Дата поступления рукописи в редакцию: 21.02.2026 г.
Дата принятия рукописи в печать: 07.04.2026 г.
DOI: 10.24412/2782-3849-2026-3-357-360

ЦАРЬКОВА Евгения Геннадьевна,
ведущий научный сотрудник ФКУ НИИ ФСИН России,
кандидат физико-математических наук,
e-mail: university69@mail.ru

ПРИМЕНЕНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ ЧАТ-БОТОВ ДЛЯ ФОРМИРОВАНИЯ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ СОТРУДНИКОВ ФСИН РОССИИ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. *Статья посвящена анализу аспектов применения чат-ботов на основе искусственного интеллекта для формирования и развития профессиональных компетенций сотрудников ФСИН России в сфере противодействия киберпреступности и обеспечения информационной безопасности. Рассматривается эволюция диалоговых систем – от сценарных ботов до решений, основанных на больших языковых моделях (LLM). Отдельное внимание уделено методологическим рекомендациям по интеграции таких систем в учебный процесс ведомственных образовательных учреждений, а также практическую деятельность органов и учреждений ФСИН России для повышения правовой и цифровой грамотности сотрудников.*

Ключевые слова: *уголовно-исполнительная система Российской Федерации, информационная безопасность, цифровая трансформация, информационные технологии, искусственный интеллект, диалоговый ассистент, искусственная нейронная сеть.*

TSARKOVA Evgeniya Gennadievna,
Senior Researcher of the Research Institute
of the Federal Penitentiary Service of Russia,
Candidate of Physico-mathematical Sciences

THE USE OF INTELLIGENT CHATBOTS FOR THE FORMATION OF PROFESSIONAL COMPETENCIES OF EMPLOYEES OF THE FEDERAL PENITENTIARY SERVICE OF RUSSIA IN THE FIELD OF COUNTERING CYBERCRIME AND ENSURING INFORMATION SECURITY

Annotation. *The article is devoted to the analysis of aspects of the use of chatbots based on artificial intelligence for the formation and development of professional competencies of employees of the Penal System in the field of countering cybercrime and ensuring information security. The evolution of dialog systems is considered, from scenario bots to solutions based on large language models (LLM). Special attention is paid to methodological recommendations for the integration of such systems into the educational process of departmental educational institutions, as well as the practical activities of the bodies and institutions of the Penal System to improve the legal and digital literacy of employees.*

Key words: *Penal System of the Russian Federation, information security, digital transformation, information technology, artificial intelligence, interactive assistant, artificial neural network.*

Цифровая трансформация и рост уровня киберугроз актуализируют необходимость повышения квалификации сотрудников правоохранительных органов, в том числе уголовно-исполнительной системы Российской Федерации (УИС). Обеспечение информационной безопасности в учреждениях УИС, противодействие киберпреступлениям, а также правовое сопровождение цифровых процессов требуют от сотрудников и курсантов ведомственных вузов не только глубоких специальных знаний, но и готовности оперативно работать с норматив-

но-правовой базой, методическими материалами и перечнем актуальных угроз для их своевременного купирования [1, с. 118]. Вместе с тем, традиционные формы обучения зачастую не успевают за динамикой изменения законодательства и тактик киберпреступников, при этом объем внутренних регламентов, инструкций и судебной практики делает ручной поиск информации затруднительным.

В данном контексте интеллектуальные диалоговые системы на основе архитектуры Retrieval-Augmented Generation (RAG) представляют собой перспективный инструмент для формирования и развития профессиональных компетенций сотрудников ФСИН России [2]. Такие системы способны предоставлять по запросу актуальные, точные и контекстуально релевантные ответы на вопросы, связанные с правовыми аспектами киберпреступлений, процедурами обеспечения информационной безопасности, особенностями расследования цифровых инцидентов в пенитенциарных учреждениях, а также с требованиями федерального законодательства (в частности, Федерального закона от 26.07.2017 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и др.).

