Обзорная статья
УДК 004.8, 04.49; DOI: 10.61260/2218-130X-2025-4-82-93

К ВОПРОСУ О ПРИМЕНИМОСТИ LLM В ЗАДАЧАХ УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ: ОБЗОР РЕЛЕВАНТНЫХ РАБОТ

Леонов Николай Викторович.
Государственный научно-исследовательский институт прикладных проблем, Санкт-Петербург, Россия.
✉**Буйневич Михаил Викторович.**
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия
✉***bmv1958@yandex.ru***

Аннотация. Работа посвящена общим вопросам применения больших языковых моделей в интересах решения стратегических задач в области информационной и кибербезопасности, а именно управления уязвимостями в программном обеспечении. Делается обзор top-10 релевантных научных статей российского сегмента на предмет решений (гипотетических и реализованных), построенных на базе языковых моделей и предназначенных для управленческих задач без привязки к конкретной предметной области. Производится сравнительный анализ результатов обзоров с позиции года публикации, области применения, конкретных решаемых задач и состояния их реализации, выбранных моделей, интеграции с системой и применяемой специфики. Делаются частные выводы, указывающие на рост актуальности и широкий охват предметных областей, разнообразие решаемых задач, сложность в реализации и популярность GPT от компании OpenAI, а также необходимость интеграции моделей в общую архитектуру системы (или, по крайней мере, в ее информационное хранилище). Отмечается возможность улучшения работоспособности моделей с помощью соответствующих надстроек. Итоговый общий вывод заключается в перспективности применения больших языковых моделей для решения задач управления уязвимостями в программном обеспечении.

Ключевые слова: информационная и кибербезопасность, программное обеспечение, уязвимость, управление, искусственный интеллект, большие языковые модели, LLM

Для цитирования: Леонов Н.В., Буйневич М.В. К вопросу о применимости LLM в задачах управления уязвимостями программного обеспечения: обзор релевантных работ // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2025. № 4. С. 82–93. DOI: 10.61260/2218-130X-2025-4-82-93.

Review article

ON THE APPLICABILITY OF LARGE LANGUAGE MODELS TO SOFTWARE VULNERABILITY MANAGEMENT: A REVIEW OF RELEVANT WORKS

Leonov Nikolay V.
State Research Institute of Applied Problems, Saint-Petersburg, Russia.
✉**Buinevich Mikhail V.**
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia
✉***bmv1958@yandex.ru***

Abstract. This paper examines the general application of large-scale language models to address strategic issues in information and cybersecurity, specifically software vulnerability management. A review of the top-10 relevant scientific articles in the Russian segment examines solutions (hypothetical and implemented) based on language models and designed for management tasks regardless of the specific subject area. A comparative analysis of the review results is provided based on the year of publication, the application area, the specific tasks being solved and their implementation status, the selected models, integration with the system, and the specifics of the application. Specific conclusions are drawn, highlighting the growing relevance and broad coverage of subject areas, the diversity of the tasks being solved, the implementation complexity and popularity of OpenAI's GPT, and the need to integrate models into the overall system architecture (or at least into its information warehouse). The possibility of improving the performance of models using appropriate add-ons is noted. The final general conclusion is that large-scale language models hold promise for solving software vulnerability management problems.

Keywords: information & cubersecurity, software, vulnerability, management, artificial intelligence, large language models, LLM

For citation: Leonov N.V., Buinevich M.V. On the applicability of large language models to software vulnerability management: a review of relevant works // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2025. № 4. P. 82–93. DOI: 10.61260/2218-130X-2025-4-82-93.

Введение

Большие языковые модели (LLM, Large Language Model) стали неотъемлемой частью большого количества решений в современном мире, характеризуемом активным развитием и внедрением искусственного интеллекта (ИИ). Однако, исходя из относительной технологической молодости (хотя зарождение идеи и было в середине прошлого века, но конкретные реализации появились лишь в конце), их применение пока носит в основном прикладной характер, избегая стратегических областей, ошибки или необоснованность решений в которых носят критический или даже фатальный характер (например, для кибербезопасности [1]). Так, например, интеллектуальные помощники для разработки программного обеспечения (ПО) или чат-боты для общения с клиентами уже стали элементами повседневной жизни из-за адаптированности ответов под конкретного пользователя, а также возможности проверки и корректировки результатов. Однако такие эффекты, как «галлюцинирование» [2], отсутствие «истинного» понимания и ответственности программного средства на базе LLM и др., пока ограничивают их применение в медицине, юриспруденции, военной и других областях. Далее приводятся результаты обзора работ по применению LLM для решения разнообразных высокоуровневых задач в различных областях, к которым относится и управление уязвимостями в ПО, активно развиваемое одним из авторов статьи [3, 4].

