ЖУРНАЛ НАУЧНЫЙ СПЕКТР

ISSN 3033-6643

№8
2026

РОССИЙСКИЙ НАУЧНЫЙ ЖУРНАЛ
ПО ПОЛНОМУ СПЕКТРУ НАПРАВЛЕНИЙ НАУКИ



Издается ООО Развитие
Россия, Казань

OPEN ACCESS

SCIENCESPECTRUM.RU

РАЗВИТИЕ

НАУЧНЫЙ СПЕКТР

№8 2026

Казань – 2026

Научный спектр. №8 2026г. – Казань: Издательство Развитие, 2026. – 38.

ISSN 3033-6643 (online)

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (реестровая запись от 15.07.2025 серия ПИ № ФС77-89760).

Журнал размещен в открытом бесплатном доступе на сайте www.sciencespectrum.ru

В журнале отражены материалы по теории и практике направлений науки, наиболее интенсивно развивающихся в настоящее время. Представлены труды ученых и специалистов вузов, институтов РАН, организаций, учреждений и предприятий, представителей органов власти.

Материалы журнала будут полезны преподавателям, научным работникам, специалистам научных предприятий, организаций и учреждений, а также аспирантам, магистрантам и студентам.

 © Развитие, 2026 г.

СОДЕРЖАНИЕ

2.1 – СТРОИТЕЛЬСТВО И АРХИТЕКТУРА

Андреев Ю.Н. Эвакуация населения в военное время: Отдельные аспекты исторического опыта 5

Казаков Ю. Н., Дзекун Д.Д., Бакулова Т. С. Вариантное проектирование и оптимизация возведения светопрозрачного купола над внутренним двором корпуса СПБГАСУ 13

2.3 – ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

Павлов Д.В., Галанина Н.А. Метрики оценки защитного контура llm/rag-систем: безопасность, полезность и ресурсы 18

5.9 – ФИЛОЛОГИЯ

Кондрашова Д.Г. Структурные модели терминов цифровых технологий в современном английском языке 28

THE RELEASE MAINTENANCE

2.1 – CIVIL ENGINEERING AND ARCHITECTURE

Andreev Yu.N. Evacuation of the population in wartime: Selected aspects of historical experience 5
Kazakov Yu. N., Dzekun D. D., Bakulova T.S. Variant design and optimization of the construction of a translucent dome over the inner courtyard of the SPBGASU building 13

2.3 – INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Pavlov D.V., Galanina N.A. Metrics for evaluating the protective contour of llm/rag systems: security, utility and resources 18

5.9 – PHILOLOGY

Kondrashova D.G. Structural Models of Digital Technology Terms in Modern English 28

2.1. СТРОИТЕЛЬСТВО И АРХИТЕКТУРА

2.1.

Эвакуация населения в военное время: Отдельные аспекты исторического опыта

Андреев Ю.Н.
ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова»,
Чебоксары, Россия
e-mail: gochgu@mail.ru

Аннотация
Исследование направлено на обобщение вопроса эволюции отечественной доктрины подготовки и проведения эвакуации населения и материальных ценностей в военное время. Изучены вопросы подготовки и проведения эвакуации во время Великой Отечественной войны 1941-1945 гг., а также основные положения меняющейся доктрины Гражданской обороны СССР по эвакуации населения в военное время. В статье даются предложения по модернизации подходов к подготовке и проведению эвакуации крупных организаций в военное время. Автор считает возможным использование исторического опыта для дальнейшего совершенствования работы органов управления гражданской обороны, осуществляющих подготовку и проведение эвакуационных мероприятий в военное время.

Ключевые слова: *гражданская оборона, эвакуация в военное время.*

В современных военных конфликтах (в том числе так называемых «гибридных войнах») гражданское население и тыловые объекты всё больше и больше становятся явной, намеренной целью противника для уничтожения с применением боевых средств поражения. В этих условиях растут требования к гражданской обороне, вынужденной адекватно реагировать на новые угрозы, связанные с изменением тактики ведения боевых действий. Отмечается «рост внешних и внутренних угроз», которые требуют пересмотра доктрины эвакуационных мероприятий [1]. Вопрос эвакуации населения в военное время стал актуальнее, чем во времена «холодной войны», а особенно – эвакуация организаций из крупных городов в безопасные районы, которая позволяет хозяйствующим субъектам даже в условиях военного времени продолжать экономическую деятельность, без чего невозможно добиться максимального поддержания обороноспособности страны. Укрытие в защитных сооружениях гражданской обороны как способ защиты не в состоянии охватить необходимое количество населения, по причине того, что изначально указанные объекты создавались исключительно для избранных предприятий и учреждений, и, во-вторых, невозможно и нецелесообразно создавать эти строительные объекты «для всех и вся». Россия находится в состоянии, когда большинство организаций (работающее и обучающееся население) и жилых кварталов (неработающее население) защитными сооружениями гражданской обороны не располагают. Когда более 75 % населения не может быть защищено способом укрытия, единственным способом его защиты априори остается эвакуация.

В статье исследуются вопросы исторического развития отечественной доктрины эвакуации гражданского населения в условиях военного времени. Особое внимание уделяется эвакуации крупных организаций, расположенных в крупных

категорированных городах и переносящих свою экономическую деятельность в запланированные безопасные районы.

Эвакуация населения в военное время: исторический опыт

Главной задачей эвакуации в военное время является минимизация людских и материальных потерь как залог сохранения мобилизационных ресурсов и производственных мощностей страны – воюющей стороны. Отмечено, что эвакуация, планируемая к проведению в условиях военного времени, когда в отношении населения возникает угроза военной агрессии, требует четкой регламентации взаимоувязанных действий органов управления [2].

В нашей стране планирование эвакуации населения и предприятий при военной угрозе началось осуществляться после образования Союза Советских Социалистических Республик (СССР): первым актом стало Положение «О вывозе из угрожаемых неприятелем районов ценного имущества, учреждений, предприятий и людского контингента», утвержденное 3 августа 1923 года Советом труда и обороны СССР, а 7 мая 1926 года появился первый план эвакуации, разработанный Наркоматом путей сообщения СССР [3].

Неизбежной стала эвакуация в годы Великой Отечественной войны (ВОВ), накануне которой, несмотря на неоднократные обращения экспертов, советским руководством эвакуация де-юре не признавалась, потому что в СССР «господствовала военная доктрина, базировавшаяся на идее ответного сокрушительного удара с целью разгрома агрессора и перенесения боевых действий на его территорию уже в первые дни войны», а в «мобилизационном плане на случай войны массовые эвакуационные перевозки не предусматривались» [4]. В середине мая 1941 года Генеральный штаб Рабоче-Крестьянской Красной Армии (ГШ РККА) предписал западным военным округам разработать планы эвакуации, но последние сделать это не успели. Продвижение немецко-фашистских войск сделало эвакуацию «нужной», в связи с чем 24 июня 1941 г. постановлением ЦК ВКП(б) и СНК СССР был создан Совет по эвакуации; основным нормативным актом стало Постановление ЦКВКП(б) и СНК СССР от 27 июня 1941 г. «О порядке вывоза и размещения людских контингентов и ценного имущества» [3]. В июле 1941 г. ГШ РККА предложил Совету по эвакуации «дать указания соответствующим наркоматам на проработку плана вывоза подведомственных им предприятий, определив для них заранее эвакобазы» [3]. Однако главному эвакуационному органу страны не удалось справиться с поставленной задачей. Вопросы эвакуации стали решаться лишь после вступления в силу постановления Государственного Комитета Обороны СССР (ГКО) от 3 июля 1941 года № 4 «О программе выпуска артиллерийского и стрелкового вооружения, плане эвакуации заводов Наркомвооружения и создании новых баз в Поволжье, на Урале и в Сибири».

Признано, что в годы ВОВ органы власти СССР организовали и провели беспрецедентные по масштабу и характеру эвакуационные мероприятия, однако, при освещении истории эвакуации населения и предприятий СССР в 1941-1942 гг. отмечено, что в начале ВОВ в ходе проведения эвакуации возникали проблемы даже по реализации директив свыше [4, 5, 6, 7, 8, 9]. Последствиями отсутствия в СССР утвержденных планов эвакуации стали хаос, бегство (включая руководящий состав советских органов власти), проявления паники и саботажа (в РСФСР законодательно признаваемого опасным деянием, угрожающим национальной безопасности [10]). Тем не менее, с июня по август 1941 года из прифронтовых областей СССР в восточном

направлении было «эвакуировано 1350 крупных предприятий» [3] (с эвакоконтингентом не менее 10 млн. чел. – *авт.*).

Опыт ВОВ показал, что советскому правительству приходилось в экстренном порядке принимать нормативные акты, регламентирующие проведение эвакуационных мероприятий, и создавать соответствующие органы управления: в частности, 5 июля 1941 г. – Постановление СНК СССР «О порядке эвакуации населения в военное время», а также «Положение об эвакопункте», утверждённое Политбюро ЦК ВКП (б). Надо признать, что эвакуационный механизм сформировался достаточно быстро: был выработан четкий порядок организации эвакуационных перевозок, а наркоматы заблаговременно представляли в СПЭ заявки по каждому предприятию, подлежавшему перебазированию в «эвакобазы».

Указанная экстренность принятия актов часто приводила к ошибкам. Так, Постановление ГКО от 11 июля 1941 года «Об эвакуации промышленных предприятий» обязывало Наркомат путей сообщения выделить более 40 тыс. вагонов. Де-факто оказалось, что потребность в указанном виде транспорта была в разы больше, т.е. расчеты были сильно занижены; к тому же для эвакуации каждого предприятия требовалось отдельное распоряжение – как итог, оперативное время было полностью упущено.

Следует отметить, что в октябре 1941 года сложилась катастрофическая ситуация, когда, с началом немецкой операции «Тайфун» (наступление на Москву), вышло постановление ГКО «Об эвакуации столицы СССР г. Москвы» и распространились слухи о сдаче столицы – среди населения возникла массовая паника: сотни тысяч человек пытались выехать из Москвы; началась массовая эвакуация предприятий из Московского региона (было вывезено более 500 предприятий и более 500 тыс. работников и членов их семей); немцы заняли Харьков и вторглись в Донбасс – по причине неудачной планировки пропускной способности эвакуационные потоки столкнулись, что привело к железнодорожному коллапсу («куйбышевская пробка»), «разрулить» который удалось только через четыре месяца (в частности, на узлах 20 станций уложили дополнительные пути, чтобы составы могли разъезжаться и принимать больше вагонов).

Запуск производства продукции эвакуированных предприятий на местах осуществлялся путем преодоления крупных проблем, но благодаря усилиям смежных ведомств и энтузиазму директоров заводов («маленьких Сталинов») их абсолютное большинство удалось наладить на необходимые мощности. Существенную помощь оказали заводам местные власти, в частности, по решению кадрового вопроса. В отдельных случаях происходило слияние местных и эвакуированных предприятий: например, челябинский Уралвагонзавод принял 11 предприятий, включая Харьковский танковый завод № 183, и стал Уральским танковым заводом им. Коминтерна (предприятие за годы ВОВ выпустило более 25 тыс. танков Т-34 или половину от общего количества) – результат успешного восстановления и функционирования эвакуированного предприятия здесь налицо.