Одним из вариантов создания программ-консультантов для автоматизации стандартных, предсказуемых задач и быстрого получения информации являются чат-боты, построенные на основе дерева интентов [3, с. 135]. Для создания таких диалоговых помощников доступен широкий спектр low-code платформ, не требующих использования программного кода для встраивания сценарного чат-бота в интерфейс сайта, социальной сети или месенджера. Чат-боты, построенные на древовидной архитектуре интентов, являются доминирующей моделью реализации диалоговых ассистентов в высших учебных заведениях. Такие системы функционируют посредством предварительного определения набора целевых категорий пользовательского взаимодействия, организованных в иерархическую структуру условных ветвлений. К преимуществам данного подхода можно отнести простоту разработки за счет использования визуальных конструкторов без необходимости написания программного кода, высокую предсказуемость поведения системы, предъявляемые минимальные вычислительные требования. Вместе с тем, указанный традиционный подход к разработке диалоговых систем в виде сценарных чат-ботов обладает существенными ограничениями в части гибкости и способности к обработке запросов в свободной форме [4, с. 261]. Отсутствие механизма семантического анализа в таких системах приводит к тому, что ассистент имеет возможность лишь шаблонного сопоставления входного текста с заранее определенными фразами, что делает его неспособным к работе с синонимичными формулировками запросов.

Качественным скачком в развитии диалоговых систем можно считать появление вопросно-ответных архитектур (QA), опирающихся на методы машинного обучения, в частности, на использование векторных представлений текста. При таком подходе система кодирует входной вопрос в многомерное векторное пространство и вычисляет меру семантической близости между вектором запроса и заранее векторизованными парами «вопрос-ответ». Однако при создании вопросно-ответных систем сохраняется основное ограничение: если в базе знаний отсутствует семантически близкий вопрос, QA-бот не способен будет выдать релевантный ответ.

Третье поколение диалоговых систем, представленное применением больших языковых моделей (Large Language Models, LLM), устранило необходимость в предварительной подготовке баз пар «вопрос-ответ» или жестких сценариев взаимодействия. Современные LLM-системы способны синтезировать ответы на основе своего параметрического знания, полученного в процессе обучения на больших текстовых корпусах. Появление больших языковых моделей открыло новые возможности для выдачи развернутых ответов на запросы пользователя, однако привело к возникновению известной проблемы генерирования недостоверной информации, появлению так называемых галлюцинаций искусственного интеллекта [5]. В качестве причин таких сбоев могут рассматриваться устаревание информации, на которой обучалась модель, а также отсутствие необходимых специфических фактов в обучающем корпусе текстов, что приводит к генерации ложной информации. При формировании учебного контента, получении юридических консультаций, в области безопасности стоимость рисков возникновения галлюцинаций становится неприемлемо высокой, что приводит к необходимости выработки механизмов, снижающих вероятность генерации нейросетью недостоверной информации [6].

Ключевым решением данной проблемы является применение RAG-подхода. Технология Retrieval-Augmented Generation (RAG), предложенная в 2021 году, объединила в рамках общей архитектуры контролируемое извлечение информации из документов и генерацию текста на основе LLM. Системы на основе RAG-архитектуры сочетают достоинства семантического поиска в нормативно-правовых документах с преимуществами открытой генерации.

RAG-система функционирует посредством трехстадийного процесса.

Первая стадия – Retrieval (извлечение релевантной информации). Процесс начинается с дробления имеющейся релевантной документации на семантически значимые фрагменты – чанки. Параметры данного этапа определяют производительность системы. Следующим подходом к разбиению документа на чанки является семантическое фрагментирование, использующее встраивание отдельных предложений и выявление границ между смысловыми блоками через анализ семантической близости соседних фрагментов. И, наконец, рекурсивное фрагментирование, сохраняющее иерархию исходного правового документа путем последовательного разбиения по логическим разделителям. Далее осуществляется векторизация и индексация. По окончании фрагментирования все чанки кодируются в векторное пространство фиксированной размерности, формируя векторную базу данных. Векторные базы данных используют алгоритмы приблизительного поиска ближайшего соседа для обеспечения оперативного поиска в больших корпусах документов, что является существенным преимуществом при создании приложений, работающих в режиме реального времени, где временная задержка неприемлема.