Эта сложная, динамичная и критически важная область кибербезопасности характеризуется следующими особенностями. Во-первых, масштаб и сложность – огромные объемы данных (исходный код, зависимости, отчеты сканеров, базы уязвимостей вроде CVE), которые необходимо анализировать быстро и контекстно. Во-вторых, мультизадачность – включает обнаружение (статический/динамический анализ), оценку (приоритизацию по критичности, «эксплойтабельности», контексту бизнеса), ремедиацию (поиск и генерацию патчей, обновление зависимостей), отслеживание и коммуникацию. В-третьих, высокие риски – ошибки в приоритизации или пропуск критической уязвимости ведут к серьезным последствиям (вплоть до компрометации системы). В-четвертых, центральная роль эксперта – область традиционно требует высокой квалификации (исследователь кибербезопасности, аналитик), которая в дефиците, при этом многие процессы рутинны и трудоемки. И, в-пятых, эволюция угроз – постоянно появляются новые векторы атак и уязвимости (0-day), что требует оперативной адаптации.

Обзор работ

Проведен обзор 10 наиболее релевантных научных статей, представленных в базе РИНЦ и отобранных с помощью встроенной поисковой системы по следующим запросам – «LLM управление» и «языковая модель управление» (при поиске с учетом морфологии).

Исследование [5] посвящено вопросу построения экспертных систем предприятия, основанных на применении LLM; основным назначением таких систем является обучение сотрудников организации. В работе производится сравнительный обзор моделей GPT-4o, DeepSeek V3 и Qwen2.5-Max в процессе решения ими тестовых задач, созданных по техническим документам и стандартам предприятия. В интересах обоснования применимости моделей создан прототип системы, основанной на RAG-технологии (от англ. Retrieval-Augmented Generation, что означает дополнение запроса и генерацию ответа с учетом дополнительной релевантной информации из отдельной базы знаний); тем самым обеспечивается интеграция рассмотренных моделей с хранилищами данных организации. Обоснована перспективность использования LLM как элемента экспертных систем.

В работе [6] предложена концептуальная модель системы управления цифровым двойником строительного проекта, использующая LLM; при этом рассматриваются и учитываются все этапы жизненного цикла строительства. Предложено отвести модели роль как анализа состояния процесса строительства, так и синтеза управленческих решений, а также прогнозирования аномалий в поведении субъектов управления. Тем самым осуществлена «бесшовная» интеграция новых решений на базе LLM в существующие экспертно-алгоритмические механизмы проектов в строительной области.

Управление знаниями организации (в части их поиска, структурировании и передачи) за счет использования LLM рассмотрено в статье [7]. Основной целью такого применения является оптимизация бизнес-процессов, учитывающая в том числе и экономические затраты на сами LLM, а также вопросы безопасности обрабатываемых ими данных. Выделены такие аспекты внедрения LLM, как интеграция с внутренними хранилищами организации, этапность, контроль качества, информационная безопасность, а также метрики и оценки итоговой эффективности после внедрения. Указаны следующие проблемы, характерные для применения LLM: доверие результатам (в том числе интерпретируемость процесса их «интеллектуального» получения), конфиденциальность данных, потребность в высоких аппаратных мощностях и снижение задействования экспертов (как контролирующей ступени решения).

В исследовании [8] произведен анализ этапов развития процессов управления финансовой составляющей организации за счет применения информационных технологий, одним из направлений в которых является ИИ. Приводится статистика, согласно которой к началу 2025 г. лишь 10–15 % финансовых организаций для управления своими процессами применяют LLM. Отмечены следующие проблемные вопросы такого внедрения: высокая

стоимость, отсутствие необходимых специалистов поддержки, интеграция в уже существующие решения, качество и достоверность данных, сопротивление сотрудников интеллектуальным инновациям. Введен ряд финансовых показателей, позволяющих оценивать эффективность замены классических решений финансового сектора на цифровые.

Интеллектуальной системе поддержки принятия решений (СППР) по управлению процессами производства в типовой металлургической компании посвящена работа [9]. Для этого спроектирован и реализован чат-бот вопрос-ответного типа на базе больших популярных LLM – Llama 2.7 и GPT-4; также произведено дообучение моделей с помощью RAG-технологии. Выявленные при работе «галлюцинации» устранялись за счет применения терминологического словаря металлургической области. Произведена базовая оценка работы двух указанных моделей, которая позволила сделать вывод об увеличении качества их работы на 16 % в случае использования словаря.