Обобщённый опыт проведения эвакуации предприятий во время ВОВ показал, что только благодаря успешным эвакуационным мероприятиям удалось сохранить экономический потенциал СССР, создать более чем эффективную промышленность в глубоком тылу и обеспечить достаточно большие объёмы выпуска оборонной продукции. Особенность проведения эвакуации в годы ВОВ заключалась в том, что угроза исходила со стороны Запада (наступающего фронта), поэтому в эвакуируемый контингент сначала сосредотачивался в узловом центре (как правило, на железнодорожной станции), откуда производился поэтапный (по принципу

приоритетности) вывоз в составе эвакоэшелонов в направлении «Восток» – именно таким образом прифронтовые регионы «опустошались», эвакуируемые предприятия прибывали в глубокий тыл (безопасный район), где возобновляли производственную деятельность, максимально сохраняя мобилизационные ресурсы страны.

По времени: в первые три недели фашистские войска продвигались со скоростью до 30 км в день – на подготовку к эвакуации крупных городов (Киев, Минск и другие) был запас не менее трёх суток, несмотря на периодические авиабомбардировки.

По территории: зоной опасности стала вся западная территория СССР до Москвы (примерно 1000 км от пограничной линии), а сплошным безопасным районом стала центральная часть СССР глубиной 3000 км и шириной 2000 км.

По транспортному обеспечению: с июня по декабрь 1941 года для нужд эвакуации предприятий и населения было задействовано около 1,5 млн. вагонов или примерно 30 тыс. поездов, а также автотранспорт.

Всего за годы ВОВ, по разным оценкам, из запада на восток СССР было эвакуировано до 25 млн. чел., в том числе 18 млн. работников эвакуированных предприятий и членов их семей.

Общий итог: несмотря на возникшие проблемы, эвакуационные органы СССР за годы ВОВ в целом обеспечили необходимые условия для проведения эвакуации и размещения населения, его трудоустройство, обеспечение продуктами питания и предметами первой необходимости.

Эвакуация в военное время: послевоенное развитие доктрины

31 октября 1949 года Совет Министров (Совмин) СССР утвердил Положение о Местной противовоздушной обороне (МПВО), в соответствии с которым на всей территории СССР создавались региональные и местные управления МПВО. Положение также расширило список категорированных городов. Однако эта доктрина работала на случай применения противником фугасных, зажигательных, химических авиабомб, и предполагала «выбор средств и способов защиты населении», не совсем эффективных при атомной угрозе (укрытие, в том числе, в переоборудованных подвалах). Лишь поняв «неизбежность применения атомного оружия в грядущей войне, советская доктрина защиты населения приступила к поискам новых мер», и 29 июня 1955 года было принято постановление «О мероприятиях по повышению готовности местной противовоздушной обороны страны к защите населения и промышленных объектов от атомного оружия», а 30 июня 1955 года – постановление «О мероприятиях по обеспечению медицинской помощи в условиях применения атомного оружия», обязывающее исполнительные органы советских республик разработать и представить в МВД СССР «планы эвакуации пораженных из городов-пунктов». Укрытие в защитных сооружениях оставалось основным способом защиты людей, хотя «всесоюзный штаб был вынужден признать, что концентрация людей в городах, даже несмотря на заблаговременное и качественное выполнение всех инженерно-технических мероприятий, все равно приведет к многочисленным жертвам среди мирного населения» [11].

К сожалению, директивы по вопросам эвакуации не выполнялись, в связи с чем 15 октября 1955 года Министр внутренних дел С.Н. Круглов приказал до 1 января 1956 года «закончить разработку планов эвакуации детей, нетрудоспособного населения и транспортабельных больных из городов-пунктов с учетом <…> потребного количества транспорта» [11]. Новый Министр Н.П. Дудоров, назначенный 31 января 1956 года, поставил задачу оценить реальное положение дел в системе МПВО страны. Проверки

выявили ряд нарушений, в частности, план эвакуации Тбилиси не предусматривал места посадки людей на железнодорожный транспорт, а в некоторых областях РСФСР разработка эвакуационных планов не была завершена даже в 1957 году. Проверки МВД СССР позволили сделать вывод: на всех уровнях начальники МПВО (председатели исполнительных комитетов) республик, областей и городов не уделяли должного внимания вопросам защиты населения, полностью делегируя задачи штабам МПВО, которые, не обладая соответствующими полномочиями, априори не могли организовать взаимодействие эвакуационных комиссий и организаций, что дало бы конкретные результаты; разработанные планы эвакуации носили формальный характер и не обладали достоверностью и детализацией.

В то же время у потенциального противника дела шли куда лучше. Необходимость заблаговременной подготовки к эвакуации хорошо понимали немецкие эксперты, получившие уроки Второй мировой войны. В 1956 году глава управления гражданской обороны ФРГ Эрих Хампе (в годы ВОВ – генерал фашистских войск) писал о планировании эвакуации «определенных категорий населения из районов, подвергающихся особой опасности, в заранее подготовленные к их приему защитные зоны» [12]. Отдельные советские авторы отмечали ответственный подход западных стран к вопросам гражданской обороны: «В США и ряде европейских стран разработаны планы защиты населения крупных городов, предусматривающие проведение эвакуации», для обеспечения «эвакуации в планах (и на учениях) предусматривается использование всех видов и средств транспорта» [13].

В СССР же в период с 1955 до 1961 годы основным способом защиты населения в условиях атомной атаки считалось укрытие в защитных сооружениях, хотя де-факто имеющийся фонд мог вместить лишь несколько процентов населения – предполагалось выкопать огромное количество простейших укрытий. Более того, 30 декабря 1959 года вышло постановление Совмина СССР «О прекращении затрат на проведение мероприятий МПВО», в соответствии с которым строительство защитных сооружений гражданской обороны было заморожено.

13 июля 1961 года Совмин СССР утвердил Положение о гражданской обороне (ГО) СССР, которое отнесло к числу основных задач гражданской обороны разработку планов эвакуации из крупных городов. О.В. Толстиков (в 1961-1965 гг. – начальник штаба гражданской обороны СССР) в книге «Гражданская оборона в современной войне» (1962) писал: «… гражданская оборона СССР считает более эффективным способом защиты населения его рассредоточение на большой территории» [11]. Авторы брошюры «Эвакуация городов – способ защиты от ядерного оружия» (1965), считали, что в ядерной войне удары «будут наноситься по городам», а в условиях страны, «имеющей обширную территорию и сравнительно большие расстояния между крупными городами, одним из эффективных способов защиты людей будет эвакуация из крупных городов» [13]. Совместное постановление ЦК КПСС и Совета Министров СССР от 4 ноября 1963 года «О мероприятиях по защите населения страны от оружия массового поражения» утвердило комплексный подход к защите населения: в мирное время убежища должны были возводиться только для рабочих смен предприятий, продолжающих работу в военное время; остальное население категорированных городов подлежала эвакуации в загородную зону [11]. Однако практика выявила проблемы: в 1967 году начальник ГО СССР В.И. Чуйков провёл учение по эвакуации Москвы и Московской области – несмотря на то, что учение длилось три месяца, поставленные учебные задачи так и не были до конца решены.

Наставление по рассредоточению и эвакуации населения (1971) признало, что «заблаговременное проведение рассредоточения и эвакуации позволяет вывести

основную массу населения в загородную зону из-под возможных ударов противника и уберечь его от поражения», а предприятия «могли обеспечить восстановление и бесперебойную работу отечественной промышленности даже в условиях ядерной войны» [11]. Был установлен вариативный подход к планированию: общая эвакуация в сжатые сроки, растянутая по времени поэтапная эвакуация, «гибкий» переход к другому плану в зависимости от изменений обстановки и т.д.

Но уже в 1972 году начальник ГО СССР А.Т. Алтунин утверждал, что главная задача ГО – быть готовой «укрыть все население с помощью защитных сооружений», а в книге «Гражданская оборона» (1974) – «обеспечить защитными сооружениями 100% населения страны» [11]. К 1986 году, стремясь учитывать не только «фактор внезапного удара», ГО СССР был введен так называемый «комбинированный способ рассредоточения и эвакуации»: отдельные категории населения должны были вывозиться в безопасную зону всеми имеющимися видами транспорта непосредственно в районы загородных зон; остальное население должно было выводиться в пешем порядке по кратчайшим маршрутам в промежуточные районы (для крупных городов с населением до миллиона человек устанавливались максимально допустимые сроки эвакуации в 16-24 часов).

Таким образом, главной задачей ГО СССР в послевоенный период – в эпоху так называемой «холодной войны» – была комплексная защита населения и материальных ценностей «в условиях крупномасштабной ракетно-ядерной войны», в том числе путем проведения «комбинированным» методом «в кратчайшие сроки» эвакуации десятков миллионов человек из сотен советских городов согласно планам эвакуации, расписанным по часам и минутам, и достоверность этих расчетов была неоднократно доказана в ходе проверок и учений по ГО.

Заключение

Таким образом, отечественный опыт показал, что успешно проведенная эвакуация в военное время обеспечивает сохранение мобилизационных ресурсов страны, без чего невозможно тыловое обеспечение вооруженных сил. Считаю, что доктрина эвакуации в военное время должна строиться с учетом исторического опыта, который позволяет делать следующие выводы.

Во-первых, отсутствие чётких планов эвакуации из крупных городов при непосредственной военной опасности может привести к крайне негативным последствиям в виде хаоса, массовой паники среди гражданского населения, бегства и саботажа со стороны должностных лиц органов власти и управления разных уровней, а в итоге – неоправданным человеческим жертвам и крупным экономическим потерям; причём взаимоувязанные планы должны быть разработаны на всех уровнях – федеральном, региональном, локальном.

Во-вторых, чрезвычайные ситуации, возникшие в ходе проведения эвакуационных мероприятий в 1941 году, оставили нам тревожные сигналы о том, что при осуществлении мер по транспортному обеспечению эвакуации необходимо предусмотреть все риски, для чего целесообразен вариативный подход к планированию; в любом случае, основные варианты планов эвакуации должны быть не только детально расписаны, но и тщательно апробированы в ходе учений и тренировок по гражданской обороне.

В-третьих, когда законодательство недостаточно регламентирует порядок работы эвакуационных органов крупных организаций, переносящих свою деятельность из категорированных городов в безопасные районы, создается риск несоответствия

требований законодательства существующим реалиям; основными причинами указанного несоответствия могут быть – как отсутствие актуальных документов, разрабатываемых органами местного самоуправления и самими организациями, так и недостаточный уровень подготовки личного состава эвакуационных органов указанных уровней.

В-четвертых, необходимо заблаговременно согласовать и утвердить планы взаимодействия муниципальных эвакуационных органов и органов управления эвакуируемых организаций – с учетом того, что эвакоконтингент крупных организаций в среднем составляет более десяти тысяч человек.

Список литературы:

1. Мануйло О.Л., Рыбаков А.В., Иванов Е.В., Копытов Д.О. О постановке задачи планирования и проведения эвакуационных мероприятий с применением агент-ориентированных моделей // Научные и образовательные проблемы гражданской защиты. 2024. № 3. С. 23-29.

2. Гущин И.А., Андреев Ю.Н., Кузьмин С.А. Проблемы подготовки и проведения эвакуации населения городов в безопасные районы // Проблемы безопасности и чрезвычайных ситуаций: научный информационный сборник. 2024. № 4. С. 85-91.

3. Ермолов А. Главная стратегическая операция: интервью / беседовала М. Якубович // Русский мир. 2020. С. 32-39.

