackMitigation) и источников данных для обнаружения (AttackDataSource, AttackDataComponent). Иерархическая структура техник и их принадлежность тактикам моделируются связями “CHILD_OF” и “PART_OF_TACTIC”
MITRE D3FEND	Включает защитные техники (D3fendTechnique) и цифровые артефакты (DigitalArtifact), на которых они разворачиваются. Связь “DEFENDS_AGAINST” обеспечивает сопоставление защитных техник с техниками атак ATT & CK
CWE-CVE-CAPEC	Объединяет записи CVE, классификацию CWE и паттерны атак CAPEC. Связи между ними позволяют проследить цепочку от конкретной уязвимости через эксплуатируемую слабость к технике атаки
CTI-отчеты о TTP	Содержит отчеты и их текстовые фрагменты, а также классы для индикаторов компрометации (IoC), вредоносных программ (Malware) и организаций (Org)
GraphRAG	Включает иерархические сообщества (GraphCommunity) и их текстовые резюме (GraphSummaryNode), формируемые конвейером Microsoft GraphRAG для поддержки глобального поиска по корпусу документов



■ ***Рис. 2.*** Физическая схема графа знаний BDU-KG
■ ***Fig. 2.*** Physical diagram of the BDU-KG knowledge graph

Экспериментальная оценка эффективности предложенного метода

Цель серии экспериментов — оценить качество автоматически построенных межонтологических связей и влияние компонентов BDU-KG на качество ответов. На первом уровне сравниваются классификаторы и методы OM/EA; на втором — конфигурации QA-системы по трем сценариям.

Для основной серии использован корпус из 2262 CTI-отчетов из 169 открытых источников (табл. 2). Он включает публикации компаний в области ИБ, публичные репозитории отчетов и бюллетени центров реагирования на компьютерные инциденты. Документы содержат сведения о TTP злоумышленников, индикаторах компрометации и мерах противодействия.

Пример межонтологической трассировки

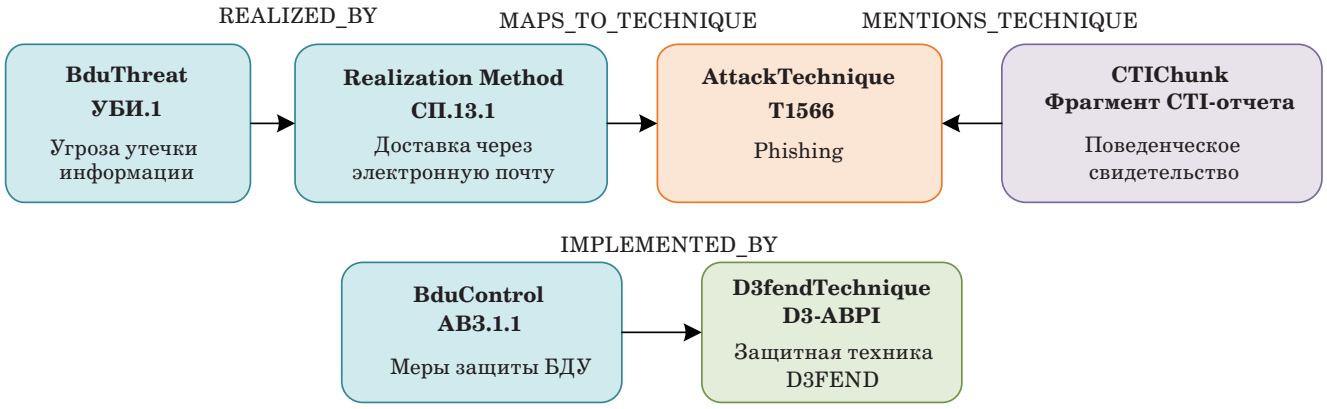
Два отдельных фрагмента межонтологической трассировки приведены на рис. 3. Нормативное отношение REALIZED_BY связывает УБИ.1 «Угроза утечки информации» со способом СП.13.1; связь MAPS_TO_TECHNIQUE соединяет способ с техникой T1566 Phishing (фишинг). Отношение MENTIONS_TECHNIQUE показывает присоединение текстового фрагмента. Отдельно мера АВЗ.1.1 связана с D3-ABPI отношением IMPLEMENTED_BY. Прямая нормативная связь УБИ.1 с АВЗ.1.1 не утверждается. Имена ребер на рисунке обозначают логические типы.

Статистика физической схемы представления графа знаний такова:

— типы узлов — 30;
— реализованные типы узлов — 24;
— типы связей — 23;
— межподсистемные связи — 5.

■ ***Таблица 2.*** Статистика собранного набора данных
■ ***Table 2.*** Statistics of the collected dataset

Характеристика	Значение
Общее количество документов	2262
Количество источников	169
Преобладающий язык	Английский (70 %)
Основные вендоры	Kaspersky, FireEye, Symantec, ESET, Trend Micro, Palo Alto Networks, CrowdStrike
Тематика	APT-группировки, вредоносное ПО, целевые атаки, IoC



■ ***Рис. 3.*** Проверяемые фрагменты межонтологической трассировки BDU-KG
■ ***Fig. 3.*** Verifiable fragments of BDU-KG cross-ontology tracing

Оценка алгоритма построения межонтологических связей

Задача сформулирована как бинарная классификация пар сущностей (u, v), где $u \in V_{BDU}$, $v \in V_{MITRE}$, $y = 1$ означает наличие корректной межонтологической связи. Подтвержденный набор содержит 2630 пар и разделен на обучающую, проверочную и тестовую части в пропорции 70/15/15: 1841, 395 и 394 пары. Разделение стратифицировано по типам сущностей и источникам.

Для каждой пары (u, v) строится вектор из 12 типов признаков (табл. 3).

Положительные примеры включают 847 экспертных пар BduThreat-AttackTechnique, 312 отношений D3FEND-ATT & CK и 156 проверенных цепочек CVE/CWE/CAPEC (табл. 4). Этот смешанный набор используется для оценки классификатора соответствий и не является отдельной оценкой двух типов связей, создаваемых алгоритмом BridgeBuild в подразделе «Алгоритм построения межонтологических связей с контролем корректности». Отрицательные примеры включают сложные пары с высоким семантическим сходством и случайные пары с балансировкой типов.

Сравниваются четыре подхода к построению классификатора (табл. 5).

Гиперпараметры подбирались с помощью кросс-валидации с пятью проходами на обучающей части, порог решения выбирался по максимуму F_1 на проверочной части. Тестовая часть использовалась для итоговой оценки согласно зафиксированному протоколу ранней редакции (табл. 6).