В работе [10] решается задача сбора и анализа данных о предметной области, которая является одной из первоочередных в любых системах управления, а не только относящихся к рассматриваемому в исследовании рынку труда Республики Беларусь. Проверяется гипотеза касательно большей эффективности методов на базе LLM по сравнению с классическими алгоритмическими – парсингом Интернет-сайтов, использованием API к информационным базам и чтением RSS-каналов. В качестве предпосылки этого указывается адаптированность моделей к неструктурированным данным, глубокое «понимание» контекста, наличие единого интерфейса, обработка больших объемов за счет масштабирования, возможность оптимизации пред обучением. Произведено качественное сравнение указанных методов сбора и анализа данных по следующим критериям: оперативность получения, качество работы, простота использования, масштабируемость и стоимость. Сделан вывод касательно превосходства RSS-каналов по сравнению с остальными методами; при этом LLM с существенным отставанием находятся на последнем месте (таким образом, гипотеза опровергается). Вторым направлением в исследовании является ранжирование производительности top-10 моделей с использованием оценок ряда показателей согласно публичному проекту Artificial Analysis на сайте Hugging Face [11]; итоговый рейтинг моделей на момент написания статьи является следующим: GPT–4o, Claude 3 Opus, Mistral Medium, Gemini 1.0 Pro, Mixtral 8x7B, Llama 3 (70B), Open Chat 3,5, DeepSeek-V2, DBRX, Arctic. Обоснована применимость LLM для решения бизнес-задач, top -3 которых составили GPT–4o, Claude 3 Opus и Gemini 1.0 Pro. Предложены следующие возможности применения моделей для управления человеческими ресурсами: адаптация требований вакансий под актуальные тренды, оптимизация программ обучения сотрудников, планирование будущих потребностей, оценка эффективности персонала и др.

Применению RAG-технологии для ИИ-помощника в типовой организации посвящена тезисная статья [12]; его функциональность заключается в предоставлении ответов на вопросы, включающие не только консультирование отдельных сотрудников, но и решение управленческих задач. Указаны такие проблемные вопросы применения ИИ-помощников, как необходимость в качественных данных, актуализация информационных хранилищ, высокие требования к аппаратной части и наличие эффекта «галлюцинирования». Аналогичным образом, работа [13] в краткой форме рассматривает возможность применения LLM для «социально-ответственных управленческих решений» при формировании развития компанией, реализующей ESG-стратегию [14] – прозрачность работы, а также ответственность по отношению к окружающей среде и социуму.

Оптимизация бизнес-процессов организации с применением LLM в интересах повышения эффективности выработки и принятия управленческих решений рассмотрена в работе [15]. В качестве основных областей применения приводятся такие, как обработка запросов, автоматизация внутренней коммуникации, анализ документов, обучение сотрудников и интеллектуализация подсистемы поддержки принятия решений. Выделены проблемы применения данной технологии, заключающиеся в интерпретируемости способов получения решений, высоких требованиях к аппаратной составляющей, наличии эффекта

галлюцинирования, обеспечении информационной безопасности и этически-правовых аспектов и др. Указана необходимость не обособленного применения LLM, а их интеграция в существующие (традиционные) решения.

В работе [16] синтезирована модель управления информацией металлургического мероприятия на всех этапах ее использования. Дается аналитическая запись модели в виде графа как совокупности взаимодействующих подсистем управления знаниями. Интеграция знаний в единую информационную плоскость осуществляется с помощью эмбендинга (то есть преобразования текста в набор числовых векторов, отражающих их смысловую близость) на базе ruBERT. В аспекте применения модели к металлургической области алгоритм ее работы состоит из получения данных от подсистем, построения графа взаимодействия, эмбендинга, объединения в единую базу данных, поиска знаний с применением LLM и формирования итогового результата. Созданный прототип и его экспериментальное исследование при обработке информации (с получением численных оценок) обосновали работоспособность и базовую эффективность модели.

Систематизация

Проведена систематизация результатов обзора отобранных научных статей с использованием следующих критериев в аспекте применения LLM для решения задач управления (с комментариями касательно возможных значений):

К_1 – область, предлагаемая для применения LLM (общая в случае – любая типовая организация);

К_2 – задача управления, решаемая с помощью LLM;

К_3 – состояние решения на базе LLM (обзор, анализ, концепция, прототип, продукт);

К_4 – указание конкретных LLM, рассмотренных для решения задач (их перечисление, иначе отметка «не указано»);

К_5 – место интеграции LLM в существующие (традиционные) решения (отсутствует, архитектура, процессы, хранилища данных, не указано);

К_6 – специфика и особенности применения LLM (RAG-технология и др.).

Результаты такого критериального сравнения представлены в таблице.