4. Потёмкина М.Н. Эвакуация в годы Великой Отечественной войны на Урале: люди и судьбы. Магнитогорск: Магнитогорский государственный университет, 2002. 265 с.

5. Куманев Г.А. Война и эвакуация в СССР. 1941-1942 годы / Г.А. Куманев // Новая и новейшая история. 2006. № 6. С. 7-27.

6. Болокина Л.А. Эвакуация населения из прифронтовой полосы на территории Калининской области в 1942 г. / Л.А. Болокина // Российская история. 2022. № 3. С. 175-190.

7. Мазурицкий А.М. Эвакуация библиотечных фондов в годы Великой Отечественной войны / А.М. Мазурицкий, Р.Ф. Исламов // Вестник Казанского государственного университета культуры и искусств. 2019. № 4. С. 45-49.

8. Нечаев М.Г. Эвакуация научных, учебных и культурных учреждений в город Молотов (Пермь) во время Великой Отечественной войны / М.Г. Нечаев // Гуманитарные исследования. История и филология. 2022. № 5. С. 16–40.

9. Потёмкина М.Н. Особенности эвакуации заключенных в начальный период Великой Отечественной войны / М.Н.Потемкина, И.О. Колдомасов // Historia Provinciae – журнал региональной истории. 2022. Т. 6. № 4. С. 1210-1251.

10. Кузнецов А.П. Саботаж в российском уголовном законодательстве: история, перспективы законодательной регламентации // Пробелы в российском законодательстве. 2024. Т. 17. № 3. С. 121-126.

11. Феоктистов И. Эвакуация как средство защиты [Электронный ресурс]. URL: https://xn--b1ae4ad.xn--p1ai/blog/post (дата обращения 22.05.2026).

12. Хампе Э. Стратегия гражданской обороны / Э. Хампе; пер. с нем. М.А. Дубянского. М.: Изд. иностр. лит., 1958. 132 с.

13. Павлий Ю.Г., Цивилев М.П. Эвакуация населения городов – способ защиты от ядерного оружия. М.: ДОСААФ, 1965. 36 с.

Evacuation of the population in wartime: Selected aspects of historical experience

Andreev Yu.N.
The Federal State Educational Establishment of Higher Education "The Chuvash state university named after I. N. Ulyanov",
Cheboksary, Russia
e-mail: gochgu@mail.ru

Abstract

The research is aimed at generalizing the issue of the evolution of the national doctrine of the preparation and conduct of evacuation of the population and material assets in wartime. The issues of preparation and conduct of evacuation during the Great Patriotic War of 1941-1945, as well as the main provisions of the changing doctrine of Civil Defense of the USSR on the evacuation of the population during wartime are studied. The article provides proposals for modernizing approaches to the preparation and conduct of evacuation of large organizations during the war. The author considers it possible to use historical experience to further improve the work of civil defense management bodies involved in the preparation and conduct of evacuation measures during wartime.

Keywords: *civil defense, evacuation in wartime.*

Вариантное проектирование и оптимизация возведения светопрозрачного купола над внутренним двором корпуса СПБГАСУ

Казаков Ю. Н.[1], Дзекун Д. Д.[2], Бакулова Т. С.[3]
Санкт-Петербургский государственный архитектурно-строительный университет, Санкт-Петербург, Россия
[1]e-mail: kazin@lan.spbgasu.ru
[2]e-mail: darya.dzekun00@mail.ru
[3]e-mail: tan.volk.21012005@gmail.com

Аннотация

Работа посвящена вариантному проектированию и оптимизации возведения светопрозрачного купола над внутренним двором-колодцем корпуса Е Санкт-Петербургского государственного архитектурно-строительного университета (ул. Егорова, д. 5/8). Объект имеет размеры в плане 39,6 × 23,0 м (площадь 560 м², высота купола 7,7 м, угол ската 35°, поверхность покрытия ≈ 680 м². В основу положен патент RU 186423 U1 (2019) на купол с выдвижным полотном. Сравниваются три варианта: стальной каркас + ETFE (полный патентный), стальной каркас + сотовый поликарбонат, алюминиевый каркас + поликарбонат. Критерий оптимизации — минимум стоимости жизненного цикла при фиксированном качестве (сухость двора зимой и осенью, сохранение инсоляции, снижение коррозии металла на 3 %/год, сохранение 150 м² и 10 машиномест). Показано, что рабочим оптимумом является вариант «сталь + сотовый поликарбонат» (~5,6 млн руб., монтаж 7–9 суток с улицы без длительного закрытия стоянки). Полный патентный вариант со сматываемым ETFE-полотном целесообразен при необходимости летнего раскрытия. Приведены укрупнённые расчёты стоимости, трудоёмкости, схема монтажа и ожидаемый годовой эффект (экономия на уборке ≈ 280 тыс. руб./год).

Ключевые слова: *светопрозрачный купол; двор-колодец; вариантное проектирование; стальной каркас; сотовый поликарбонат; ETFE; оптимизация стоимости; монтаж без закрытия стоянки; патент RU 186423 U1; климат Санкт-Петербурга.*

Внутренние дворы-колодцы исторической застройки Санкт-Петербурга, как правило, используются под стоянку и транзитное движение. Открытое небо приводит к накоплению снега, листвы и мусора, ускоренной коррозии металлических элементов и необходимости регулярной уборки. Корпус Е СПбГАСУ на ул. Егорова, д. 5/8, имеет типичный двор-колодец размерами 39,6 × 23,0 м (560 м²). Высота окружающих стен ≈ 13 м. В настоящее время двор открыт, что создаёт сезонные эксплуатационные проблемы.

В 2019 г. сотрудниками кафедры технологии строительного производства СПбГАСУ (Казаков Ю. Н., Шахназаров С. С.) был получен патент на полезную модель RU 186423 U1 «Купол над внутренними дворами с выдвижным полотном» [1]. Идея предусматривает пирамидальный каркас с возможностью сматывания светопрозрачного полотна на бобины, что позволяет летом открывать двор. Однако до настоящего времени отсутствовал сравнительный инженерно-экономический анализ вариантов заполнения и каркаса применительно к конкретному объекту с учётом

климата Санкт-Петербурга, требований к монтажу без длительного закрытия стоянки и критерия минимума стоимости жизненного цикла.

Цель работы — вариантное проектирование и оптимизация возведения светопрозрачного купола над двором корпуса на ул. Егорова, 5/8. Задачи: определение геометрии, сравнение трёх конструктивных вариантов, расчёт стоимости и трудоёмкости, разработка схемы монтажа с улицы, выбор рабочего решения по критерию минимума капитальных и эксплуатационных затрат при заданном качестве.

2. Объект и исходные данные

Объект — внутренний двор корпуса Е СПбГАСУ (ул. Егорова, д. 5/8). Контур двора ломаный, размеры в плане 39,6 × 23,0 м, площадь 560 м^2. Принята пирамидальная форма купола с опиранием на существующие кровли стен. Высота купола от опорного контура до вершины — 7,7 м, угол ската — 35° (обеспечивает самостоятельный сход снега). Поверхность покрытия ≈ 680 м^2. Высота стен двора ≈ 13 м.

Натурные обследования (14.09.2026) подтвердили использование двора под стоянку и транзит, наличие открытого неба, сезонного заноса снегом и листвой [7]. Геометрия принята по существующему контуру без спрямления (контрольный обмер требуется перед рабочей документацией).

Требования к качеству (ограничения): двор остаётся сухим зимой и осенью; сохраняется инсоляция окон; снег сходит самостоятельно; коррозия металла во дворе снижается не менее чем на 3 %/год [5]; сохраняются ≈ 150 м^2 парковочной площади и 10 машиномест для преподавателей; монтаж выполняется преимущественно с улицы (ул. Егорова) без длительного закрытия стоянки.

3. Методы и варианты

Методы: геометрическое моделирование (пирамида на ломаном контуре), укрупнённый стоимостной расчёт по открытым ценам проката и зенитных фонарей Санкт-Петербурга 2026 г., расценкам ГЭСН 34 и 46 [6], оценка трудоёмкости, анализ монтажной схемы. Нормативная база: СП 20.13330.2016 [3], СП 17.13330.2017 [4], СП 28.13330 [5]. Технологические подходы соответствуют [2].

Рассмотрены три варианта:

V1 — стальной каркас (труба прямоугольная ≈ 21 т) + ETFE-полотно со сматыванием на бобины (полный патент RU 186423 U1);

V2 — тот же стальной каркас + сотовый поликарбонат 8–10 мм;

V3 — алюминиевый каркас + сотовый поликарбонат.

ПВХ в качестве несущего каркаса на пролёте 20–26 м исключён как неработоспособный.

4. Результаты сравнительного анализа

Стоимость (укрупнённо, млн руб., без НДС и проектных работ, цены СПб 2026) представлена в табл. 1.

Таблица 1 — Укрупнённая стоимость вариантов, млн руб.

Статья	**V1 (сталь+ETFE)**	**V2 (сталь+ПК)**	**V3 (Al+ПК)**
Каркас (материал + завод)	2,4	2,4	4,0
Заполнение	2,9	1,8	1,8
Монтаж и кран	1,3	1,1	1,2
Желоба, обогрев, узлы	0,3	0,3	0,3
Итого	**6,9**	**5,6**	**7,3**

Источники: прокат трубы ≈ 68 000 руб./т; ГЭСН 46-02-005-02; прайсы зенитных фонарей и поликарбоната.

Трудоёмкость представлена в табл. 2.

Таблица 2 — Трудоёмкость и сроки монтажа

Показатель	**V1**	**V2**	**V3**
Каркас, чел.-ч	720	720	540
Заполнение и механика, чел.-ч	320	210	230
Всего, чел.-ч	**1040**	**930**	**770**
Бригада, чел.	12–14	10–12	10–12
Календарный монтаж, сут	10–13	7–9	7–9

Преимущества и недостатки вариантов:

V1 максимально соответствует патенту, позволяет летнее раскрытие, минимальная масса заполнения; недостатки — высокая стоимость плёнки и механики, необходимость сервиса моторов, импортные комплектующие, обогрев коробов бобин.

V2 дешевле, доступен на рынке РФ, постоянно закрывает двор от осадков, держит снеговую нагрузку; недостатки — отсутствие раскрытия, возможное пожелтение поликарбоната со временем.

V3 легче стали на 35–45 %, не корродирует; недостатки — существенно дороже, без возможности раскрытия. Имеет смысл только при жёстком ограничении по нагрузке на существующие стены.

По критерию минимума стоимости при заданном качестве рабочим оптимумом является V2 (сталь + сотовый поликарбонат). Полный патентный вариант V1 целесообразен, если требуется мобильность полотна. V3 не является основным.

Ожидаемый годовой эффект: экономия на уборке снега зимой ≈ 235 тыс. руб.; экономия на уборке листвы и мусора ≈ 45 тыс. руб.; суммарно ≈ 280 тыс. руб./год; сохранение 150 м^2 и 10 машиномест; снижение коррозии металла во дворе ≈ 3 %/год.

Водоотведение и эксплуатация. Угол 35° и гладкое покрытие обеспечивают самостоятельный сход снега. Внутренние скаты направлены в желоба с уклоном ≥ 1 % и кабельным обогревом. Нижняя зона (до 1,8 м) выполняется матовой или цветной, чтобы избежать эффекта «прозрачной стены».