На второй стадии (Augmented, аугментация, расширение контекста) найденные чанки встраиваются в специальный текстовый запрос (промпт) вместе с исходным вопросом пользователя, что позволяет создать расширенный контекст, в котором языковая модель имеет доступ к релевантным достоверным фактам. При этом качественный промпт должен включать явное назначение роли диалоговой системы в рассматриваемом контексте, запрещать генерирование информации вне предоставленного контекста, предоставлять примеры желаемого формата ответа, а также содержать явные инструкции для обработки случаев, когда ответ отсутствует в обучающем корпусе текстов.

На третьей стадии (Generation) осуществляется генерация ответа большой языковой моделью по предоставленному промпту с учетом предоставленной пользователем информации. Здесь основным отличием данного процесса от безконтекстной генерации становятся ограничения модели, при которых ответ ограничивается информацией, содержащейся в контексте.

Целью настоящего исследования является анализ архитектурных и практических аспектов разработки и внедрения RAG чат-бота как инструмента оперативного консультирования и обучения сотрудников ФСИН России в области информационной безопасности и противодействия киберугрозам. На примере методологии построения подобной системы рассматриваются возможности low-code платформ для быстрого создания специализированных ассистентов, работающих на основе внутренних документов, правовых актов и методических материалов пенитенциарного ведомства.

Для реализуемого чат-бота «Киберконсультант ФСИН России» в качестве источников информации собрана и структурирована открытая документация, включающая нормативно-правовые акты, учебные и иные материалы по правовым основам и методикам обеспечения информационной безопасности в учреждениях УИС. Общий объем корпоративной документации составил порядка 350 страниц текста. Документы были предварительно загружены в систему, а в качестве интерфейса чат-бота выбран канал месенджера, подключенного с помощью токена.

Результатом исследования является реализация RAG-системы, обеспечивающей следующие функциональные возможности:

– консультирование по вопросам информационной безопасности и противодействию киберпреступности. Например, на вопрос типа «Способы идентификации фишинговых атак на ведомственные информационные ресурсы» система извлекает релевантные методические материалы и генерирует структурированный ответ с конкретными указаниями;
– методологическая поддержка;
– информационный поиск. Система эффективно локализирует информацию о способах защиты от атак на почтовые серверы, систему ведомственного электронного документооборота, доступных инструментах противодействия киберугрозам и др.

Использование RAG подхода при создании диалогового ассистента служит повышению точности получаемой информации, покрывает большую часть возможных пользовательских запросов, не требует непрерывного обновления, а применение каналов месенджеров в качестве интерфейса снижает трудозатраты на разработку диалоговой системы. Вместе с тем, построенный чат-бот не лишен недостатков. Как RAG-система, он включает риски по воспроизведению ошибок и неточностей, если исходная документация содержала ошибки, противоречия или устаревшую информацию. Поэтому важными направлениями работ является фаза подготовки, проведение качественного аудита загружаемой нормативно-правовой документации, выявление пробелов и противоречий, определение приоритетных сценариев защиты от киберугроз, а также регулярный мониторинг метрик качества языковой модели [7].

Таким образом, технология RAG представляет собой эффективный архитектурный паттерн для разработки интеллектуальных ассистентов в

интересах ФСИН России за счет строгой привязки ответов к актуальной нормативно-правовой и методической базе ведомства. На примере рассмотренного подхода показано, что даже без наличия значительного объема IT-специалистов возможно создание функционального чат-бота, который может выступать в роли оперативного консультанта по правовым аспектам киберпреступлений и требованиям информационной безопасности, быть инструментом методологической поддержки при расследовании инцидентов, связанных с цифровыми правонарушениями в учреждениях УИС, а также средством обучения и проверки знаний, предоставляющим сотрудникам и курсантам структурированные ответы на основе внутренних регламентов и учебных материалов в области киберпреступлений, включая соответствующую судебную практику.