Таблица

Результаты критериального сравнения применения LLM (согласно обзора)

Название	Год	К_1	К_2	К_3	К_4	К_5	К_6
Исследование возможностей модели LLM: новые горизонты генерации текста [5]	2025	Организация	Обучение персонала	Анализ предметной области	GPT-4o, DeepSeek V3, Qwen2.5-Max	Хранилища данных	–
Концептуальная модель системы управления цифровыми двойниками проекта строительства из крупногабаритных железобетонных модулей на основе больших языковых моделей [6]	2024	Строительство	Управление проектом	Концепция	Не указано	Процессы	–
Роль больших языковых моделей в оптимизации бизнес-процессов и управлении знаниями в корпоративных структурах [7]	2024	Организация	Оптимизация бизнес-процессов	Анализ предметной области	Не указано	Хранилища данных	–

Название	Год	К_1	К_2	К_3	К_4	К_5	К_6
Анализ применения цифровых технологий в управлении финансами организаций [8]	2025	Организация	Финансовый менеджмент	Обзор	Не указано	Архитектура	–
Интеллектуальная поддержка принятия управленческих решений в MES-системах с использованием больших языковых моделей [9]	2024	Металлургия	Управление производством в реальном времени	Прототип	Llama 2.7, GPT-4	Хранилища данных	RAG
Современные методы сбора и обработки информации о рынке труда и направления их использования в практике управления человеческими ресурсами [10]	2024	Организация	Сбор и анализ данных, решение бизнес-задач	Анализ предметной области	GPT–4o, Claude 3 Opus, Mistral	Архитектура	–
Методы и технологии повышения эффективности работы организации на основе ИИ [12]	2025	Организация	Оптимизация бизнес-процессов	Анализ предметной области	Не указано	Хранилища данных	RAG
Инновационные подходы к реализации ESG-стратегий: роль больших языковых моделей в инвестиционной и корпоративной практике [13]	2025	Организация	Внедрение инноваций	Анализ предметной области	Не указано	Не указано	ESG
Оптимизация бизнес-процессов с помощью LLM [15]	2025	Организация	Оптимизация бизнес-процессов	Анализ предметной области	Не указано	Не указано	–
Модель управления знаниями металлургического предприятия на основе эмбединговых моделей [16]	2025	Металлургия	Управление знаниями	Прототип	Не указано	Архитектура	ruBERT

Анализ полученной систематизации позволил сделать следующие частные выводы.

Во-первых, из всех десяти статей четыре опубликованы в 2024 г., а шесть – в 2025 г., что может говорить не только об актуальности применения LLM в последние два года, но и о постоянном увеличении ее роста (с учетом того, что еще не все публикации текущего года проиндексированы в РИНЦ). Таким образом, можно предположить еще бóльшее увеличение количества исследований по данной теме.

Во-вторых, основной областью применения является достаточно общая – управление организацией, ее процессами и данными (семь статей); также отдельный интерес к моделям проявляется в металлургической области (две статьи) и строительстве (одна статья). Следовательно, что закономерно, исходя из широкого предназначения моделей [17, 18], специфика предметной области их применение существенно не ограничивает.

В-третьих, область управленческих задач, решаемых (или предлагаемых) с помощью LLM, крайне разнообразна – только различные аспекты оптимизации бизнес-процессов встречаются сразу в трех статьях. То есть, LLM применимы для широкого круга задач, оптимальность выполнения которых находится на переднем плане.

В-четвертых, упоминания каких-либо готовых (так как «коробочных») продуктов в публикациях найдено не было – в основном проводились теоретические исследования (шесть раз анализ предметной области и один раз общий обзор), а также создавалась общая концепция (в одной статье); и лишь в двух работах описаны и протестированы работоспособные программные прототипы. Все это позволяет говорить об определенной сложности в реализации полноценных решений (в том числе, вычислительного генеза).

В-пятых, из всех наборов LLM, которые упоминались в статьях, лишь продукт GPT-4o встречается повторно (три раза). Его компания-производитель OpenAI традиционно славится топовыми разработками в области ИИ [19]. Следует уточнить, что в работе [10] приводится, в том числе, сравнение top-10 моделей, которые в текущем анализе не учитывались из-за отсутствия ориентации на задачи управления.

В-шестых, с позиции интеграции LLM в систему, решающую задачи управления, с небольшим перевесом (в одну статью) указываются хранилища данных, за которыми идет общая архитектура системы (то есть данные и процессы управления); и лишь в одной статье упоминаются отдельно процессы. Таким образом, текущий тренд интеграции LLM в традиционные системы управления состоит в переходе от «вспомогательно-аналитических» к «управляюще-исполнительным» функциям, что отражает стремление к прагматичности индустрии с точки зрения новаций.

И, в-седьмых, можно отметить такие особенности применения LLM, как наличие «надстроек» в виде RAG-технологий (две статьи), а также применение эмбендинга и ориентация на типовые стратегии управления (по одной статье). То есть, практическое применение LLM чаще всего связано с указанной технологией, что также указывает на текущие тренды и пробелы в исследуемой области.

Резюмирование сделанных выводов может быть представлено в виде следующих тезисов (по каждому критерию): ощутимо растущая актуальность LLM, широкая область применения, разнообразие решаемых задач, сложность в реализации, популярность модели GPT, постепенная интегрируемость в критические процессы управления через данные, применение дополнительных надстроек.