■ ***Таблица 3.*** Векторы признаков, используемые для обучения классификатора
■ ***Table 3.*** Feature vectors used to train the classifier

Признак	Описание	Диапазон
sim_vec	Косинусное сходство BGE-M3 вложений	[0, 1]
sim_title	Косинусное сходство только заголовков	[0, 1]
jaccard_keywords	Коэффициент Жаккара для извлеченных ключевых слов	[0, 1]
score_rule_type	Оценка совместимости типов (0/0,5/1)	{0, 0,5, 1}
score_rule_struct	Наличие подтверждающего пути в графе	{0, 1}
path_length	Минимальная длина пути через CVE/CWE/CAPEC	[0, 10]
common_tactics	Число общих тактик ATT & CK	[0, 14]
common_platforms	Число общих платформ	[0, 8]
score_llm	Оценка LLM-верификатора	[0, 1]
llm_confidence	Эвристическая оценка по длине обоснования LLM (не калиброванная вероятность)	[0, 1]
desc_length_ratio	Отношение длин описаний	[0, 1]
lang_match	Совпадение языка описаний	{0, 1}

■ ***Таблица 4.*** Структура набора данных для оценки межонтологических связей
■ ***Table 4.*** Dataset structure for evaluating cross-ontology links

Класс	Количество пар	Источник
Положительный	847	Экспертно проверенные пары BduThreat-AttackTechnique
	312	Определенные в исходных онтологиях пары D3FEND-ATT & CK
	156	Цепочки CVE/CWE/CAPEC с экспертной проверкой
Отрицательный	420	Сложные отрицательные пары: $s_{vec} > 0{,}7$, отклоненные экспертами
	895	Случайные отрицательные пары с балансировкой типов

■ ***Таблица 5.*** Проанализированные подходы к построению классификатора
■ ***Table 5.*** Analyzed approaches to classifier construction

Обозначение	Название	Характеристика
M_{base}	Линейная комбинация (контрольная модель)	Формула (1) с весами $\alpha = 0{,}4$, $\beta = 0{,}3$, $\gamma = 0{,}3$, порогом $\tau = 0{,}6$, подобранными с помощью grid search на validation set
M_{LR}	Логистическая регрессия	12 признаков с L2-регуляризацией ($C = 1{,}0$) Интерпретируемые веса признаков
M_{MLP}	Многослойный перцептрон	Количество нейронов по слоям: 12, 32, 16, 1 Функции активации: ReLU (скрытые слои), Sigmoid (выход) Dropout: 0,3 между слоями Оптимизатор: Adam, lr = 0,001 Early stopping по validation loss (patience = 10)
M_{XGB}	Gradient Boosting (XGBoost)	n_estimators = 100, max_depth = 4 Автоматический подбор важности признаков

■ ***Таблица 6.*** Качество классификации межонтологических связей на тестовой выборке
■ ***Table 6.*** Cross-ontology link classification quality on the test set

Модель	Precision	Recall	F_1	AUC-ROC	Accuracy
M_{base}	0,78	0,71	0,74	0,81	0,76
M_{LR}	0,82	0,79	0,80	0,87	0,81
M_{MLP}	0,85	0,82	0,83	0,91	0,84
M_{XGB}	0,84	0,83	0,83	0,90	0,85

Наибольшее значение F_1, равное 0,83, получено для M_{MLP} и M_{XGB}. По результатам классификации соответствий M_{XGB} рекомендован для дальнейшего применения с учетом возможности анализа важности признаков. Наиболее значимыми признаками были семантическое сходство описаний (0,23), наличие структурного подтверждающего пути (0,18), LLM-оценка (0,15) и длина пути через CVE/CWE/CAPEC (0,12) (табл. 7).

Статистическая значимость различий в качестве классификатора связей оценивалась непараметрическим методом bootstrap. Для 1000 ресэмплирований тестового набора с возвращением вычислялась метрика F_1 и разность $\Delta = F_1(B) - F_1(A)$. Далее строился 95%-й доверительный интервал для Δ процентильным методом; отсутствие нуля в интервале интерпретировалось как статистически значимое различие на уровне ($\alpha = 0{,}05$).

Анализ ошибок выявил 23 ложноположительных случая, обусловленных, главным образом, смешением уровней абстракции и поверхностным семантическим сходством, и 28 ложноотрицательных случаев, связанных с неочевидными путями CVE/CWE и мультиязычными парами с низкой векторной близостью.

Качественный анализ ошибочных классификаций связей приведен в табл. 8.

Предложенный алгоритм сопоставлялся с пороговым косинусным сходством, LogMap-Lite, прямой LLM-проверкой и LLM-проверкой кандидатов Top-K (табл. 9).

Алгоритм BridgeBuild в варианте M_{XGB} обеспечил значение для метрики $F_1 = 0{,}83$ при среднем времени обратки 0,33 с на пару. На тестовом множестве число LLM-вызовов сократилось приблизительно в семь раз. При обработке полного

■ ***Таблица 7.*** Важность признаков по модели M_{XGB} (нормализованная)
■ ***Table 7.*** Feature importance according to the M_{XGB} model (normalized)

Ранг	Признак	Важность	Интерпретация
1	sim_vec	0,23	Семантическое сходство текстовых описаний — основной признак
2	score_rule_struct	0,18	Структурные пути в графе критичны для верификации связей
3	score_llm	0,15	LLM-оценка значима, но не доминирует
4	path_length	0,12	Короткие пути через CVE/CWE подтверждают связь
5	common_tactics	0,09	Общие тактики — косвенный индикатор
6	jaccard_keywords	0,07	Лексическое пересечение полезно
7	score_rule_type	0,06	Совместимость типов — необходимое условие
8–12	Остальные	0,10	Вспомогательные признаки

■ ***Таблица 8.*** Анализ основных ошибочных классификаций связей
■ ***Table 8.*** Analysis of the main misclassifications of relationships

Типы ошибок	Описание
False Positives (ложные связи)	14 случаев: высокое текстовое сходство при разных уровнях абстракции (например, общая угроза БДУ сопоставлена с узкоспециализированной техникой ATT & CK) 9 случаев: ошибочная LLM-верификация из-за поверхностного семантического сходства
False Negatives (пропущенные связи)	16 случаев: связи через неочевидные цепочки CVE/CWE, не покрытые признаками 12 случаев: мультиязычные пары с низким sim_vec из-за ошибочного сопоставления

■ ***Таблица 9.*** Сравнение методов построения межонтологических связей
■ ***Table 9.*** Comparison of cross-ontology link construction methods

Метод	Описание	Категория	Precision	Recall	F_1	Время, с/пара	LLM-вызовы
Cosine-Threshold	Косинусное сходство BGE-M3 векторов вложений с порогом $\tau = 0{,}75$	На основе векторов вложений	0,62	0,78	0,69	0,002	0
LogMap-Lite	Версия LogMap с лексическим и структурным сопоставлением	Классический OM	0,71	0,54	0,61	0,008	0
LLM-Direct	Прямой запрос к LLM для каждой пары без предварительной фильтрации	LLM-based	0,79	0,81	0,80	2,1	645
LLM-TopK	Генерация Top-K кандидатов по векторам вложений и LLM-верификация всех кандидатов	Гибридный	0,76	0,84	0,80	1,8	6450
BridgeBuild M_{base}	Предложенный метод с линейной комбинацией оценок	Предложенный	0,78	0,71	0,74	0,31	89
BridgeBuild M_{XGB}	Предложенный метод с обучаемым классификатором	Предложенный	0,84	0,83	0,83	0,33	92

пространства (1247 сущностей БДУ × 623 техники ATT & CK) возможных пар сущностей каскадная фильтрация сократила число LLM-проверок приблизительно до 1200. Время работы алгоритма BridgeBuild распределялось следующим образом: генерация кандидатов — 12 %, доменные правила — 8 %, LLM-проверка — 78 %, классификация — 2 %.