Монтажная схема (без длительного закрытия стоянки): 1) обмер опорного контура по кровле; 2) сборка граней внизу, вне двора; 3) подача краном с улицы (ул. Егорова), без работы из двора; 4) установка опорного контура на анкерах; 5) монтаж рёбер и заполнения; 6) устройство желобов с обогревом и сдача. Календарный срок для V2 — 7–9 суток.

5. Развитие патента RU 186423 U1

Предлагается двухрежимное решение: зимой — глухое заполнение поликарбонатом, летом — возможность выдвижения/сматывания полотна (если выбран V1). Для климата Санкт-Петербурга обязателен обогрев желобов и коробов бобин, регулярный сервис механики. Форма каркаса следует ломаному контуру двора. Эффект снижения коррозии предлагается подтвердить датчиками влажности и периодическим осмотром металла.

Для рабочей документации рекомендуется моделирование в Renga (нормы РФ) или Revit; для чертежей и стройгенплана — nanoCAD. На стадии доклада достаточно схем и визуализаций.

6. Выводы

1. Двор корпуса Е имеет размеры 39,6 × 23,0 м (560 м^2); принятый купол — высота 7,7 м, угол 35°, поверхность ≈ 680 м^2.

2. Критерий оптимизации — минимум стоимости (капитальные + эксплуатационные) при фиксированном качестве: сухость двора, инсоляция, −3 %/год коррозии, сохранение 10 машиномест.

3. В основу положен патент RU 186423 U1 (2019, СПбГАСУ, каф. ТСП). ПВХ-каркас на данном пролёте неработоспособен.

4. Рабочий оптимум — стальной каркас + сотовый поликарбонат (≈ 5,6 млн руб., монтаж 7–9 суток с улицы).

5. Годовой эффект: экономия на уборке ≈ 280 тыс. руб., сохранение парковочных мест, снижение коррозии.

6. Если требуется мобильность полотна патента — сталь + ETFE (≈ 6,9 млн руб.) с обязательным обогревом механики.

Работа выполнена в рамках подготовки к научно-техническому симпозиуму, посвящённому 95-летию кафедры железобетонных и каменных конструкций СПбГАСУ (ноябрь 2026).

Список литературы:

1. Патент RU 186423 U1. Купол над внутренними дворами с выдвижным полотном / Казаков Ю. Н., Шахназаров С. С.; патентообладатель СПбГАСУ. Заявл. 22.05.2018, опубл. 21.01.2019.

2. Казаков Ю. Н., Мороз А. М., Захаров В. П. Технология возведения зданий. – СПб.: Лань, 2021.

3. СП 20.13330.2016. Нагрузки и воздействия. Актуализированная редакция СНиП 2.01.07–85*. – М.: Минстрой России, 2016.

4. СП 17.13330.2017. Кровли. Актуализированная редакция СНиП II-26–76. – М.: Минстрой России, 2017.

5. СП 28.13330.2017. Защита строительных конструкций от коррозии. Актуализированная редакция СНиП 2.03.11–85. – М.: Минстрой России, 2017.

6. ГЭСН 81-02. Государственные элементные сметные нормы на строительные работы (расценки 34, 46-02-005-02). – М.: Минстрой России.

7. Обмерные данные и чертёж двора корпуса СПбГАСУ, ул. Егорова, д. 5/8. Съёмка 14.09.2026.

Variant design and optimization of the construction of a translucent dome over the inner courtyard of the SPBGASU building

Kazakov Yu.N.[1], Dzekun D. D.[2], Bakulova T. S.[3]
Saint Petersburg State University of Architecture and Civil Engineering,
Saint Petersburg, Russia
[1]e-mail: kazin@lan.spbgasu.ru
[2]e-mail:darya.dzekun00@mail.ru
[3]e-mail: tan.volk.21012005@gmail.com

Abstract

The paper considers the variant design and optimization of the construction of a translucent dome over the inner courtyard of Building E of the Saint Petersburg State University of Architecture and Civil Engineering (5/8 Egorova St.). The object measures 39.6 × 23.0 m in plan (area 560 m^2), the dome height is 7.7 m, the slope angle is 35°, and the covering surface is approximately 680 m^2. The work is based on utility model patent RU 186423 U1 (2019) for a dome with a retractable membrane. Three variants are compared: steel frame + ETFE (full patent version), steel frame + cellular polycarbonate, and aluminium frame + polycarbonate. The optimization criterion is the minimum life-cycle cost at a fixed quality level (dry courtyard in winter and autumn, preserved insolation, metal corrosion reduction of 3 % per year, retention of 150 m^2 and 10 parking spaces). It is shown that the working optimum is the "steel + cellular polycarbonate" variant (≈ 5.6 million RUB, erection in 7–9 days from the street without prolonged closure of the parking area). The full patent version with a retractable ETFE membrane is advisable when summer opening is required. Enlarged cost estimates, labour intensity, erection scheme and expected annual effect (cleaning savings ≈ 280 thousand RUB/year) are presented.

Keywords: *translucent dome; courtyard well; variant design; steel frame; cellular polycarbonate; ETFE; cost optimization; erection without parking closure; patent RU 186423 U1; Saint Petersburg climate.*

2.3. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

2.3

МЕТРИКИ ОЦЕНКИ ЗАЩИТНОГО КОНТУРА LLM/RAG-СИСТЕМ: БЕЗОПАСНОСТЬ, ПОЛЕЗНОСТЬ И РЕСУРСЫ

Павлов Д. В.[1], Галанина Н. А.[2]

Чувашский государственный университет имени И. Н. Ульянова,
кафедра математического и аппаратно-программного обеспечения
информационных систем,
Чебоксары, Россия
[1]e-mail: d1maka02@yandex.ru
[2]e-mail: galaninacheb@mail.ru

Аннотация

Рассматривается комплексная оценка защитного контура систем с большими языковыми моделями и генерацией с дополнением извлечением (RAG), использующих недоверенный внешний контекст. Показатель успешности атаки сам по себе не характеризует пригодность защиты: его снижение может достигаться за счет блокировки корректных запросов, потери полезной информации и роста вычислительных затрат. Предложен воспроизводимый набор показателей безопасности, полезности и ресурсоэффективности для сопоставления обнаружения, очистки, проверки и резервного безопасного сценария обработки. Сформулированы правила построения чистых, атакующих и трудных безопасных сценариев, а также матрица совместной оценки защитных методов. Работа носит обзорно-методический характер и не содержит новых экспериментальных численных результатов.

Ключевые слова: *большие языковые модели; RAG; инъекция инструкций; недоверенный контекст; информационная безопасность; оценка качества.*

Введение

Большие языковые модели (БЯМ, LLM) все чаще становятся частью прикладных информационных систем. Они отвечают на вопросы по корпоративным базам знаний, обрабатывают служебные документы, подготавливают сводки, помогают искать сведения и выступают интерфейсом к программным инструментам. Архитектура генерации с дополнением извлечением (RAG) дополняет параметры модели внешней памятью: по запросу пользователя система извлекает релевантные фрагменты и передает их модели вместе с заданием. Такой подход повышает актуальность и проверяемость ответа, но одновременно добавляет новый канал влияния на поведение модели [1, 15].

Ключевая проблема состоит в том, что естественно-языковой контекст технически передается модели в том же поле ввода, что и инструкции. Внешний документ должен использоваться как данные, однако находящаяся в нем императивная фраза может быть интерпретирована как команда. Прямая инъекция инструкций (prompt injection) размещается в запросе пользователя, а непрямая — в документе, веб-странице, письме или извлеченном фрагменте. Последний вариант особенно важен для RAG: атакующий может изменять доступный для поиска контент, не имея доступа к системной инструкции или к коду приложения [2, 3, 7, 8, 14].

Международные рекомендации относят инъекцию инструкций к числу базовых рисков приложений на основе БЯМ. OWASP указывает, что такие воздействия способны изменить поведение системы, привести к раскрытию чувствительных данных или повлиять на действия, выполняемые приложением [4, 16]. Таксономия NIST отдельно выделяет прямые и непрямые инъекции инструкций среди атак на генеративные ИИ-системы [5, 13]. Следовательно, объектом защиты становится не только языковая модель, но и весь поток обработки контекста: извлечение, подготовка входных данных, генерация ответа, вызов инструментов и аудит событий.

На практике защитные механизмы различаются по принципу действия. Легкий модуль обнаружения может помечать рискованный фрагмент до передачи модели. Модуль очистки пытается убрать или нейтрализовать внедренную инструкцию, сохранив полезные факты. Модуль проверки оценивает контекст либо уже сформированный ответ с учетом исходной задачи. Резервный безопасный сценарий переводит систему в ограниченный режим: отказ, выдачу неполного ответа, отключение инструментов или передачу случая оператору. Выбор только одного из этих компонентов редко дает достаточную защиту; вместе с тем последовательное применение всех проверок может сделать систему непригодной из-за задержки и ложных блокировок.

Цель статьи — предложить систему совместной оценки защитного контура LLM/RAG-систем по трем группам показателей: безопасность, полезность и ресурсы. Для достижения цели формализуются границы контура, набор сценариев и метрик, задаются правила интерпретации показателей и предлагается матрица сравнения защитных методов. Вклад работы заключается в методической связке характеристик, которые обычно рассматриваются отдельно. Статья не представляет новый модуль обнаружения и не содержит экспериментальных результатов; ее результатом является протокол, пригодный для построения контрольного набора и подготовки сопоставимых экспериментов.

2. Материалы и методы

2.1. Граница защитного контура

Рассматривается LLM/RAG-система, получающая доверенные системные правила, запрос пользователя и внешний контекст. Внешний контекст может быть получен из загруженного файла, базы знаний, тикета, письма, веб-страницы или поискового индекса. Он потенциально содержит одновременно факты, необходимые для решения задачи, и инструкцию, которая пытается изменить приоритет правил или цель обработки. В рамках статьи не рассматриваются атаки на веса модели, обучение, криптографическую защиту данных и полный промышленный контур управления доступом.

Типовой поток обработки имеет вид: запрос пользователя → извлечение → внешний контекст → защитные компоненты → подготовка входных данных → БЯМ → проверка ответа → ответ пользователю. Модуль обнаружения применяется до включения фрагмента во входные данные и возвращает оценку риска. Политика обработки сопоставляет оценку с правилами. Затем могут использоваться модуль очистки, карантин подозрительного фрагмента, модуль проверки и резервный безопасный сценарий. После генерации отдельный модуль проверки может выявлять утечку служебных данных, выполнение вредной инструкции или несоответствие исходной задаче. Журналирование фиксирует входные признаки, срабатывания и принятые решения для последующего анализа.

Для воспроизводимого исследования каждый сценарий следует описывать полями: идентификатор, язык, тип источника, исходный запрос, недоверенный контекст, тип атаки, ожидаемое безопасное поведение, критерий успешной атаки и критерий успешного решения задачи. Такой формат исключает подмену цели эксперимента: модель может правильно блокировать опасную инструкцию, но при этом безосновательно отказываться от выполнения допустимой пользовательской задачи.