Обсуждения

Как можно видеть, область управления уязвимостями ПО находится вне зоны публикационной активности в контексте LLM (по крайней мере, в российском сегменте), однако выше сделанные выводы, в частности о широкой области применения, позволяют предположить некие точки приложения их возможностей для решения этой стратегической задачи кибербезопасности.

Во-первых, управление уязвимостями – это изначально работа с данными (код, CVE, лог-файлы). LLM можно безопасно интегрировать как аналитический движок поверх этих данных, не заменяя собой критическое решение (например, развертывание патча), но сильно помогая его принять. Поэтому *тезис* «Постепенная интегрируемость в критические процессы управления через данные» корреспондирует с такой *характеристикой* предметной области управления уязвимостями ПО как «Масштаб и сложность данных».

Во-вторых, LLM может закрывать *характеристику* «Мультимодальность» управления уязвимостями ПО как множество рутинных задач предметной области, а именно: классифицировать уязвимости по описанию CVE, переводить технические отчеты для менеджеров, предлагать векторы исправления в коде, интегрировать результаты сканирования, на что явно указывает *тезис* «Разнообразие решаемых задач».

В-третьих, «сырая» LLM не может быть доверенной в критичных решениях из-за галлюцинаций, поэтому необходимы настройки и надстройки (*тезис* «Применение дополнительных надстроек»), например, RAG-технология для доступа к актуальным базам CVE, агентские фреймворки для проверок, fine-tuning (то есть тонкая настройка) на security-датасетах. Это делает реализацию действительно ментально трудоемкой (в подтверждение *тезиса* «Сложность в реализации»), но крайне необходимой ввиду «Высоких рисков» при решении задач управления уязвимостями ПО как *характеристики* предметной области.

В-четвертых, наличие мощных, доступных через API открытых LLM (типа GPT – *тезис* «Популярность модели GPT») дает стартовую точку для экспериментов и быстрого создания прототипов инструментов для экспертов и аналитиков по кибербезопасности (*характеристика* «Роль эксперта»), снижая порог входа в предметную область. LLM действует как «силовой множитель» (от англ. force multiplier), беря на себя рутину и ускоряя работу аналитиков с огромными объемами неструктурированных данных (логи, CVE, отчеты), а будучи «дообучены» – становятся ассистентом эксперта, доступным 24/7.

В-пятых, традиционные сигнатурные методы явно отстают от динамики киберугроз. LLM, обученные на большом корпусе кода и соответствующей технической литературы, могут выявлять новые, сложные паттерны уязвимостей и адаптироваться к новым языкам/фреймворкам быстрее, чем «правило-базированные» системы – их актуальность (*тезис* «Ощутимо растущая актуальность LLM») растет вместе с проблемой (*характеристика* «Эволюция угроз».

Таким образом, предметная область «Управление уязвимостями ПО» является чуть ли не «идеальным» кандидатом для применения LLM именно в той парадигме, которая выявлена в обзоре. Исходя из частных выводов, можно сделать основой вывод касательно стратегических задач управления уязвимостями в ПО, который заключается в перспективности применения для их решения LLM; при этом внедрение моделей можно непосредственно производить в саму архитектуру соответствующей СППР отдельным модулем, а дополнительную оптимизацию осуществлять необходимыми надстройками над этим модулем.

Заключение

Проведенный обзор и последующий анализ десяти наиболее релевантных научных работ российского сегмента позволили подвести итоги исследования о применимости LLM в стратегических задачах управления [20], с фокусом на область управления уязвимостями ПО.

В отличие от существующих обзоров, сфокусированных на технических аспектах LLM или их применении в узких задачах (например, генерации кода), данная работа впервые осуществляет целенаправленную систематизацию российских исследований по применению LLM именно для управленческих задач общего характера. Это позволило выявить специфические для данной предметной области тренды, неочевидные при рассмотрении LLM в отрыве от контекста управления. На основе сравнительного анализа установлено, что доминирующей и принципиально новой парадигмой интеграции LLM в критические системы управления является экспансия на управляющие функции: от усиления экспертов до автономного принятия интеллектуальных решений – это ключевое теоретическое положение, уточняющее путь внедрения ИИ в стратегические задачи управления уязвимостями ПО.

Доказано, что выявленные в обзоре характеристики применения LLM (работа с большими объемами неструктурированных данных, мультизадачность, необходимость надстроек типа RAG) сильно коррелируют с ключевыми вызовами предметной области (масштаб данных, мультизадачность, эволюция угроз, дефицит экспертов).

Практическая значимость полученных результатов состоит в том, что они задают конкретное направление для создания специализированных инструментов в помощь (и местами – на замену) экспертами по безопасности кода и указывают на критическую важность применения технологий типа RAG и «дообучения», что позволяет сфокусировать ресурсы на решении актуальных проблем, а не на базовой адаптации моделей.