Сценарии и конфигурации тестирования на корпусе CTI-отчетов

Проанализированы три класса QA-задач, различающиеся центральной сущностью запроса и требуемой глубиной рассуждения. Для BDU-QA сценариев центральной сущностью является угроза из БДУ ФСТЭК России, представляемая узлом BduThreat. Для Crosswalk-QA сценариев требуется переход между TTP-фрагментом, техниками ATT & CK, угрозами БДУ и защитными техниками D3FEND. Для сценариев TTP-QA основной входной объект — фрагмент CTI-отчета.

Цель эксперимента — оценить вклад каждого компонента архитектуры BDU-KG в качество ответа: векторного извлечения, структурного расширения подграфа, межонтологических связей M_1/M_2 и слоя обобщения групп сущностей.

В эксперименте используются следующие источники знаний, импортируемые в единый BDU-KG:

— БДУ ФСТЭК: угрозы (УБИ), объекты, компоненты, способы реализации, меры защиты, негативные последствия, профили нарушителей;

— ATT & CK (STIX): Enterprise/ICS/Cloud. В качестве эталонного формата используется репозиторий MITRE CTI/STIX;

— MITRE D3FEND (онтология): защитные техники и артефакты;

— CVE2CAPEC: связка CVE-CWE-CAPEC-ATT & CK-D3FEND как независимый слой для проверки качества связей;

— корпус CTI-отчетов как источник текстовых свидетельств и задач CTI-QA.

Векторный слой реализуется в СУБД Qdrant. Используются коллекции “kg_nodes”, “descriptions” и “cti_chunks”. Коллекция “kg_nodes’ содержит векторные представления карточек сущностей графа; “descriptions” — расширенные текстовые описания узлов и отношений; “cti_chunks” — фрагменты CTI-отчетов. Такая декомпозиция позволяет отдельно оценивать вклад поиска по графовым сущностям и поиска по текстовым свидетельствам.

Загрузка CTI-документов создает узлы отчетов и фрагментов, нормализует идентификаторы и сохраняет ссылку на снимок источника. Векторные представления карточек сущностей, описаний и CTI-фрагментов индексируются раздельно, что позволяет оценивать вклад структурного и текстового каналов.

Эксперименты формируются в трех взаимодополняющих сценариях.

Сценарий A (BDU-QA) проверяет ответы на вопросы по структуре БДУ: затронутые объекты и компоненты, негативные последствия, способы реализации, меры защиты и релевантность профилей нарушителя. Эталонная разметка задается в виде текстового ответа и множества идентификаторов БДУ.

Сценарий B (Crosswalk-QA) проверяет построение сквозных сопоставлений. На вход подается фрагмент CTI-отчета; требуется извлечь TTP и другие сущности, сопоставить их с УБИ и сформировать объяснение через подграф «TTP — ATT & CK — БДУ — меры БДУ — D3FEND».

Сценарий C (TTP-QA) проверяет способность системы по фрагменту CTI-отчета определить техники ATT & CK, возможные УБИ и релевантные контрмеры D3FEND/БДУ.

В качестве базовых конфигураций сравнения использованы: B_0 — Microsoft GraphRAG retrieval, использующий суммаризацию сообществ узлов и текстовые фрагменты корпуса без обращения к структурному графу BDU-KG; B_1 — KG-only QA, использующий только графовый поиск и расширение подграфа в Neo4j без векторного слоя; C_0 — Text-RAG, основанный на векторном поиске по фрагментам CTI-отчетов. Предлагаемые графовые конфигурации C_1–C_4 позволяют последовательно оценить вклад BDU-KG, межонтологических связей M_1/M_2 и слоя суммаризации сообществ (табл. 10).

Во всех конфигурациях использовались одинаковые векторные представления BGE-M3 и единый LLM-слой генерации ответов — Gemma3:27B через Ollama. Для оценки метрик с помощью RAGAS отдельно применялась модель GPT-4o в роли модели-судьи, что исключает совпадение генератора ответа и оценивателя.

Для каждого из трех сценариев сформировано по 250 тестовых вопросов, всего 750 вопросов. Эталонная разметка включает нормализованное множество идентификаторов и, где применимо, текстовое пояснение. Вопросы BDU-QA охватывают атрибуты угроз БДУ; Crosswalk-QA требуют междоменного перехода; TTP-QA направлены на извлечение техник и связанных защитных сущностей из CTI-фрагментов.

Наборы вопросов сформированы стратифицированно по типам запросов, целевым сущностям и языку источника. Для BDU-QA выровнены классы по объектам, компонентам, последствиям, способам реализации и мерам защиты; для Crosswalk-QA и TTP-QA контролировались тип цепочки и язык исходного фрагмента. Отдельный независимый набор, полностью исключенный из разработки графа и настройки порогов, в основной серии не формировался.

Метрики и протокол оценки сценариев

Метрики качества ответа на уровне идентификаторов. Точное совпадение (Exact Match, EM) равно 1 при полном совпадении нормализованного множества идентификаторов с эталоном и 0 в противном случае. Мера F_1 (F1-score) представляет собой гармоническое среднее точности и полноты: точность (Precision) отражает долю корректных идентификаторов среди выданных,

■ ***Таблица 10.*** Сравниваемые конфигурации в одинаковых условиях векторных представлений и LLM-слоя
■ ***Table 10.*** Comparable configurations under the same embedding/LLM backend conditions