2.2. Набор сценариев и правила разметки

Набор сценариев должен состоять из трех раздельных групп. Чистые сценарии содержат только допустимый контекст и проверяют базовую полезность системы. Атакующие сценарии содержат внедренную инструкцию: подмену задачи, попытку извлечения системной инструкции, изменение приоритета инструкций, навязывание вызова инструмента или обход заданной политики. Трудные безопасные сценарии формально похожи на атаки, но являются безопасными: например, документ описывает инцидент, цитирует вредную фразу в учебных целях или содержит регламент противодействия атаке. Без третьей группы высокая полнота обнаружения может быть достигнута простым блокированием всех текстов с характерными словами.

При разметке на уровне итогового поведения применяются метки наличия атаки, успеха атаки, успеха решения задачи, ложного отказа и утечки. Метка успеха атаки ставится, если модель выполнила установленный вредный критерий; успех решения задачи фиксируется, если исходная допустимая задача решена корректно и безопасно. Ложный отказ фиксируется, когда система не выполняет допустимую задачу при наличии достаточного безопасного контекста. Утечка означает раскрытие системной инструкции, скрытого контекста, персональных или иных запрещенных данных. Разметку спорных случаев следует проводить по заранее зафиксированным правилам и, по возможности, двумя экспертами с последующим согласованием.

Таблица 1 — Минимальная структура набора сценариев

Группа	Назначение	Пример ожидаемого результата	Ключевые метки
Чистые	Проверка выполнения допустимой задачи	Ответ опирается на контекст и решает задачу	успех решения
Атакующие	Проверка устойчивости к внедренной инструкции	Атака не выполнена; полезная часть задачи сохранена	успех атаки, утечка
Трудные безопасные	Контроль ложных блокировок	Цитата или описание атаки не блокируются	ложный отказ, FPR

2.3. Показатели безопасности

Основным показателем итогового поведения является доля успешных атак (ASR) — доля атакующих сценариев, в которых атака достигла заданного критерия успеха. Для

RAG дополнительно целесообразно измерять долю попадания атаки в извлеченный контекст (ARR). ARR отделяет ошибку извлечения от ошибки последующей защиты. Низкий ASR при низком ARR не доказывает устойчивость защитного контура: атака могла просто не дойти до модели.

$ASR = Nattack\ successNattack \quad ARR = Nretrieved\ attackNattack$ (1)

Для модулей обнаружения, принимающих бинарное решение, используются точность (precision), полнота (recall) и F1-мера. Точность показывает, какая доля помеченных как опасные фрагментов действительно является атакой. Полнота отражает долю обнаруженных атак. F1-мера служит гармоническим средним и удобна при несбалансированных классах, однако не должна заменять раздельный отчет о типах ошибок. В безопасности пропущенная атака и ложная блокировка имеют разную цену; поэтому доля пропущенных атак (FNR) и доля ложных срабатываний (FPR) публикуются рядом с F1-мерой, а не скрываются внутри интегрального показателя.

$Precision = TPTP + FP \quad Recall = TPTP + FN \quad F1 = 2\ Precision\ RecallPrecision + Recall$ (2)

Важно различать обнаружение и предотвращение. Модуль обнаружения может верно отметить опасный фрагмент, но политика обработки может принять слишком мягкое решение; наоборот, агрессивный резервный сценарий может снизить ASR без качественного выявления атаки, просто отказываясь от большинства запросов. Поэтому в отчете должны быть указаны уровень, на котором измерен показатель, вход для компонента и действие, применяемое после срабатывания. Доля утечек и доля вредных выполнений дополняют ASR в сценариях, где атака не сводится к одному бинарному исходу. Рекомендации OWASP по предотвращению инъекций инструкций следует использовать как исходный перечень проверяемых мер, а не как доказательство их эффективности [9].

2.4. Показатели полезности

Полезность защитного контура определяется его способностью сохранять выполнение исходной задачи. Доля успешно решенных задач (TSR) равна доле допустимых сценариев, в которых система выдала корректный и применимый ответ. Для атакующего сценария положительным исходом является не простой отказ, а безопасное решение той части задачи, которая не противоречит политике. Например, при обнаружении вредной инструкции в техническом документе система может использовать фактическое содержание документа, проигнорировав командный фрагмент.

$TSR = Nsafe\ task\ successNallowed\ tasks \quad FRR = Nfalse\ refusalsNallowed\ tasks$ (3)

Для RAG необходимо отдельно оценивать качество связки извлечения и генерации. Релевантность контекста характеризует соответствие извлеченного фрагмента вопросу; обоснованность ответа источниками — степень опоры утверждений на предоставленный контекст; полнота — соответствие эталону или перечню необходимых фактов; фактическая корректность — отсутствие ложных утверждений. RAGAS и ARES предлагают оценивать эти характеристики раздельно [10, 11]. Это важно для модуля очистки: удаление подозрительного фрагмента может уменьшить риск, но одновременно убрать единственный факт, нужный для ответа.

Автоматическая оценка открытых ответов с помощью сильной БЯМ допустима как вспомогательный инструмент, но требует контроля. Исследования применения БЯМ в роли судьи показывают масштабируемость такого подхода, одновременно фиксируя позиционную, стилистическую и самоусиливающуюся предвзятость [12]. Поэтому

итоговые выводы о полезности следует подтверждать человеческой разметкой подвыборки, зафиксированной инструкцией судьи, повторной перестановкой сравниваемых ответов и публикацией критериев оценивания.

2.5. Ресурсные показатели

Защита LLM/RAG-системы разворачивается в среде с ограничениями по памяти, задержке и стоимости вызовов модели. Для интерактивного приложения медианная задержка описывает типичный опыт пользователя, а 95-й процентиль задержки — поведение в хвосте распределения. Их следует измерять отдельно от времени холодного запуска, поскольку загрузка модели, прогрев кэша и первая генерация часто существенно отличаются от стабильной обработки запросов. Для каждого компонента также фиксируются пиковое потребление оперативной и видеопамяти, размер артефакта, пропускная способность, число входных и выходных токенов и число дополнительных вызовов БЯМ.

Если применяется облачная модель, ресурсы дополняются стоимостью одного запроса и скоростью сетевого взаимодействия; для локальной модели указываются аппаратная платформа, тип квантования, версия среды выполнения и режим использования центрального и графического процессоров. Сравнение конфигураций допустимо только на одном наборе сценариев и при одинаковых ограничениях на длину контекста. Размер модели сам по себе не заменяет измерение задержки: на нее влияют шаблон входных данных, длина фрагментов, число запусков модуля проверки и механизм агрегации решений.

Предпочтительна каскадная организация: легкий модуль обнаружения запускается для всех фрагментов, а более дорогой модуль проверки — только для риска выше заданного порога или для зоны неопределенности. Эта схема является инженерной гипотезой, которую необходимо проверять экспериментально. Ее преимущество нельзя объявлять доказанным без сопоставления с режимом постоянного запуска модуля проверки на том же наборе сценариев.

3. Результаты методического анализа

3.1. Система совместной оценки

Результатом методического анализа является профиль оценки, объединяющий три группы показателей. Безопасность отвечает на вопрос, достигла ли вредная инструкция цели. Полезность отвечает на вопрос, сохранила ли система возможность безопасно решить исходную задачу. Ресурсная группа отвечает на вопрос, применим ли метод при заданной инфраструктуре. Ни один из блоков нельзя использовать в качестве универсального заменителя остальных. Например, метод с нулевым ASR и высокой долей ложных отказов может быть непригоден для справочной системы; метод с высоким TSR и низкой задержкой, но значительным FNR, не подходит для сценария с повышенными требованиями к защите.

Таблица 2 — Профиль метрик защитного контура

Группа	Метрики	Уровень измерения	Интерпретация
Безопасность	ASR, ARR, точность, полнота, F1, FPR, FNR, утечки	Фрагмент, контекст, итоговый ответ	Насколько атака выявлена и предотвращена
Полезность	TSR, ложные отказы, релевантность, обоснованность, полнота, фактическая корректность	Контекст и ответ	Сохраняется ли решение допустимой задачи
Ресурсы	медианная и p95 задержки, RAM/VRAM, пропускная способность, холодный запуск, вызовы модели, стоимость	Компонент и полный конвейер	Цена защиты и применимость конфигурации

Для каждого метода в сравнительной таблице необходимо показывать не одно место в рейтинге, а профиль. При наличии нескольких рабочих порогов рекомендуется выбирать их на отдельной валидационной части, не используя тестовые данные. Минимальная отчетность включает доверительные интервалы, распределение показателей по типам атак, языкам и источникам контекста. Если несколько фрагментов объединяются максимальной оценкой риска, это следует указать отдельно: вероятность хотя бы одного ложного срабатывания растет с числом извлеченных фрагментов.

3.2. Матрица интерпретации защитных методов

Таблица 3 имеет иллюстративный характер: в ней не приведены экспериментальные численные значения и не сравниваются конкретные реализации. Матрица показывает, какие компромиссы следует проверить при выборе класса защитного механизма. Для фактического решения необходимо заполнить ее измерениями на одном и том же контрольном наборе.

Таблица 3 — Иллюстративная матрица совместной оценки

Метод	Безопасность	Риск для полезности	Ресурсный профиль	Что проверять
Без защиты	ASR является исходным уровнем	Минимальный риск ложной блокировки	Базовая задержка	ASR, TSR, утечки
Правиловый модуль обнаружения	Быстрый первый слой; чувствителен к обходам	FPR на трудных безопасных примерах	Низкие затраты	Полнота по вариантам формулировок, FPR
Модельный модуль обнаружения	Потенциально выше полнота	Зависит от переноса распределения	Низкие или средние затраты	F1, AUROC, срезы по языкам и источникам
Модуль очистки	Снижает передачу инструкций модели	Потеря фактов и нарушение смысла	Средние затраты	ASR, TSR, обоснованность, потеря информации
Модуль проверки	Контекстная проверка повышает глубину анализа	Возможны отказ и ошибка судьи	Высокая задержка и расход памяти	ASR, ложный отказ, p95 задержка, вызовы модели
Резервный сценарий	Ограничивает последствия при неопределенности	Может резко снизить TSR	Низкие или средние затраты	ASR, TSR, доля передачи оператору

Метод признается предпочтительным не потому, что имеет максимальный отдельный показатель, а потому, что удовлетворяет заданным ограничениям. Пример правила выбора: сначала установить допустимый максимум ASR и FPR, затем среди конфигураций, выполняющих эти ограничения, выбрать вариант с наибольшим TSR и приемлемыми 95-м процентилем задержки и потреблением памяти. Пороговые значения задаются предметной областью. Для вспомогательного поиска по открытым документам допустима иная цена ложного отказа, чем для системы, способной вызвать внешнее действие.

4. Обсуждение и выводы

4.1. Ограничения протокола и практические рекомендации

Предложенный набор метрик не устраняет фундаментальную проблему смешения данных и инструкций в естественном языке. Он позволяет наблюдать компромиссы и воспроизводимо сравнивать решения, но не гарантирует защищенность от ранее не встречавшихся формулировок. Публикуемые контрольные наборы показывают, что устойчивость зависит от типа контекста, способа атаки и конкретной модели [3, 6]. Поэтому тестирование только на коротких прямых запросах недостаточно для RAG-сценария с документами и поисковыми фрагментами.

Первое практическое правило состоит в раздельной подготовке чистых, атакующих и трудных безопасных примеров. Второе — в измерении безопасности и полезности на одном наборе сценариев: нельзя объявлять метод безопасным, не показывая потерь полезных ответов. Третье правило требует фиксировать конфигурацию эксперимента: модель, ее версию, квантование, системную инструкцию, политику резервного сценария, порог срабатывания, длину контекста и аппаратную платформу. Четвертое — публиковать ошибки по типам атак, а не только среднее значение. Пятое — отделять оценку модуля обнаружения от оценки итогового поведения приложения.