Таким образом, проведенное исследование подтверждает высокую перспективность применения LLM для трансформации управления уязвимостями ПО, задает теоретические рамки и практические ориентиры для этой трансформации и очерчивает конкретные направления для последующей научно-исследовательской и опытно-конструкторской работы. В качестве перспективных направлений дальнейших исследований можно отметить создание и апробацию архитектур модулей на базе LLM для интеграции в СППР по управлению уязвимостями ПО, а также проведение сравнительных экспериментов по оценке точности, полноты и скорости работы различных LLM на конкретных задачах жизненного цикла управления уязвимостями.

Список источников

1. Адилжанова С.А., Курасбек А.Н., Кенжебаева М.О. Применение LLM в кибербезопасности: обзор приложений и уязвимостей LLM // Вестник Академии гражданской авиации. 2025. № 3 (38). С. 118–136. DOI: 10.53364/24138614_2025_38_3_10.

2. Иванов В.О. Механизмы возникновения и подавления фактологических искажений в авторегрессионных языковых моделях // Нейрокомпьютеры: разработка, применение. 2025. Т. 27. № 3. С. 40–48. DOI: 10.18127/j19998554-202503-06.

3. Леонов Н.В. Методология и элементы технологии моделирования стратегических задач управления уязвимостями в ПО. Часть 1. Концептуальные основы и онтологическая модель // Защита информации. Инсайд. 2025. № 3 (123). С. 17–21.

4. Леонов Н.В. Методология и элементы технологии моделирования стратегических задач управления уязвимостями в ПО. Часть 2. Имитационное моделирование и оценка состояния // Защита информации. Инсайд. 2025. № 4 (124). С. 56–61.

5. Бондаренко Е.В., Шумаков М.В., Ильиных Е.В. Исследование возможностей модели LLM: новые горизонты генерации текста // Экономическое развитие России. 2024. Т. 31. № 3. С. 83–85. DOI: 10.6060/ivecofin.2025653.738.

6. Амбарцумян С.А., Мочалин Д.Е. Концептуальная модель системы управления цифровыми двойниками проекта строительства из крупногабаритных железобетонных модулей на основе больших языковых моделей // Строительное производство. 2024. № 4. С. 17–22. DOI: 10.54950/26585340_2024_4_17.

7. Булаев Я.А., Бурцев Д.С. Роль больших языковых моделей в оптимизации бизнес-процессов и управлении знаниями в корпоративных структурах // Журнал монетарной экономики и менеджмента. 2025. № 7. С. 72–80. DOI: 10.26118/2782-4586.2025.36.39.009.

8. Мицич А.Д. Анализ применения цифровых технологий в управлении финансами организаций // Вестник евразийской науки. 2025. Т. 17. № S2.

9. Добренко Н.В., Добренко Д.А., Улизько М.В. Интеллектуальная поддержка принятия управленческих решений в MES-системах с использованием больших языковых моделей // Экономика. Право. Инновации. 2024. № 3. С. 47–59. DOI: 10.17586/2713-1874-2024-3-47-59.

10. Калиновская И.Н. Современные методы сбора и обработки информации о рынке труда и направления их использования в практике управления человеческими ресурсами // Вестник Витебского государственного технологического университета. 2024. № 2 (48). С. 82–101. DOI: 10.24412/2079-7958-2024-2-82-101.

11. Ait A., Izquierdo J.L.C., Cabot J. HFCommunity: A Tool to Analyze the Hugging Face Hub Community // The proceedings of IEEE International Conference on Software Analysis, Evolution and Reengineering (Taipa, Macao, 21–24 March 2023). 2023. P. 728–732. DOI: 10.1109/SANER56733.2023.00080.

12. Березовский Б.Ю. Методы и технологии повышения эффективности работы организации на основе искусственного интеллекта // Вестник науки. 2025. Т. 3. № 6 (87). С. 1687–1693.

13. Стрижов С.А., Беляева И.Ю., Абрамович С.Ю. Инновационные подходы к реализации ESG-стратегий: роль больших языковых моделей в инвестиционной и корпоративной практике // Инновации и инвестиции. 2025. № 10. С. 23–25.

14. Teja K.R., Liu C.-M. ESG Investing: A Statistically Valid Approach to Data-Driven Decision Making and the Impact of ESG Factors on Stock Returns and Risk // IEEE Access. 2024. Vol. 12. P. 69434–69444. DOI: 10.1109/ACCESS.2024.3401873.

15. Андрончик Г.В. Оптимизация бизнес-процессов с помощью LLM // Universum: технические науки. 2025. № 5-1 (134). С. 15–20.