Ключевыми условиями успешного внедрения подобной системы в деятельность органов и учреждений ФСИН России являются тщательный аудит и подготовка исходной документации (текстов законов, ведомственных приказов, инструкций, методических рекомендаций), а также формулировка четких промптов, требующих от языковой модели ссылок только на загруженные в систему источники. Практическая значимость работы заключается в предложении методологии, позволяющей сотрудникам учреждений и органов ФСИН России относительно быстро внедрять современные AI-решения для повышения правовой и цифровой грамотности личного состава, что в конечном итоге способствует повышению уровня комплексной безопасности в учреждениях УИС.

Список литературы:

[1] Голованова Н.А., Гравина А.А., Зайцев О.А. Уголовно-юрисдикционная деятельность в условиях цифровизации: монография. М.: ИЗиСП, КОНТРАКТ, 2019. 212 с.

[2] Царькова Е.Г., Кочкина О.В. Применение искусственного интеллекта при обработке данных в научной и образовательной деятельности Федеральной службы исполнения наказаний // Ведомости уголовно-исполнительной системы. 2022, № 9(244). С. 51-59.

[3] Царькова Е.Г. К вопросу формирования обучающих датасетов для выявления источников распространения экстремистского контента в сети Интернет // Научно-технический вестник Поволжья. 2024. № 3. С. 134-136.

[4] Пальянова Н.В. Использование искусственного интеллекта в сфере Legal Tech: современные возможности и перспективы // Социально-экономическое развитие и качество правовой среды: Труды VIII Моск. юрид. форума, XIX Междунар. науч.-прак. конф. Ч. 2. М.: МГЮА, 2021 С. 260-267.

[5] Понкин И.В. Государственное управление и регуляторное пространство в сфере искусственного интеллекта // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022, № 11 (99). С. 108-116.

[6] Минбалеев А.В. Регулирование использования искусственного интеллекта в России // Информационное право. 2020. № 1. С. 36-39.

[7] Понкин И.В., Редькина А.И. Искусственный интеллект с точки зрения права // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2018. Т. 22, № 1. С. 91-109.

References:

[1] Golovanova N.A., Gravina A.A., Zaitsev O.A. Criminal jurisdictional activities in the context of digitalization: monograph. M.: IZiSP, CONTRACT, 2019. 212 pp.

[2] Tsarkova E.G., Kochkina O.V. The use of artificial intelligence in data processing in the scientific and educational activities of the Federal Penitentiary Service//Vedomosti of the penitentiary system. 2022, № 9(244). S. 51-59.

[3] Tsarkova E.G. On the formation of training datasets to identify sources of distribution of extremist content on the Internet//Scientific and Technical Bulletin of the Volga Region. 2024. № 3. S. 134-136.

[4] N.V. Palyanova. The use of artificial intelligence in the field of Legal Tech: modern opportunities and prospects//Socio-economic development and quality of the legal environment: Proceedings VIII Mosk. jurid. forum, XIX International. scientific-practical. conf. PART 2. M.: MOSCOW STATE LAW ACADEMY, 2021 S. 260-267.

[5] Ponkin I.V. Public administration and regulatory space in the field of artificial intelligence//Bulletin of the University named after O.E. Kutafina (MSLA). 2022, № 11 (99). S. 108-116.

[6] Minbaleev A.V. Regulation of the use of artificial intelligence in Russia//Information law. 2020. № 1. S. 36-39.

[7] Ponkin I.V., Redkina A.I. Artificial intelligence from the point of view of law//Bulletin of the Peoples' Friendship University of Russia. Series: Legal Sciences. 2018. VOL. 22, NO. 1. S. 91-109.