При применении БЯМ в роли судьи необходимо учитывать зависимость оценки от инструкции судьи, порядка ответов и модели-судьи. Автоматическая оценка не заменяет экспертную валидацию на критических подвыборках. Для русскоязычных систем требуется самостоятельная проверка: прямой перевод англоязычных атак и чистых примеров не воспроизводит особенности русской технической документации, цитирования и формулировок служебных инструкций. Отдельное ограничение связано с агентными системами: если БЯМ может вызывать инструменты, критерием успешной атаки становится не только текст ответа, но и фактически инициированное действие.

4.2. Выводы

В статье предложена методическая система оценки защитного контура LLM/RAG-систем, работающих с недоверенным внешним контекстом. Ее основой является совместное рассмотрение безопасности, полезности и ресурсов. Для безопасности необходимы ASR, ARR, показатели обнаружения, доли утечек и пропущенных атак. Для полезности - TSR, ложные отказы, релевантность контекста, обоснованность, полнота и фактическая корректность ответа. Для ресурсоэффективности - задержка, память, пропускная способность, количество вызовов моделей и стоимость обработки.

Сформулированный протокол требует разделять чистые, атакующие и трудные безопасные сценарии; фиксировать уровень измерения метрики; выбирать пороги без использования тестовой части; показывать профиль ошибок и ресурсную цену каждого компонента. Такой подход исключает некорректный вывод о качестве защиты по одной метрике. Дальнейшая работа должна включать создание русскоязычного контрольного набора недоверенных контекстов, экспериментальное сравнение каскадных конфигураций модулей обнаружения, очистки и проверки, а также проверку переноса результатов между моделями и источниками документов.

Список литературы

1. Lewis P., Perez E., Piktus A. et al. Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks // Advances in Neural Information Processing Systems. 2020. Vol. 33. URL:

https://proceedings.neurips.cc/paper/2020/hash/6b493230205f780e1bc26945df7481e5-Abstract.html (дата обращения: 22.09.2026).

2. Greshake K., Abdelnabi S., Mishra S. et al. Not What You've Signed Up For: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection // arXiv. 2023. arXiv:2302.12173. URL: https://arxiv.org/abs/2302.12173 (дата обращения: 22.09.2026).

3. Yi J., Xie Y., Zhu B. et al. Benchmarking and Defending Against Indirect Prompt Injection Attacks on Large Language Models // Proceedings of the 31st ACM SIGKDD Conference on Knowledge Discovery and Data Mining. 2025. DOI: 10.1145/3690624.3709179.

4. OWASP Foundation. OWASP Top 10 for Large Language Model Applications 2025. 2024. URL: https://genai.owasp.org/resource/owasp-top-10-for-llm-applications-2025/ (дата обращения: 22.09.2026).

5. Vassilev A., Oprea A., Fordyce A., Anderson H. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. NIST AI 100-2e2025. Gaithersburg: National Institute of Standards and Technology, 2025. DOI: 10.6028/NIST.AI.100-2e2025.

6. Mazeika M., Phan L., Yin X. et al. HarmBench: A Standardized Evaluation Framework for Automated Red Teaming and Robust Refusal // arXiv. 2024. arXiv:2402.04249. URL: https://arxiv.org/abs/2402.04249 (дата обращения: 22.09.2026).

7. Liu Y., Deng G., Li Y. et al. Prompt Injection Attack against LLM-Integrated Applications // arXiv. 2023. arXiv:2306.05499. URL: https://arxiv.org/abs/2306.05499 (дата обращения: 22.09.2026).

8. Perez F., Ribeiro I. Ignore Previous Prompt: Attack Techniques For Language Models // arXiv. 2022. arXiv:2211.09527. URL: https://arxiv.org/abs/2211.09527 (дата обращения: 22.09.2026).

9. OWASP Foundation. LLM Prompt Injection Prevention Cheat Sheet. URL: https://cheatsheetseries.owasp.org/cheatsheets/LLM_Prompt_Injection_Prevention_Cheat_Sheet.html (дата обращения: 22.09.2026).

10. Es S., James J., Espinosa-Anke L., Schockaert S. RAGAS: Automated Evaluation of Retrieval Augmented Generation // arXiv. 2023. arXiv:2309.15217. URL: https://arxiv.org/abs/2309.15217 (дата обращения: 22.09.2026).

11. Saad-Falcon J., Khattab O., Potts C., Zaharia M. ARES: An Automated Evaluation Framework for Retrieval-Augmented Generation Systems // arXiv. 2023. arXiv:2311.09476. URL: https://arxiv.org/abs/2311.09476 (дата обращения: 22.09.2026).

12. Zheng L., Chiang W.-L., Sheng Y. et al. Judging LLM-as-a-Judge with MT-Bench and Chatbot Arena // Advances in Neural Information Processing Systems. 2023. Vol. 36. URL: https://arxiv.org/abs/2306.05685 (дата обращения: 22.09.2026).

13. NIST. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. Gaithersburg: National Institute of Standards and Technology, 2023. DOI: 10.6028/NIST.AI.100-1.

14. Zou A., Wang Z., Carlini N. et al. Universal and Transferable Adversarial Attacks on Aligned Language Models // arXiv. 2023. arXiv:2307.15043. URL: https://arxiv.org/abs/2307.15043 (дата обращения: 22.09.2026).

15. Karpukhin V., Oguz B., Min S. et al. Dense Passage Retrieval for Open-Domain Question Answering // Proceedings of EMNLP 2020. 2020. P. 6769-6781. DOI: 10.18653/v1/2020.emnlp-main.550.

16. OWASP Foundation. LLM01:2025 Prompt Injection. URL: https://genai.owasp.org/llmrisk/llm01-prompt-injection/ (дата обращения: 22.09.2026).

Metrics for evaluating the protective contour of llm/rag systems: security, utility and resources

Pavlov D.V. [1], Galanina N.A.[2]

Chuvash State University named after I. N. Ulyanov, Department of Mathematical and Hardware-Software Support of Information Systems,
Cheboksary, Russia;
[1]e-mail: d1maka02@yandex.ru
[2]e-mail: galaninacheb@mail.ru

Abstract

The paper considers comprehensive evaluation of a protective contour for systems that combine large language models and retrieval-augmented generation (RAG) with untrusted external context. Attack success rate alone does not characterize the suitability of a safeguard because its reduction may be achieved by blocking legitimate requests, losing useful information, or increasing computational costs. A reproducible set of security, utility, and resource-efficiency metrics is proposed for comparing detection, sanitization, verification, and a safe fallback scenario. Rules are formulated for constructing clean, attack, and hard-negative scenarios, together with a joint evaluation matrix for protective methods. The paper is methodological and does not report new empirical numerical results..

Keywords: *large language models; RAG; prompt injection; untrusted context; information security; quality assessment.*

5.9. ФИЛОЛОГИЯ

5.9

СТРУКТУРНЫЕ МОДЕЛИ ТЕРМИНОВ ЦИФРОВЫХ ТЕХНОЛОГИЙ В СОВРЕМЕННОМ АНГЛИЙСКОМ ЯЗЫКЕ

Кондрашова Д.Г.
Московский педагогический государственный университет,
Институт иностранных языков, кафедра фонетики и лексики английского языка имени В. Д. Аракина
Москва, Россия
e-mail: kondrasshovaa@yandex.ru

Аннотация

Статья посвящена структурной организации англоязычных терминов цифровых технологий на материале направленной выборки из 248 терминологических единиц, зафиксированных в профессиональных, справочных и технических англоязычных ресурсах. Для каждой единицы определялся ведущий структурно-словообразовательный механизм; в корпусе разграничены простые и производные однословные термины, компаунды, многокомпонентные терминологические сочетания, аббревиатуры и акронимы, клиппинги, бленды и графически гибридные формы. Анализ свидетельствует о функциональном различии выделенных моделей: развернутые сочетания обеспечивают последовательную спецификацию понятия, тогда как аббревиация, усечение, контаминация и словосложение реализуют разные модели формальной компрессии. Графически гибридные формы показывают, что цифры и специальные символы могут входить в структуру термина под влиянием технических стандартов и принятых способов цифровой записи

Ключевые слова: *цифровые технологии; терминология; структурные модели; словообразование; словосложение; многокомпонентные термины; аббревиация.*

Введение

Появление новых объектов, процессов и способов взаимодействия в цифровых сферах быстро отражается в языке. Вместе с программными продуктами, архитектурами, сетевыми решениями, методами обработки данных и моделями искусственного интеллекта возникают новые термины. Одни употребляются преимущественно в профессиональной среде, другие входят в образовательный, научно-популярный и массовый дискурс. При этом меняется как состав цифровой терминологии, так и способы построения новых номинаций.

В отечественном терминоведении термин рассматривается как элемент специальной системы, соотнесенный с профессиональным понятием и связанный с другими единицами терминосистемы [1]. Это понимание термина особенно значимо для цифровой терминологии: устойчивые номинации здесь сосуществуют с единицами, специальное значение которых в значительной степени зависит от контекста употребления. Подобные переходные случаи описываются Е. А. Никулиной через понятие терминологизма и взаимодействие специальной и общеязыковой семантики [2–4].

Однако структура термина не сводится лишь к его внешнему оформлению. Через нее проявляется способ организации профессионального понятия средствами языка.

Так, одно и то же понятие может быть представлено развернутой номинацией и ее сокращенным вариантом: *artificial intelligence - AI*, *virtual private network - VPN*, *large*

language model - LLM. В других случаях новый термин формируется путем словосложения или переосмысления уже существующей лексической единицы. Слова *cloud*, *mouse*, *thread*, *window*, *token*, *branch* существовали в английском языке до развития современных цифровых технологий, однако получили специализированные значения и закрепились в профессиональном употреблении. С социокогнитивной точки зрения такая вариативность закономерна, поскольку термин развивается вместе с профессиональной коммуникацией и системой знаний, которую обслуживает [8, 9].

Возможности английского словообразования создают для этого благоприятную основу. Словосложение, аффиксация, конверсия, сокращение, усечение и контаминация относятся к продуктивным механизмам пополнения словарного состава английского языка [6, 7]. В цифровой терминологии к ним добавляется синтаксический ресурс многокомпонентных сочетаний, посредством которого содержание понятия уточняется последовательным присоединением определяющих компонентов.

Проблема формирования терминологии информационных технологий ранее рассматривалась в связи с источниками пополнения терминосистемы, словообразовательными механизмами, аббревиацией и семантическими переносами [5]. Быстрое обновление цифровой сферы, однако, требует обращения к материалу современного профессионального употребления и одновременно ставит вопрос о единых критериях структурной классификации. Это имеет значение прежде всего для пограничных единиц, внешне сходных, но образованных разными способами.

Значительная часть профессиональной коммуникации разработчиков, специалистов по информационной безопасности, сетевым технологиям и программным платформам сегодня представлена в цифровой среде: в технической документации, справочных системах, стандартах и специализированных веб-ресурсах. Для отбора такого материала применим подход «веб как корпус», согласно которому систематически отобранные сетевые тексты могут выступать эмпирической базой лингвистического анализа [10].