16. Веденеев В.А., Ершов Е.В., Ковыршин Р.Г. Модель управления знаниями металлургического предприятия на основе эмбединговых моделей // Вестник Череповецкого государственного университета. 2025. № 3 (126). С. 7–16. DOI: 10.23859/1994-0637-2025-3-126-1.

17. Антипова С.А., Тляшев О.М. Перспективы применения мультимодальных моделей искусственного интеллекта в системах поддержки и принятия решений военного назначения // Военная мысль. 2024. № 6. С. 117–128.

18. Ковалёв А.К., Панов А.И. Применение предобученных больших языковых моделей в задачах воплощенного искусственного интеллекта // Доклады Российской академии наук. Математика, информатика, процессы управления. 2022. Т. 508. № 1. С. 94–99. DOI: 10.31857/S268695432207013X.

19. Butgereit L. A Comparison of Three AI Tutoring Bots Communicating in isiZulu Using OpenAI's GPT-3.5-turbo, GPT-4-turbo, and GPT-4o // The proceedings of IST-Africa Conference (Nairobi, Kenya, 28–30 May 2025). 2025. P. 1–8. DOI: 10.23919/IST-Africa67297.2025.11060061.

20. Матвеев А.В., Иванов А.Ю. Использование больших языковых моделей в области безопасности в чрезвычайных ситуациях: обзор исследований и анализ возможностей // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2025. № 3. С. 136–146. DOI: 10.61260/2218-130X-2025-3-136-146.

References

1. Adilzhanova S.A., Қurasbek A.N., Kenzhebaeva M.O. Primenenie LLM v kiberbezopasnosti: obzor prilozhenij i uyazvimostej LLM // Vestnik Akademii grazhdanskoj aviatsii. 2025. № 3 (38). S. 118–136. DOI: 10.53364/24138614_2025_38_3_10.

2. Ivanov V.O. Mekhanizmy vozniknoveniya i podavleniya faktologicheskikh iskazhenij v avtoregressionnykh yazykovykh modelyakh // Nejrokomp′yutery: razrabotka, primenenie. 2025. T. 27. № 3. S. 40–48. DOI: 10.18127/j19998554-202503-06.

3. Leonov N.V. Metodologiya i elementy tekhnologii modelirovaniya strategicheskikh zadach upravleniya uyazvimostyami v PO. Chast′ 1. Kontseptual′nye osnovy i ontologicheskaya model′ // Zashchita informatsii. Insajd. 2025. № 3 (123). S. 17–21.

4. Leonov N.V. Metodologiya i elementy tekhnologii modelirovaniya strategicheskikh zadach upravleniya uyazvimostyami v PO. Chast′ 2. Imitatsionnoe modelirovanie i otsenka sostoyaniya // Zashchita informatsii. Insajd. 2025. № 4 (124). S. 56–61.

5. Bondarenko E.V., Shumakov M.V., Il′inykh E.V. Issledovanie vozmozhnostej modeli LLM: novye gorizonty generatsii teksta // Ekonomicheskoe razvitie Rossii. 2024. T. 31. № 3. S. 83–85. DOI: 10.6060/ivecofin.2025653.738.

6. Ambartsumyan S.A., Mochalin D.E. Kontseptual′naya model′ sistemy upravleniya tsifrovymi dvojnikami proekta stroitel′stva iz krupnogabaritnykh zhelezobetonnykh modulej na osnove bol′shikh yazykovykh modelej // Stroitel′noe proizvodstvo. 2024. № 4. S. 17–22. DOI: 10.54950/26585340_2024_4_17.

7. Bulaev Ya.A., Burtsev D.S. Rol′ bol′shikh yazykovykh modelej v optimizatsii biznes-protsessov i upravlenii znaniyami v korporativnykh strukturakh // Zhurnal monetarnoj ekonomiki i menedzhmenta. 2025. № 7. S. 72–80. DOI: 10.26118/2782-4586.2025.36.39.009.

8. Mitsich A.D. Analiz primeneniya tsifrovykh tekhnologij v upravlenii finansami organizatsij // Vestnik evrazijskoj nauki. 2025. T. 17. № S2.

9. Dobrenko N.V., Dobrenko D.A., Uliz′ko M.V. Intellektual′naya podderzhka prinyatiya upravlencheskikh reshenij v MES-sistemakh s ispol′zovaniem bol′shikh yazykovykh modelej // Ekonomika. Pravo. Innovatsii. 2024. № 3. S. 47–59. DOI: 10.17586/2713-1874-2024-3-47-59.

10. Kalinovskaya I.N. Sovremennye metody sbora i obrabotki informatsii o rynke truda i napravleniya ikh ispol′zovaniya v praktike upravleniya chelovecheskimi resursami // Vestnik Vitebskogo gosudarstvennogo tekhnologicheskogo universiteta. 2024. № 2 (48). S. 82–101. DOI: 10.24412/2079-7958-2024-2-82-101.