ID	Конфигурация	Векторный вывод	Структурный вывод на KG	Межонтологические связи	Community/ Summary слой	Источники контекста	Роль в эксперименте
B_0	Microsoft GraphRAG-	Да	Нет	Нет	Да	TTP-корпус и обобщения сообществ, построенные по документам и сущностному графу корпуса	Базовая модель из класса GraphRAG: global retrieval по обобщениям без использования доменного графа и ограничений
B_1	KG-only QA без векторного поиска	Нет	Да	Нет	Нет	BDU-KG (узлы и ребра Neo4j)	Оценка вклада только структурного графа без векторного слоя и без обобщений
C_0	Text-RAG	Да	Нет	Нет	Нет	TTP-корпус	Базовый Text-RAG: только векторный поиск по фрагментам текста
C_1	GraphRAG-BDU	Да	Да	Нет	Нет	BDU-KG (без межонтологического выравнивания) и TTP	Базовый граф и векторный поиск: предлагаемый алгоритм извлечения контекста внутри БДУ-домена
C_2	Bridges-M1 (curated)	Да	Да	Да (M_1)	Нет	BDU-KG и межонтологические связи (M_1) и TTP	Основная конфигурация для Crosswalk-QA
C_3	Bridges-M2 (auto)	Да	Да	Да	Нет	BDU-KG и межонтологические связи (M_2) и TTP	Автоматизированное выравнивание
C_4	C3 и Communities	Да	Да	Да (M_2)	Да	BDU-KG, межонтологические связи (M_2), TTP-корпус и суммаризация сообществ	Усиление полноты контекста (для TTP-QA) за счет глобального слоя обобщения; возможное снижение Context Precision

а полнота (Recall) — долю найденных идентификаторов среди эталонных. Метрики рассчитываются раздельно для идентификаторов УБИ, ATT & CK, D3FEND и CVE/CWE/CAPEC после нормализации форматов. Для каждого вопроса мера F_1 рассчитывается по пересечению нормализованных множеств идентификаторов ответа и эталона. В таблицах приведено среднее арифметическое индивидуальных значений F_1 по вопросам соответствующего сценария, все вопросы имеют одинаковый вес.

Метрики RAGAS [24]. Faithfulness оценивает долю утверждений, поддержанных предоставленным контекстом, и не является оценкой фактической истинности. Answer Relevancy отражает соответствие ответа вопросу, Context Precision — релевантность и порядок извлеченных фрагментов. Оценивание выполнялось LLM GPT-4o отдельно от локальной модели-генератора Gemma3:27B. Экспертная калибровка моделисудьи в основной серии не проводилась, поэтому RAGAS-метрики используются как вторичные.

Метрики извлечения контекста. Entity Recall@K определяется как доля эталонных сущностей, присутствующих среди K элементов контекста. Для Text-RAG сущности восстанавливаются по каноническим идентификаторам и привязкам фрагментов к сущностям графа. При $K = 50$ в контекст включались карточки узлов, типизированные отношения и краткие CTI-фрагменты; средний объем составлял около 3000 токенов.

Экспериментальные результаты

Значения метрики Entity Recall@K рассчитывались при $K = 50$. Агрегированные результаты по трем сценариям тестирования представлены в табл. 11–13. Сценарий BDU-QA предназначен для оценки ответов на вопросы по структуре БДУ ФСТЭК России. Сценарий Crosswalk-QA оценивает качество сквозного сопоставления между отчетами кибервразведки, техниками атак, УБИ и мерами защиты. Сценарий TTP-QA направлен на проверку качества анализа фрагментов отчетов о тактиках, техниках и процедурах злоумышленников.

■ ***Таблица 11.*** Качество ответов BDU-QA
■ ***Table 11.*** BDU-QA response quality

Конфигурация	EM	F_1	Entity Recall@50	Faithfulness	Answer Relevancy	Context Precision
B_0	0,55	0,70	0,66	0,82	0,87	0,60
B_1	0,63	0,76	0,72	0,90	0,85	0,74
C_0	0,48	0,65	0,62	0,80	0,86	0,55
C_1	0,77	0,86	0,88	0,93	0,89	0,78
C_2	0,78	0,86	0,89	0,92	0,90	0,74
C_3	0,76	0,85	0,88	0,92	0,89	0,73
C_4	0,78	0,86	0,90	0,92	0,90	0,72

■ ***Таблица 12.*** Качество ответов Crosswalk-QA
■ ***Table 12.*** Crosswalk-QA response quality

Конфигурация	EM	F_1	Entity Recall@50	Faithfulness	Answer Relevancy	Context Precision
B_0	0,26	0,44	0,36	0,74	0,83	0,48
B_1	0,25	0,42	0,34	0,75	0,81	0,58
C_0	0,21	0,38	0,30	0,70	0,82	0,46
C_1	0,34	0,52	0,47	0,78	0,84	0,53
C_2	0,63	0,74	0,79	0,90	0,88	0,69
C_3	0,56	0,68	0,72	0,87	0,87	0,64
C_4	0,65	0,75	0,81	0,89	0,89	0,66

■ ***Таблица 13.*** Качество ответов TTP-QA
■ ***Table 13.*** TTP-QA response quality

Конфигурация	EM	F_1	Entity Recall@50	Faithfulness	Answer Relevancy	Context Precision
B_0	0,36	0,54	0,47	0,76	0,84	0,46
B_1	0,30	0,45	0,40	0,74	0,81	0,57
C_0	0,26	0,41	0,33	0,68	0,80	0,44
C_1	0,38	0,55	0,49	0,78	0,83	0,50
C_2	0,49	0,63	0,60	0,84	0,85	0,54
C_3	0,46	0,61	0,57	0,82	0,85	0,53
C_4	0,55	0,69	0,71	0,86	0,88	0,52

Внутреннее сопоставление конфигураций показывает различия в полноте извлечения релевантных сущностей и поддержке ответов контекстом. Наиболее простой вариант текстовой генерации с расширенным поиском, обозначенный как Text-RAG (C_0), использует только векторный поиск по текстовым фрагментам. В отличие от него конфигурация GraphRAG-BDU (C_1) дополнительно применяет структурное расширение по графу знаний BDU-KG. За счет этого в контекст включаются не только найденные текстовые фрагменты, но и связанные с ними сущности: угрозы, объекты воздействия, способы реализации угроз и меры защиты.

Переход от конфигурации C_0 к конфигурации C_1 приводит к росту точного совпадения ответа с эталоном в сценариях BDU-QA и TTP-QA. Кроме того, в сценарии BDU-QA наблюдается увеличение Entity Recall@50, что указывает на более полное извлечение нормативных сущностей банка данных угроз. Данный результат согласуется с принципом работы графового расширения: после нахождения исходных релевантных узлов система дополнительно включает в контекст связанные с ними элементы подграфа, необходимые для построения обоснованного ответа.

Таким образом, эксперимент подтверждает, что графовый контекст обеспечивает более устойчивую основу для ответа на многошаговые вопросы, чем изолированный поиск по текстовым фрагментам. При этом полученный прирост следует интерпретировать как результат более полного включения структурированных сущностей и связей в тех сценариях, где ответ требует перехода между несколькими предметными слоями. Полученные различия характеризуют исследованные конфигурации и набор вопросов. Они не отделяют эффект графовой структуры от эффекта доступа к дополнительным нормативным фактам и межонтологическим связям и не доказывают переносимость результата на независимую выборку.