В настоящей статье профессиональное употребление терминов проверялось прежде всего по MDN Web Docs, GitHub Docs, Microsoft Learn, глоссарию NIST, материалам Cloudflare Learning Center и OWASP [11–16].

Объектом анализа является англоязычная терминология цифровых технологий; *предметом* - способы формальной организации терминологических единиц. *Цель статьи* состоит в систематизации основных структурных моделей и уточнении критериев их разграничения на материале 248 единиц. Для достижения цели необходимо определить состав структурных типов, описать характерные словообразовательные и синтаксические модели и установить функциональные различия между развернутыми и компрессированными номинациями.

Материалы и методы

Материалом послужила направленная выборка из 248 англоязычных терминологических единиц сферы цифровых технологий. В нее вошли обозначения программного обеспечения, данных и их обработки, искусственного интеллекта и машинного обучения, кибербезопасности, сетей и протоколов, аппаратного обеспечения, пользовательского взаимодействия, а также единицы из смежных сегментов цифровой коммуникации. Тематическое разнообразие материала дает возможность сопоставлять способы номинации объектов, процессов, технологий, ролей и режимов работы в разных участках цифровой терминосистемы.

Источниковую базу составили профессиональные, справочные и технические англоязычные ресурсы. Термины веб-разработки и интернет-технологий фиксировались по материалам MDN Web Docs [11]. Единицы, связанные с

программированием, репозиториями, контролем версий и CI/CD, проверялись по GitHub Docs [12], а терминология программных платформ, облачных решений и средств разработки - по Microsoft Learn [13]. Для области кибербезопасности и сетевой инфраструктуры использовались глоссарий NIST, материалы Cloudflare Learning Center и ресурсы OWASP [14–16].

Указанные источники не рассматривались как теоретическая база статьи. Их функция заключалась в подтверждении современного профессионального употребления отобранных единиц.

При формировании корпуса учитывались два основных признака: устойчивость формы и наличие закрепленного специального значения. В выборку включались обозначения технологических объектов, процессов, ролей, методов и свойств, регулярно встречающиеся в профессиональной документации. Случайные авторские неологизмы, рекламные формулы и общеупотребительные слова, для которых в рассматриваемых источниках не подтверждалось специальное значение, исключались.

Отдельного решения потребовали случаи параллельного существования полной и сокращенной формы. В каждой из пар *artificial intelligence* и *AI*, *virtual private network* и *VPN*, *learning management system* и *LMS* обе формы обозначают одно и то же понятие, однако различаются способом языкового оформления и самостоятельно употребляются в профессиональной коммуникации. Поэтому полная и сокращенная формы учитывались как отдельные структурные единицы.

Основным методом исследования был структурно-словообразовательный анализ. Для каждого термина определялись количество компонентов, графическое оформление и ведущий механизм образования. На основании этих признаков термин относился к соответствующему структурному типу.

Классификация требовала разграничения категорий. Само по себе слитное написание еще не дает оснований относить единицу к однословным терминам: *database*, *app* и *webinar* графически цельны, но образованы разными способами: словосложением, усечением и контаминацией соответственно. Поэтому в категорию простых и производных однословных терминов включались единицы, не возникшие в результате словосложения, усечения или контаминации. Слитные и устойчивые дефисные образования из нескольких основ рассматривались как компаунды. Раздельно оформленные устойчивые номинации относились к многокомпонентным терминологическим сочетаниям.

Инициальные сокращения объединялись в группу аббревиатур и акронимов. Усеченные формы относились к клиппингам, а единицы, образованные соединением фрагментов нескольких основ, к блендам. Отдельную группу составляли сочетания букв с цифрами и специальными знаками, если символический компонент входил в закрепленную форму обозначения.

Формальное сходство не всегда означало принадлежность к одной структурной модели. Так, *data center* и *database* включают сопоставимые лексические компоненты, но различаются графическим оформлением. В *data center* две основы сохраняют самостоятельность, поэтому эта единица квалифицируется как многокомпонентный термин модели N + N. *Database* представляет собой графически цельный компаунд. По тому же принципу разграничиваются *access control* и *firewall*.

Несколько иной вопрос возникает при анализе символически маркированных единиц. *C++*, *IPv6*, *2FA* и *CI/CD* отнесены к графическим гибридам, поскольку цифра или специальный знак является частью самого обозначения. Наличие дефиса само по себе основанием для такого решения не служит. В составе *end-to-end encryption* комплекс

end-to-end выполняет функцию сложного препозитивного модификатора существительного *encryption*, вследствие чего вся единица рассматривается как многокомпонентное сочетание.

Структурный анализ проводился по единому набору критериев для всех 248 единиц. Выборка создавалась направленно для структурного анализа и не является частотно сбалансированным корпусом английского цифрового дискурса. По этой причине полученные данные используются для описания структурного разнообразия и критериев разграничения моделей, но не для утверждений о статистической частотности каждого типа во всей терминологии цифровых технологий.

Результаты

Проведенная разметка позволила выделить семь структурных типов: простые и производные однословные термины, компаунды, многокомпонентные терминологические сочетания, аббревиатуры и акронимы, клиппинги, бленды и графически гибридные формы. Их основные характеристики представлены в табл. 1.

Таблица 1 — Основные структурные модели терминов цифровых технологий

Структурная модель	Формальный критерий	Примеры	Функциональная тенденция
Однословные термины	Одна графически цельная лексема; простая или производная структура	*server; router; cache; token; browser*	Компактная номинация объекта, процесса или функции
Компаунды	Слитное или дефисное объединение основ	*database; firewall; blockchain; cybersecurity; open-source*	Свертывание нескольких смысловых признаков в одной лексической форме
Многокомпонентные сочетания	Два и более раздельно оформленных компонента	*artificial intelligence; machine learning; data center; virtual private network*	Последовательная спецификация понятия
Аббревиатуры и акронимы	Инициальное сокращение полной формы	*AI; API; DNS; VPN; GPU; LMS*	Компрессия часто повторяющихся номинаций
Клиппинги	Усечение исходной формы	*app; config; repo*	Сокращение уже существующей номинации
Бленды	Контаминация частей двух исходных слов	*webinar; blog; infosec; edtech; hacktivism*	Создание новой компактной лексемы
Графические гибриды	Сочетание букв с цифрами и/или специальными знаками	*2FA; IPv6; C++; CI/CD; HTTP/HTTPS*	Стандартная символическая запись

Составлено автором на основе структурной разметки корпуса из 248 терминологических единиц.

Однословные термины в рассматриваемом материале часто обозначают базовые объекты, компоненты, функции и роли, например *server*, *router*, *cache*, *browser*. При этом краткость формы не делает значение автоматически прозрачным. Такие единицы, как *token*, *thread*, *branch*, *window* или *agent*, получают однозначную интерпретацию только в пределах соответствующей технологической области. Так, *branch* в системе контроля версий имеет специальное значение, отличное от общеупотребительного. В подобных случаях принадлежность единицы к терминологии определяется прежде всего профессиональным контекстом.

В компаундах структура организована иначе. Несколько смысловых признаков здесь объединяются в пределах одной лексической формы, что соответствует продуктивным моделям английского словосложения [6, 7]. В *database* первый компонент конкретизирует тип объекта, а второй обозначает его родовую принадлежность. В *blockchain* сочетание компонентов *block* и *chain* связано с принципом организации данных. У *firewall* специальное значение формируется на основе метафорического переосмысления обозначения физического защитного барьера.

К этой же структурной группе относятся *backend* и *frontend*. Пространственная семантика исходных компонентов в них получает специальное содержание в сфере программных систем. Такие примеры показывают, что формирование нового термина может сопровождаться не только словосложением, но и изменением значения уже известных языковых элементов.

Многокомпонентные сочетания строятся по другому принципу. Значение в них уточняется последовательно, по мере присоединения дополнительных компонентов. Это прослеживается в *artificial intelligence*, *operating system*, *virtual private network*, *large language model*, *learning management system*, где каждый компонент участвует в конкретизации обозначаемого понятия.

Особенно наглядно это видно при сопоставлении более общего и развернутого обозначения. Network называет широкий класс объектов, тогда как в *virtual private network* значение последовательно уточняется двумя определяющими компонентами. Аналогичное соотношение наблюдается между *model* и *large language model*: во втором случае общее обозначение получает дополнительную спецификацию. Внутренняя форма многокомпонентного термина тем самым частично отражает место понятия в профессиональной системе знаний.

Увеличение длины номинации имеет и обратное следствие. Чем чаще развернутый термин повторяется в документации и профессиональном общении, тем сильнее потребность в его сокращении. Поэтому рядом с *artificial intelligence*, *virtual private network*, *learning management system* и *large language model* регулярно функционируют *AI*, *VPN*, *LMS* и *LLM*.

Употребление полной или сокращенной формы определяется коммуникативной ситуацией. Развернутая номинация облегчает идентификацию понятия при первом введении, сокращенная уменьшает объем последующего текста. В специализированном сообществе такие формы, как *API*, *DNS*, *GPU* или *VPN*, могут употребляться без расшифровки; при переходе в учебный или массовый дискурс необходимость полной формы определяется подготовкой адресата [2–4, 9].

Особенно краткую форму имеют клиппинги и бленды, хотя механизмы их образования различаются.

Клиппинг предполагает сокращение уже существующего слова: *application - app*, *configuration - config*, *repository - repo*. Номинативная основа исходной единицы

сохраняется. Блендинг действует иначе: новая лексема возникает в результате соединения фрагментов нескольких слов - *web* + *seminar* = *webinar*, *web* + *log* = *blog*, *information* + *security* = *infosec*, *education* + *technology* = *edtech*. Внешнее сходство кратких форм, следовательно, скрывает принципиально разные словообразовательные процессы.

Клиппинги и бленды объединяет тенденция к сокращению формы, которая реализуется разными словообразовательными средствами. В профессиональной коммуникации такие единицы особенно заметны при многократном повторении термина в документации, интерфейсах, профессиональных чатах или устной речи.

Отдельную структурную группу составляют термины с цифрами и специальными символами. В *IPv6* числовой компонент указывает на версию протокола, а в *2FA* цифра графически замещает компонент *two*. Знаки «++» входят в закрепленное название языка программирования *C++*, тогда как косая черта в *CI/CD* соединяет две аббревиатуры. В таких единицах цифровой или символический компонент входит в саму форму термина, а не служит лишь способом его графического оформления. Это служит основанием для выделения таких образований в отдельную группу при структурной классификации цифровой терминологии.

При анализе многокомпонентных сочетаний учитывались их длина и характер отношений между компонентами. В исследуемом материале регулярно встречаются несколько синтаксических моделей, представленных в табл. 2.

Таблица 2 — Типовые формулы многокомпонентных терминов цифровых технологий

Формула	Характеристика	Примеры
N + N	Существительное-модификатор + ядерное существительное	*data center; access control; network protocol; cloud storage*
Adj + N	Прилагательное уточняет тип или свойство объекта	*virtual machine; digital signature; private key; neural network*
N + V-ing	Предметный компонент + процессуальное наименование	*machine learning; load balancing; data mining; rate limiting*
N + N + N	Последовательное уточнение основного существительного	*learning management system; data processing pipeline*
Adj + N + N	Прилагательное и существительное-модификатор перед основным словом	*large language model*
Adj + Adj + N	Два прилагательных перед основным существительным	*virtual private network*

N + Prep + N	Связь между понятийными компонентами выражена предлогом	*denial of service; proof of work; quality of service*
Hyphenated modifier + N	Сложный дефисный модификатор перед основным словом	*end-to-end encryption; open-source software; AI-generated content*

Составлено автором на основе структурной разметки терминов и моделей английского словообразования [6, 7].