11. Ait A., Izquierdo J.L.C., Cabot J. HFCommunity: A Tool to Analyze the Hugging Face Hub Community // The proceedings of IEEE International Conference on Software Analysis, Evolution and Reengineering (Taipa, Macao, 21–24 March 2023). 2023. P. 728–732. DOI: 10.1109/SANER56733.2023.00080.

12. Berezovskij B.Yu. Metody i tekhnologii povysheniya effektivnosti raboty organizatsii na osnove iskusstvennogo intellekta // Vestnik nauki. 2025. T. 3. № 6 (87). S. 1687–1693.

13. Strizhov S.A., Belyaeva I.Yu., Abramovich S.Yu. Innovatsionnye podkhody k realizatsii ESG-strategij: rol′ bol′shikh yazykovykh modelej v investitsionnoj i korporativnoj praktike // Innovatsii i investitsii. 2025. № 10. S. 23–25.

14. Teja K.R., Liu C.-M. ESG Investing: A Statistically Valid Approach to Data-Driven Decision Making and the Impact of ESG Factors on Stock Returns and Risk // IEEE Access. 2024. Vol. 12. P. 69434–69444. DOI: 10.1109/ACCESS.2024.3401873.

15. Andronchik G.V. Optimizatsiya biznes-protsessov s pomoshch′yu LLM // Universum: tekhnicheskie nauki. 2025. № 5-1 (134). S. 15–20.

16. Vedeneev V.A., Ershov E.V., Kovyrshin R.G. Model′ upravleniya znaniyami metallurgicheskogo predpriyatiya na osnove embedingovykh modelej // Vestnik Cherepovetskogo gosudarstvennogo universiteta. 2025. № 3 (126). S. 7–16. DOI: 10.23859/1994-0637-2025-3-126-1.

17. Antipova S.A., Tlyashev O.M. Perspektivy primeneniya mul′timodal′nykh modelej iskusstvennogo intellekta v sistemakh podderzhki i prinyatiya reshenij voennogo naznacheniya // Voennaya mysl′. 2024. № 6. S. 117–128.

18. Kovalyov A.K., Panov A.I. Primenenie predobuchennykh bol′shikh yazykovykh modelej v zadachakh voploshchennogo iskusstvennogo intellekta // Doklady Rossijskoj akademii nauk. Matematika, informatika, protsessy upravleniya. 2022. T. 508. № 1. S. 94–99. DOI: 10.31857/S268695432207013X.

19. Butgereit L. A Comparison of Three AI Tutoring Bots Communicating in isiZulu Using OpenAI\'s GPT-3.5-turbo, GPT-4-turbo, and GPT-4o // The proceedings of IST-Africa Conference (Nairobi, Kenya, 28–30 May 2025). 2025. P. 1–8. DOI: 10.23919/IST-Africa67297.2025.11060061.

20. Matveev A.V., Ivanov A.Yu. Ispol′zovanie bol′shikh yazykovykh modelej v oblasti bezopasnosti v chrezvychajnykh situatsiyakh: obzor issledovanij i analiz vozmozhnostej // Nauchno-analiticheskij zhurnal «Vestnik Sankt-Peterburgskogo universiteta Gosudarstvennoj protivopozharnoj sluzhby MChS Rossii». 2025. № 3. S. 136–146. DOI: 10.61260/2218-130X-2025-3-136-146.

Информация о статье:
Статья поступила в редакцию: 12.11.2025; одобрена после рецензирования: 14.12.2025;
принята к публикации: 15.12.2025

The information about article:
The article was submitted to the editorial office: 12.11.2025; approved after review: 14.12.2025;
accepted for publication: 15.12.2025

Информация об авторах:
Леонов Николай Викторович, начальник лаборатории Государственного научно-исследовательского института прикладных проблем (191167, Санкт-Петербург, наб. Обводного канала, д. 29), кандидат технических наук, доцент, e-mail: leonov-nv@yandex.ru, https://orcid.org/0000-0005-1295-5343, SPIN-код: 4986-8670
Буйневич Михаил Викторович, профессор кафедры прикладной математики и безопасности информационных технологий Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), доктор технических наук, профессор, e-mail: bmv1958@yandex.ru, https://orcid.org/0000-0001-8146-0022, SPIN-код: 9339-3750

Information about authors:
Leonov Nikolay V., chief of the State Research Institute of Applied Problems laboratory (191167, Saint-Petersburg, Obvodny Canal emb, 29), candidate of technical sciences, associate professor, e-mail: leonov-nv@yandex.ru, https://orcid.org/0000-0005-1295-5343, SPIN: 4986-8670,
Buinevich Mikhail V., professor department of applied mathematics and information technology security of Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), doctor of technical sciences, professor, e-mail: bmv1958@yandex.ru, https://orcid.org/0000-0001-8146-0022, SPIN: 9339-3750