В сценарии Crosswalk-QA, предназначенном для оценки сквозного сопоставления между отчетами о тактиках, техниках и процедурах злоумышленников, базой MITRE ATT & CK, БДУ ФСТЭК России и MITRE D3FEND, основной прирост качества обеспечивается межонтологическими связями. Добавление экспертно подготовленных связей M_1 в конфигурации C_2 повышает значение точного совпадения с эталоном с 0,34 для C_1 до 0,63. Автоматически построенные связи M_2 в конфигурации C_3 дают значение 0,56. Различие между C_2 и C_3 составляет 0,07 по точному совпадению и 0,06 по мере F_1, что показывает применимость автоматизированного выравнивания при ограниченных возможностях ручной проверки.

Переход к графовым конфигурациям также повышает контекстную подтвержденность ответов. В Crosswalk-QA Faithfulness возрастает с 0,70 для C_0 до 0,90 для C_2. Это означает, что большая доля утверждений поддерживается переданным контекстом (показатель не следует интерпретировать как доказательство фактической истинности ответа).

Слой сводных описаний сообществ графа, используемый в конфигурации C_4, повышает полноту извлечения сущностей, особенно в сценарии TTP-QA, где ответ требует обобщения сведений из нескольких отчетов. Однако включение таких обобщений может снижать точность контекста, поскольку часть фрагментов имеет косвенную, а не прямую связь с запросом. Поэтому C_4 следует рассматривать как конфигурацию, ориентированную на повышение полноты, но не как универсально лучшую по всем метрикам.

Сравнение с базовыми подходами B_0 и B_1 показывает различную роль компонентов системы. Для BDU-QA более эффективен структурный поиск по графу знаний, тогда как для TTP-QA больший вклад дают сводные описания корпуса. В сценарии Crosswalk-QA оба базовых подхода остаются близкими к текстовой генерации с расширенным поиском, поскольку не используют слой межонтологического выравнивания. Существенное улучшение качества достигается только в конфигурациях C_2 и C_3, где явно заданы связи между доменами знаний.

Для дополнительной проверки устойчивости после основной серии был выполнен детерминированный замер на отдельном наборе TTP-QA. Парный кластерный бутстрэп с 10 000 повторных выборок и поправкой Холма показал прирост Entity Recall@50 графовой конфигурации относительно BM25, равный 0,5225 при 95%-м доверительном интервале [0,4825; 0,5611] на 216 вопросах ($p < 0{,}0004$). После удаления кодов и названий техник из 208 вопросов прирост составил 0,5467 [0,5063; 0,5849] ($p < 0{,}0004$).

Замена линейной модели M_{base} на M_{XGB} в конфигурации C_3 повысила EM с 0,56 до 0,61, F_1 — с 0,68 до 0,72, Faithfulness — с 0,87 до 0,89 (табл. 14). Основное сравнение C_0–C_4 сохраняет исходную конфигурацию C_3 с M_{base}.

Дополнительный эксперимент с тремя генеративными моделями и тремя моделями векторного представления текста подтвердил устойчивость полученных результатов (табл. 15, 16, лучший результат выделен полужирным; формат ячейки: EM / F_1 / Faithfulness): конфигурация C_2 превосходит C_0 во всех рассмотренных комбинациях. Это свидетельствует о том, что основной вклад в повышение качества вносит не выбор конкретной языковой модели, а использование межонтологических связей и графового извлечения контекста.

Прирост точного совпадения с эталоном (EM) наблюдается для всех сочетаний генеративных и векторных моделей, что подтверждает устойчивость преимущества графовой генерации с расширенным поиском при наличии межонтологических связей. При этом качество модели векторного представления текста оказывает более заметное влияние на результат, чем выбор LLM. Наилучшие значения в проведенных экспериментах получены при совместном использовании Gemma3:27B и BGE-M3.

Результаты показывают различную роль компонентов системы. Структурный граф БДУ ФСТЭК России наиболее эффективен для нормативных запросов, межонтологические связи определяют качество сквозного сопоставления между доменами знаний, а слой сводных описаний

■ ***Таблица 14.*** Влияние классификатора связей на Crosswalk-QA

■ ***Table 14.*** Effect of the link classifier on Crosswalk-QA

Конфигурация	EM	F_1	Faithfulness
C_3 с M_{base}	0,56	0,68	0,87
C_3 с M_{XGB}	0,61	0,72	0,89

■ ***Таблица 15.*** Качество ответов Crosswalk-QA для конфигурации C_2 (Bridges-M1)
■ ***Table 15.*** Crosswalk-QA response quality for configuration C_2 (Bridges-M1)

Embedding / LLM	Gemma3:27B	Llama-3.1-70B	Qwen2.5-32B
BGE-M3	**0,63** / **0,74** / **0,90**	0,61 / 0,72 / 0,88	0,59 / 0,70 / 0,87
multilingual-e5-large	0,58 / 0,69 / 0,88	0,56 / 0,67 / 0,86	0,54 / 0,65 / 0,85
LaBSE	0,55 / 0,66 / 0,86	0,53 / 0,64 / 0,84	0,51 / 0,62 / 0,83

■ ***Таблица 16.*** Качество ответов Crosswalk-QA для конфигурации C_0 (Text-RAG)
■ ***Table 16.*** Crosswalk-QA response quality for configuration C_0 (Text-RAG)

Embedding / LLM	Gemma3:27B	Llama-3.1-70B	Qwen2.5-32B
BGE-M3	**0,21** / **0,38** / **0,70**	0,20 / 0,36 / 0,68	0,18 / 0,34 / 0,67
multilingual-e5-large	0,19 / 0,35 / 0,68	0,18 / 0,33 / 0,66	0,16 / 0,31 / 0,65
LaBSE	0,17 / 0,32 / 0,66	0,16 / 0,30 / 0,64	0,14 / 0,28 / 0,62

сообществ повышает полноту при анализе слабоструктурированных отчетов о тактиках, техниках и процедурах злоумышленников. Конфигурация C_4 обеспечивает наибольшую полноту контекста и лучшие значения метрик EM и F_1 в сценариях Crosswalk-QA и TTP-QA, однако не является оптимальной по всем метрикам. Для запросов по БДУ более строгие конфигурации C_1–C_3 сохраняют более высокую точность контекста. Следовательно, в пределах исследованного набора выбор конфигурации должен определяться типом аналитической задачи: нормативные запросы требуют более компактного и точного графового контекста, а вопросы по отчетам кибербразведки выигрывают от добавления обобщающего слоя.

Ограничения исследования

Сравниваемые конфигурации различаются способом представления и доступом к структурированным знаниям: Text-RAG использует преимущественно CTI-фрагменты, тогда как графовые варианты получают БДУ и межонтологические связи. Основной эксперимент оценивает интегрированную архитектуру и не проводит детальную оценку изолированного эффекта формата представления знаний в виде графа. Текстовая конфигурация с теми же фактами не строилась.

Полная независимость основной серии из 750 вопросов от разработки графа и настройки параметров не обеспечена; полный протокол составления и проверки эталонов не восстановлен. Для смешанного набора из 2630 пар отсутствует отдельная оценка двух типов связей действующей модели.