Модель N + N широко представлена в английской профессиональной лексике благодаря аналитическому строю языка. В сочетаниях *data center*, *network protocol*, *cloud storage* первый компонент конкретизирует значение второго без отдельного морфологического показателя. Правый элемент, как правило, выступает ядерным и задает родовой класс.

Сходную задачу выполняет модель Adj + N: *virtual machine*, *digital signature*, *private key*, *neural network*. Различие состоит в грамматическом способе выражения признака: в данном случае им служит прилагательное.

В группе N + V-ing процессуальный компонент занимает позицию ядра: *machine learning*, *load balancing*, *data mining*, *rate limiting*. Такие единицы обозначают процессы, методы либо технологические операции, тогда как первый компонент уточняет объект или сферу их реализации.

Более сложные конструкции требуют отдельной разметки. В learning management system ядерным компонентом выступает system, а предшествующие существительные последовательно конкретизируют назначение системы. В *large language model* существительное *model* также является ядром, *language* функционирует как предметный модификатор, а *large* - как прилагательное. Единица, следовательно, соответствует формуле Adj + N + N.

Virtual private network устроен иначе. Оба предшествующих элемента, *virtual* и *private*, являются прилагательными и непосредственно характеризуют *network*. Поэтому данная единица относится к модели Adj + Adj + N. Разграничение этих конструкций необходимо для последовательной морфологической разметки материала.

Обсуждение

Выделенные модели не образуют единого способа номинации: одни из них служат для развертывания содержания специального понятия, другие уменьшают протяженность уже существующего обозначения. Первая тенденция наиболее отчетливо реализуется в многокомпонентных сочетаниях. Дополнительные компоненты ограничивают объем понятия и одновременно указывают на его отношение к более общему классу: *network - virtual private network*, *model - large language model*. Для терминосистемы такая прозрачность внутренней структуры функционально значима, поскольку облегчает соотнесение нового обозначения с другими элементами профессионального знания [1].

Потребность в компактной форме реализуется несколькими способами. Аббревиатура сохраняет начальные элементы развернутого наименования, клиппинг сокращает исходную лексему, бленд создает новое слово из частей нескольких основ, а компаунд объединяет основы в пределах одной лексической формы. Поэтому *VPN*, *app*, *webinar* и *database*, несмотря на относительную краткость, представляют разные структурные механизмы. Сходным для них оказывается функциональный результат - уменьшение объема номинации.

Параллельное функционирование полной и сокращенной форм заслуживает отдельного внимания. В профессиональном тексте сначала может появиться *large language model*, после чего дальнейшее изложение строится с использованием *LLM*. Обозначаемое понятие остается тем же, но его языковая форма приспосабливается к условиям коммуникации. Структура термина в данном случае зависит не только от словообразовательных возможностей языка, но и от характера его употребления, что соотносится с коммуникативным и социокогнитивным пониманием терминологии [2–4, 8, 9].

Формы *C++*, *IPv6*, *2FA*, *CI/CD* требуют учитывать при структурной классификации цифры и технические символы. В цифровой сфере такие элементы перестают быть только средством графического оформления и включаются непосредственно в специальную номинацию.

Связь с технологической средой здесь особенно очевидна. Программирование, сетевые протоколы, версии стандартов и системы аутентификации предполагают собственные правила записи; некоторые из них переходят непосредственно в языковую форму термина.

Сетевые профессиональные ресурсы дают возможность наблюдать такие единицы в актуальном функционировании. MDN Web Docs фиксирует лексику веб-разработки [11], GitHub Docs - репозиториев, контроля версий и автоматизации [12], Microsoft Learn - программных платформ и облачных технологий [13]. NIST и OWASP предоставляют материал по нормативно-справочной терминологии кибербезопасности [14, 16]. Использование нескольких источников снижает зависимость корпуса от терминологии одной компании или технологической платформы и соответствует принципу «веб как корпус» [10].

Вместе с тем отобранные 248 единиц не дают основания говорить о статистическом преобладании какой-либо структурной модели во всей англоязычной цифровой терминологии. Для решения такой задачи необходим иной дизайн материала: частотно сбалансированный корпус, единые временные границы и полная количественная разметка каждого структурного класса.

В пределах настоящей выборки существеннее последовательность самих критериев классификации. Сопоставление *data center* и *database*, клиппинга *app* и бленда *webinar*, многокомпонентного *end-to-end encryption* и графически гибридного *2FA* подтверждает, что одного формального признака недостаточно для классификации. При разметке необходимо одновременно учитывать графическое оформление, состав компонентов и способ образования формы.

Заключение

В результате анализа 248 англоязычных терминологических единиц выделены семь структурных типов: простые и производные однословные термины, компаунды, многокомпонентные терминологические сочетания, аббревиатуры и акронимы, клиппинги, бленды и графические гибриды. Основанием для разграничения этих групп служил ведущий способ формальной организации единицы. Особенно важен этот метод оказался при классификации внешне сходных терминов, образованных разными способами.

Каждая из выделенных моделей имеет свои особенности организации номинации. Многокомпонентные сочетания последовательно уточняют специальное понятие, а компаунды объединяют несколько смысловых признаков в пределах одной лексической формы. Аббревиатуры и клиппинги сокращают уже существующее обозначение. При блендинге новая лексема формируется путем соединения фрагментов исходных основ.

Полная и сокращенная формы могут функционировать параллельно. В парах *artificial intelligence* и *AI*, *virtual private network* и *VPN*, *large language model* и *LLM* выбор формы связан с условиями употребления термина в профессиональной коммуникации. Развернутая номинация сохраняет большую семантическую прозрачность, а сокращенная форма удобна при повторном употреблении термина, уже известного адресату.

Отдельную группу составляют графические гибриды. В обозначениях *C++*, *IPv6*, *2FA*, *CI/C*D цифры и специальные символы входят в закрепленную форму термина. Эти примеры показывают, что графические средства могут непосредственно участвовать в структурной организации цифровой терминологии.

Наибольшего внимания при разметке потребовали пограничные случаи: число компонентов или наличие дефиса сами по себе не всегда позволяют однозначно определить структурный тип. Такие единицы разграничивались с учетом способа образования, графической самостоятельности компонентов и их функции в составе всей номинации.

Структурное разнообразие современной английской терминологии цифровых технологий формируется в результате нескольких параллельных процессов. Новое понятие может получать развернутое и семантически прозрачное обозначение, сокращаться по мере закрепления в профессиональном употреблении, объединять несколько основ в одной лексеме или включать элементы технической записи. Для количественного сопоставления продуктивности этих моделей в дальнейшем потребуется частотно сбалансированный корпус с полной структурной разметкой; представленная выборка служит основой для их последовательной классификации.

Список литературы:

1. Лейчик В. М. Терминоведение: предмет, методы, структура. — М.: ЛКИ, 2007. — 256 с.
2. Никулина Е. А. Терминологизмы и контекст (на материале современного английского языка) // Преподаватель XXI век. — 2013. — № 1. — Ч. 2. — С. 282–288.
3. Никулина Е. А. К типологии английских терминологизмов // Преподаватель XXI век. — 2015. — № 4. — Ч. 2. — С. 318–323.
4. Никулина Е. А., Соколова М. А. Опыт корпусного исследования английских субстантивных терминологизмов // Преподаватель XXI век. — 2024. — № 2. — Ч. 2. — С. 421–430.
5. Молнар А. А. Особенности формирования терминосистемы информационных технологий // Вестник Московского государственного лингвистического университета. — 2011. — № 620. — С. 90–107.
6. Plag I. Word-Formation in English. — Cambridge: Cambridge University Press, 2003.
7. Bauer L., Lieber R., Plag I. The Oxford Reference Guide to English Morphology. — Oxford: Oxford University Press, 2013. — 691 p.
8. Cabré M. T. Terminology: Theory, Methods and Applications / ed. by J. C. Sager; transl. by J. A. DeCesaris. — Amsterdam; Philadelphia: John Benjamins, 1999.
9. Temmerman R. Towards New Ways of Terminology Description: The Sociocognitive Approach. — Amsterdam; Philadelphia: John Benjamins, 2000. — 258 p.
10. Kilgarriff A., Grefenstette G. Introduction to the Special Issue on the Web as Corpus // Computational Linguistics. — 2003. — Vol. 29, No. 3. — P. 333–347.

11. MDN Web Docs. Glossary of web terms [Электронный ресурс]. — URL: https://developer.mozilla.org/en-US/docs/Glossary (дата обращения: 24.08.2026).
12. GitHub Docs [Электронный ресурс]. — URL: https://docs.github.com/en (дата обращения: 24.08.2026).
13. Microsoft Learn. Technical documentation [Электронный ресурс]. — URL: https://learn.microsoft.com/en-us/docs/ (дата обращения: 24.08.2026).
14. NIST Computer Security Resource Center. Glossary [Электронный ресурс]. — URL: https://csrc.nist.gov/glossary (дата обращения: 24.08.2026).
15. Cloudflare. Learning Center [Электронный ресурс]. — URL: https://www.cloudflare.com/learning/ (дата обращения: 24.08.2026).

OWASP Foundation. Secure Coding Practices: Glossary [Электронный ресурс]. — URL: https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/ (дата обращения: 24.08.2026).

Structural Models of Digital Technology Terms in Modern English

Kondrashova D.G.
Moscow Pedagogical State University, Institute of Foreign Languages, Department of Phonetics and Lexicology of the English Language named after V. D. Arakin
Moscow, Russia
e-mail: kondrasshovaa@yandex.ru

Annotation

The paper examines the structural organization of English digital technology terms using a targeted sample of 248 terminological units attested in professional, reference, and technical English-language resources. Each unit was classified according to its leading structural and word-formation mechanism; the corpus distinguishes simple and derived one-word terms, compounds, multiword terminological units, abbreviations and acronyms, clippings, blends, and graphic hybrids. The analysis reveals functional differences between these models: expanded multiword units provide stepwise conceptual specification, whereas abbreviation, clipping, blending, and compounding realize different forms of formal/lexical compression. Graphic hybrids demonstrate the influence of technical standards and digital notation on contemporary specialized nomenclature/terminological naming.

Keywords: *digital technologies; terminology; structural models; word-formation; compounding; multiword terms; abbreviation*

Для заметок

НАУЧНОЕ ИЗДАНИЕ
НАУЧНЫЙ СПЕКТР

№8 2026
www.sciencespectrum.ru

Реестровая запись от 15.07.2025 серия ПИ № ФС77-89760

Подписано в печать 25.09.2026 Формат А4. Печать цифровая.
Дата выхода в свет 25.09.2026

2,3 усл.печ.л. 2,5 уч.изд.л. Тираж 100 экз. Заказ 182.

Учредитель: ООО "Развитие":
420111, Республика Татарстан, г. Казань, ул. Университетская, д. 22,401

Адрес редакции, издательства, типографии – ООО "Развитие":
420111, Республика Татарстан, г. Казань, ул. Университетская, д. 22, 401

Цена - договорная
© ООО "Развитие"
mail@sciencespectrum.ru
Отпечатано с готового оригинал-макета
ООО "Развитие"