Отдельная оценка запросов RU-RU, EN-EN, RU-EN и EN-RU не проводилась. Значения параметров запуска seed, temperature и top_p для всех исходных запусков не были полностью зафиксированы. Оценки Faithfulness не калибровались на экспертной подвыборке.

Система анализирует угрозы, тактики, техники, уязвимости, последствия и меры защиты и не выполняет полную оценку риска ИБ для конкретной информационной системы: не учитываются ценность активов, фактически установленные версии программного обеспечения, реализованные меры, вероятность реализации угрозы и остаточный риск.

Промышленная апробация с аналитиками SOC, интеграция с CMDB, SIEM, SOAR, MISP и TAXII, обработка TLP-меток и отдельная оценка устойчивости к отравлению графа или внедрению вредоносных инструкций не проводились. Результаты имеют рекомендательный характер и требуют последующей интеграции в существующие системы мониторинга ИБ.

Заключение

В работе предложена модель графа знаний BDU-KG и два алгоритма анализа данных кибербразведки: алгоритм BridgeBuild для построения межонтологических связей и алгоритм DualLoopContext для двухконтурного извлечения нормативного и доказательного контекста. Модель реализована в виде ориентированного типизированного графа свойств с атрибутами и объединяет БДУ ФСТЭК России, базы знаний

MITRE ATT & CK, MITRE D3FEND, CVE, CWE, CAPEC и CTI-отчеты.

Оценка алгоритма BridgeBuild на тестовой выборке из 394 пар показала $F_1 = 0{,}83$ для M_{MLP} и M_{XGB}. Алгоритм BridgeBuild при использовании M_{XGB} превысил лучший из рассмотренных альтернативных методов по F_1 на 0,03 и сократил число LLM-вызовов приблизительно в семь раз в тестовом протоколе.

В основной серии на 750 вопросах графовые конфигурации обеспечили наибольший выигрыш в многошаговых сценариях. В BDU-QA рост EM с 0,48 до 0,77; в Crosswalk-QA рост с 0,21 до 0,63. Автоматические межонтологические связи M_2 позволили получить значение EM = 0,56 при EM = 0,63 для экспертных межонтологических связей M_1.

Дополнительный статистический замер подтвердил устойчивое преимущество графового извлечения над алгоритмом BM25 по Entity Recall@50, в том числе после маскирования идентификаторов. Полученные выводы относятся к исследованным источникам и сценариям экспериментов и не означают универсального превосходства графового подхода.

Полное независимое преимущество графового извлечения по дополнительной серии TTP-QA не установлено из-за зависимости эталона и доступного слоя связей. Проверка качества на новых документах требует отдельного протокола, исключающего использование эталонных связей при извлечении и контролирующего пересечение документов и их дубликатов.

Практическая значимость определяется возможностью применения разработанной системы для поддержки принятия решений аналитиками SOC при разборе CTI-отчетов, сопоставлении TTP злоумышленников с угрозами БДУ, формировании рекомендаций по мерам защиты и описания инцидентов ИБ с использованием международных таксономий. Полная оценка риска ИБ, промышленная интеграция и апробация в действующем SOC остаются направлениями дальнейшей работы.

Литература

1. **Tounsi W., Rais H.** A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, 2018, vol. 72, pp. 212–233. doi:10.1016/j.cose.2017.09.001
2. **Мещеряков Р. В., Исхаков С. Ю.** Исследование индикаторов компрометации для средств защиты информационных и киберфизических систем. *Вопросы кибербезопасности*, 2022, № 5(51), с. 82–99. doi:10.21681/2311-3456-2022-5-82-99
3. **Zhang J., Bu H., Wen H., Liu Y., Fei H., Xi R., Li L., Yang Yu., Zhu H., Meng D.** When LLMs meet cybersecurity: a systematic literature review. *Cybersecurity*, 2025, vol. 8, pp. 1–55. doi:10.1186/s42400-025-00361-w
4. **Котенко И. В., Абраменко Г. Т.** Использование больших языковых моделей для поиска угроз кибербезопасности на основе методов глубокого обучения: анализ современных исследований. *Правовая информатика*, 2024, № 3, с. 32–42. doi:10.24412/1994-1404-2024-3-32-42
5. **Würsch M., Kucharavy A., Percia David D., Mermoud A.** LLM-based entity extraction is not for cybersecurity. *Extraction and Evaluation of Knowledge Entities from Scientific Documents (EEKE2023) and AI+ Informetrics (AII2023)*, 2023, vol. 3451, pp. 26–32.
6. **Lewis P., Perez E., Piktus A., Petroni F., Karpukhin V., Goyal N., Küttler H., Lewis M., Yih W., Rocktäschel T., Riedel S., Kiela D.** Retrieval-augmented generation for knowledge-intensive NLP tasks. *Advances in Neural Information Processing Systems*, 2020, vol. 33, pp. 9459–9474. doi:10.48550/arXiv.2005.11401
7. **Rajapaksha S., Rani R., Karafili E.** A RAG-based question-answering solution for cyber-attack investigation and attribution. *European Symposium on Research in Computer Security*, LNCS, vol. 15264, Cham, Springer Nature Switzerland, 2024, pp. 238–256. https://doi.org/10.1007/978-3-031-82362-6_15
8. **Edge D., Trinh H., Cheng N., Bradley J., Chao A., Mody A., Truitt S., Larson J.** From local to global: A graph RAG approach to query-focused summarization. *arXiv:2404.16130*, 2024. doi:10.48550/arXiv.2404.16130
9. **Луцкович А. И., Васильев В. И., Вульфин А. М., Кириллова А. Д., Сулавко А. Е.** Автоматизированная система анализа слабоструктурированных данных киберразведки с использованием больших языковых моделей. *Информационно-управляющие системы*, 2025, № 2, с. 50–67. doi:10.31799/1684-8853-2025-2-50-67, EDN: QFQTPU
10. **Hu Y., Lei Z., Zhang Z., Pan B., Ling C., Zhao L.** GRAG: Graph Retrieval-Augmented Generation. *Findings of the Association for Computational Linguistics: NAACL 2025*, 2025, pp. 4145–4157. doi:10.18653/v1/2025.findings-naacl.232
11. **Zhu X., Xie Y., Liu Y., Li Y., Hu W.** Knowledge Graph-Guided Retrieval Augmented Generation. *Proceedings of the 2025 Conference of the Nations of the Americas Chapter of the Association for Computational Linguistics: Human Language Technologies*, 2025, pp. 8912–8924. doi:10.18653/v1/2025.naacl-long.449
12. **Манжосов А. В., Болодурина И. П.** Метод автоматизированного построения графа знаний связности формальных моделей норм и требований в области информационной безопасности. *Вестник УрФО. Безопасность в информационной сфере*, 2022, № 2(44), с. 49–56. doi:10.14529/secur220207

13. **Sikos L. F.** Cybersecurity knowledge graphs. *Knowledge and Information Systems*, 2023, vol. 65, no. 9, pp. 3511–3531. doi:10.1007/s10115-023-01860-3
14. **Chepurova A., Kuratov Y., Bulatov A., Burtsev M.** Prompt me one more time: A two-step knowledge extraction pipeline with ontology-based verification. *Graph-based Methods for Natural Language Processing: Proceedings of TextGraphs-17,* 2024, pp. 61–77. doi:10.18653/v1/2024.textgraphs-1.5
15. **Fieblinger R., Alam M. T., Rastogi N.** Actionable cyber threat intelligence using knowledge graphs and large language models. *2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Vienna, Austria, IEEE, 2024, pp. 100–111. doi:10.1109/EuroSPW61312.2024.00018
16. **Wu Z., Tang F., Zhao M., Li Y.** KGV: Integrating Large Language Models with knowledge graphs for cyber threat intelligence credibility assessment. *IEEE Transactions on Mobile Computing*, 2026, pp. 1–16. doi:10.1109/TMC.2026.3692451
17. **Peng B., Zhu Y., Liu Y., Bo X., Shi H., Hong C., Zhang Y., Tang S.** Graph Retrieval-Augmented Generation: A survey. *ACM Transactions on Information Systems*, 2025, vol. 44, no. 2, pp. 1–52. doi:10.1145/3777378
18. **Kurniawan K., Kiesling E., Ekelhart A.** CyKG-RAG: Towards knowledge-graph enhanced retrieval augmented generation for cybersecurity. *International Semantic Web Conference (ISWC): CEUR Workshop Proceedings*, Baltimore, USA, November 2024, vol. 3950, pp. 1–14.
19. **Rahman M. R., Hezaveh R. M., Williams L.** What are the attackers doing now? Automating cyberthreat intelligence extraction from text on pace with the changing threat landscape: A survey. *ACM Computing Surveys*, 2023, vol. 55, no. 12, pp. 1–36. doi:10.1145/3571726
20. **Nour B., Pourzandi M., Qureshi R. K., Debbabi M.** Automa: Automated generation of attack hypotheses and their variants for threat hunting using knowledge discovery. *IEEE Transactions on Network and Service Management*, 2024, vol. 21, no. 5, pp. 5178–5196. doi:10.1109/TNSM.2024.3378972
21. **Huang L., Xiao X.** CTIKG: LLM-powered knowledge graph construction from cyber threat intelligence. *First Conf on Lang Modeling*, 2024, pp. 1–24.
22. **Cheng Y., Bajaber O., Tsegai S. A., Song D., Gao P.** CTINexus: Automatic cyber threat intelligence knowledge graph construction using Large Language Models. *2025 IEEE 10th European Symposium on Security and Privacy (EuroS&P)*, Venice, Italy, 30 June–04 July 2025, IEEE, 2025, pp. 923–938. doi:10.1109/EuroSP63326.2025.00057
23. **Hu Y., Zou F., Han J., Sun X., Wang Y.** LLM-TIKG: Threat intelligence knowledge graph construction utilizing large language model. *Computers & Security*, 2024, vol. 145, pp. 103999. doi:10.1016/j.cose.2024.103999
24. **Es S., James J., Espinosa-Anke L., Schockaert S.** RAGAS: Automated evaluation of Retrieval Augmented Generation. *Proceedings of the 18th Conference of the European Chapter of the Association for Computational Linguistics: System Demonstrations*, 2024, pp. 150–158. doi:10.18653/v1/2024.eacl-demo.16

UDC 004.056.53
doi:10.31799/1684-8853-2026-5-37-55
EDN: IULELD

A model and algorithms for cyber threat intelligence data analysis based on a knowledge graph

A. M. Vulfin[a], Dr. Sc., Tech., Professor, orcid.org/0000-0001-5857-2413, vulfin.alexey@yandex.ru
V. I. Vasilyev[a], Dr. Sc., Tech., Professor, orcid.org/0000-0002-6105-5481
A. I. Lutskovich[a], Senior Lecturer, orcid.org/0009-0000-7257-6947
A. D. Kirillova[a], PhD, Tech., Associate Professor, orcid.org/0009-0000-4164-2526
[a]Ufa University of Science and Technology, 12, K. Marx St., 450008, Ufa, Russian Federation

Introduction: Traditional retrieval-augmented generation systems based on vector search on chunks are limited in multi-step mapping of cyber threat intelligence reports, national threat classifiers, and international knowledge bases. **Purpose:** To develop and give experimental evaluation of a knowledge graph model and algorithms for cross-ontology alignment and dual-loop context extraction in the analysis of cyber threat intelligence data. **Methods:** The model is implemented as a directed, typed graph of properties with a set of attributes that integrates a national threat database, international knowledge bases on attack tactics and techniques, protective measures, vulnerability registries, software weakness classifiers, attack pattern catalogs, and a corpus of cyber threat intelligence reports. The achievement of the goal is assessed by quantitative metrics when constructing cross-ontological connections and analyzing the capabilities of the question-answer system. **Results:** We develop an algorithm for constructing cross-ontological links with verification of semantic similarity, domain constraints, and alignment with correctness control using large language models. We implement a dual-loop context extraction algorithm that combines a knowledge graph and an evidential layer of text fragments. We propose a method for analyzing cyber threat intelligence data based on a knowledge graph model, algorithms for constructing cross-ontological links and context extraction. On the test set, the trained classifier of cross-ontological relationships has achieved the metric value F1 = 0.83. The introduced expert connections have increased the value of the EM metric of complete coincidence of the predicted and reference set of identifiers from 0.34 to 0.63, automatic connections have ensured the value of the EM = 0.56. A significant increase in the Entity Recall@50 metric has been obtained relative to text search: 0.5225, and after hiding the identifiers of tactics and techniques, the increase equals 0.5467. **Practical relevance:** The method is designed to support decision-making by analysts at the Information Security Operations Center when comparing cyber threat intelligence reports with national and international knowledge bases. **Discussion:** Cross-ontological links improve the verifiability of the answer by aligning with correctness control, and the layer of summary descriptions of the graph communities increases the consistency of the answer with the extracted context with a moderate decrease in accuracy.

Keywords – knowledge graph, graph retrieval-augmented generation, cyber threat intelligence data, tactics and techniques, ontology matching, entity alignment, large language models, MITRE ATT & CK, MITRE D3FEND, BDTV FSTEC.

For citation: Vulfin A. M., Vasilyev V. I., Lutskovich A. I., Kirillova A. D. A model and algorithms for cyber threat intelligence data analysis based on a knowledge graph. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 5, pp. 37–55 (In Russian). doi:10.31799/1684-8853-2026-5-37-55, EDN: IULELD

References

1. Tounsi W., Rais H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, 2018, vol. 72, pp. 212–233. doi:10.1016/j.cose.2017.09.001
2. Meshcheryakov R. V., Iskhakov S. U. Study of compromet-ation indicators for improvement of information and cyber-physical systems protection facilities. *Cybersecurity Issues*. 2022, no. 5(51), pp. 82–99 (In Russian). doi:10.21681/2311-3456-2022-5-82-99
3. Zhang J., Bu H., Wen H., Liu Y., Fei H., Xi R., Li L., Yang Yu., Zhu H., Meng D. When LLMs meet cybersecurity: A systematic literature review. *Cybersecurity*, 2025, vol. 8, pp. 1–55. doi:10.1186/s42400-025-00361-w
4. Kotenko I. V., Abramenko G. T. Using large language models for cyber threat hunting based on deep learning methods: Analysis of modern research. *Legal Informatics*, 2024, no. 3, pp. 32–42 (In Russian). doi:10.24412/1994-1404-2024-3-32-42
5. Würsch M., Kucharavy A., Percia David D., Mermoud A. LLM-based entity extraction is not for cybersecurity. *Extraction and Evaluation of Knowledge Entities from Scientific Documents (EEKE2023) and AI+ Informetrics (AII2023)*, 2023, vol. 3451, pp. 26–32.
6. Lewis P., Perez E., Piktus A., Petroni F., Karpukhin V., Goyal N., Küttler H., Lewis M., Yih W., Rocktäschel T., Riedel S., Kiela D. Retrieval-augmented generation for knowledge-intensive NLP tasks. *Advances in Neural Information Processing Systems*, 2020, vol. 33, pp. 9459–9474. doi:10.48550/arXiv.2005.11401
7. Rajapaksha S., Rani R., Karafili E. A RAG-based question-answering solution for cyber-attack investigation and attribution. *European Symposium on Research in Computer Security*, LNCS, vol. 15264, Cham, Springer Nature Switzerland, 2024, pp. 238–256. https://doi.org/10.1007/978-3-031-82362-6_15
8. Edge D., Trinh H., Cheng N., Bradley J., Chao A., Mody A., Truitt S., Larson J. From local to global: A graph RAG approach to query-focused summarization. *arXiv:2404.16130*, 2024. doi:10.48550/arXiv.2404.16130
9. Lutskovich A. I., Vasiluev V. I.., Vulfin A. M., Kirillova A. D., Sulavko A. E. Automated system for analyzing weakly structured threat intelligence data using large language models. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2025, no. 2, pp. 50–67 (In Russian). doi:10.31799/1684-8853-2025-2-50-67, EDN: QFQTPU
10. Hu Y., Lei Z., Zhang Z., Pan B., Ling C., Zhao L. GRAG: Graph Retrieval-Augmented Generation. *Findings of the Association for Computational Linguistics: NAACL 2025*, 2025, pp. 4145–4157. doi:10.18653/v1/2025.findings-naacl.232
11. Zhu X., Xie Y., Liu Y., Li Y., Hu W. Knowledge Graph-Guided Retrieval Augmented Generation. *Proceedings of the 2025 Conference of the Nations of the Americas Chapter of the Association for Computational Linguistics: Human Language Technologies*, 2025, pp. 8912–8924. doi:10.18653/v1/2025.naacl-long.449
12. Manzhosov A. V., Bolodurina I. P. Automated construction of the knowledge graph of reference to formal models of norms and treatments in the field of information security method. *Journal of the Ural Federal District. Information Security*, 2022, no. 2(44), pp. 49–56 (In Russian). doi:10.14529/secur220207
13. Sikos L. F. Cybersecurity knowledge graphs. *Knowledge and Information Systems*, 2023, vol. 65, no. 9, pp. 3511–3531. doi:10.1007/s10115-023-01860-3
14. Chepurova A., Kuratov Y., Bulatov A., Burtsev M. Prompt me one more time: A two-step knowledge extraction pipeline with ontology-based verification. *Graph-based Methods for Natural Language Processing: Proceedings of TextGraphs-17,* 2024, pp. 61–77. doi:10.18653/v1/2024.textgraphs-1.5
15. Fieblinger R., Alam M. T., Rastogi N. Actionable cyber threat intelligence using knowledge graphs and large language models. *2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Vienna, Austria, IEEE, 2024, pp. 100–111. doi:10.1109/EuroSPW61312.2024.00018
16. Wu Z., Tang F., Zhao M., Li Y. KGV: Integrating Large Language Models with knowledge graphs for cyber threat intelligence credibility assessment. *IEEE Transactions on Mobile Computing*, 2026, pp. 1–16. doi:10.1109/TMC.2026.3692451
17. Peng B., Zhu Y., Liu Y., Bo X., Shi H., Hong C., Zhang Y., Tang S. Graph Retrieval-Augmented Generation: A survey. *ACM Transactions on Information Systems*, 2025, vol. 44, no. 2, pp. 1–52. doi:10.1145/3777378
18. Kurniawan K., Kiesling E., Ekelhart A. CyKG-RAG: Towards knowledge-graph enhanced retrieval augmented generation for cybersecurity. *International Semantic Web Conference (ISWC): CEUR Workshop Proceedings*, Baltimore, USA, November 2024, vol. 3950, pp. 1–14.
19. Rahman M. R., Hezaveh R. M., Williams L. What are the attackers doing now? Automating cyberthreat intelligence extraction from text on pace with the changing threat landscape: A survey. *ACM Computing Surveys*, 2023, vol. 55, no. 12, pp. 1–36. doi:10.1145/3571726
20. Nour B., Pourzandi M., Qureshi R. K., Debbabi M. Automa: Automated generation of attack hypotheses and their variants for threat hunting using knowledge discovery. *IEEE Transactions on Network and Service Management*, 2024, vol. 21, no. 5, pp. 5178–5196. doi:10.1109/TNSM.2024.3378972
21. Huang L., Xiao X. CTIKG: LLM-powered knowledge graph construction from cyber threat intelligence. *First Conf on Lang Modeling*, 2024, pp. 1–24.
22. Cheng Y., Bajaber O., Tsegai S. A., Song D., Gao P. CTINexus: Automatic cyber threat intelligence knowledge graph construction using Large Language Models. *2025 IEEE 10th European Symposium on Security and Privacy (EuroS&P)*, Venice, Italy, 2025, IEEE, 2025, pp. 923–938. doi:10.1109/EuroSP63326.2025.00057
23. Hu Y., Zou F., Han J., Sun X., Wang Y. LLM-TIKG: Threat intelligence knowledge graph construction utilizing large language model. *Computers & Security*, 2024, vol. 145, pp. 103999. doi:10.1016/j.cose.2024.103999
24. Es S., James J., Espinosa-Anke L., Schockaert S. RAGAS: Automated evaluation of Retrieval Augmented Generation. *Proceedings of the 18th Conference of the European Chapter of the Association for Computational Linguistics: System Demonstrations*, 2024, pp. 150–158. doi:10.18653/v1/2024.eacl-demo.16