

Дата поступления рукописи в редакцию: 05.09.2026 г.

DOI: 10.24412/2782-3830-2026-10-75-78

Дата принятия рукописи в печать: 09.10.2026 г.

ЛОГИНОВ Валерий Викторович,

кандидат технических наук, доцент, профессор кафедры
безопасности в ЧС, Уральский институт ГПС МЧС
России, г. Екатеринбург,
e-mail: bazalt@mail.ru

ИСПОЛЬЗОВАНИЕ ДАННЫХ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОЦЕССЕ ПРИНЯТИЯ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ В ОБЛАСТИ ЗАЩИТЫ НАСЕЛЕНИЯ ОТ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

Аннотация. В статье рассмотрены принципы разработки алгоритмов взаимодействия человека и искусственного интеллекта для информационной поддержки принятия решений при возникновении чрезвычайных ситуаций. Обосновываются правила обращения к искусственному интеллекту при сборе данных об обстановке в зоне её возникновения. Изложены требования нормативных документов, касающихся защиты информации, в контексте работы с источниками информации, находящимися вне государственной юрисдикции. Делаются выводы о возможном использовании данных в системе обеспечения комплексной безопасности.

Ключевые слова: искусственный интеллект, принятие решений, информационная поддержка, защита информации, алгоритм взаимодействия.

LOGINOV Valery Viktorovich,

Candidate of Technical Sciences, Associate Professor,
Professor at the Department of Emergency Safety, Ural Institute
of State Fire Service of EMERCOM of Russia, Yekaterinburg

USE OF ARTIFICIAL INTELLIGENCE DATA IN MANAGERIAL DECISION-MAKING FOR POPULATION PROTECTION AGAINST EMERGENCIES

Annotation. The article examines the principles of developing algorithms for human-AI interaction to provide information support for decision-making during emergency situations. It outlines the rationale for engaging artificial intelligence when gathering data on the situation within the affected area. The requirements of regulatory documents regarding information protection are outlined in the context of working with information sources located outside state jurisdiction. Conclusions are drawn concerning the potential use of such data within a comprehensive security system.

Key words: artificial intelligence, decision-making, information support, information protection, interaction algorithm.

В современных условиях искусственный интеллект (ИИ) активно внедряется во все области деятельности современного общества. Его применение принципиально меняет функциональную структуру участия человека в тех или иных процессах, а также изменяет принципы использования информации, как основы принятия решений в том или ином виде деятельности [1].

При использовании ИИ в области принятия решений наиважнейшей его задачей является автоматизированный сбор данных аналитики о возможном (или свершившемся) событии в некой функционирующей структуре и влияния послед-

ствий этого события на цели функционирования данной структуры. Также от ИИ в идеале требуется не только оценка последствий, но и предложение вариантов решений, направленных на восстановление функционирования структуры.

Рассматривая возможности применения ИИ при принятии решений, важно учитывать масштаб охвата решением конкретной площади территории, с учетом её критической важности и количества населения, на ней находящегося. В системах национальной и региональной безопасности, полагаться на ИИ будет опрометчиво с точки зрения многообразия факторов, влияющих на безопас-

ность. Но при её обеспечении на муниципальном и, особенно на объектовом уровне, есть основания опираться на данные полученные при использовании ИИ.

Принципиально ИИ способен выполнить эту задачу, если в соответствующих базах данных будет необходимая информация, касающаяся свойств и параметров объекта, которые влияют на достижение системой безопасности целей функционирования. Можно представить базу данных, обрабатываемых ИИ, множеством:

$$Q_{ИИ} = \{q_1; q_2 \dots q_n\}$$

где:

q показатель параметра события;

n количество показателей.

Обработка ИИ этого множества, будет основой принятия решения на определенные действия, которые будут выполнены с определенной достоверностью I.

Между тем реальная обстановка будет характеризоваться множеством параметров, представляющим условную базу для принятия наиболее эффективного решения:

$$Q_{РО} = \{q_{P1}; q_{P2} \dots q_{Pn}\}$$

где:

qP реальный показатель параметра события;

nP количество показателей, оценивающих реальную обстановку.

Важно заметить, что для принятия обоснованных решений необходимо знать параметры обстановки, необязательно полностью соответствующие ей, но отклонения от их значений, не должны иметь влияния на общий замысел решения и пути достижения цели. Теоретически, для определения влияний отклонений параметров оценки обстановки, необходимо будет определить значимость отдельного показателя параметра ситуации:

$$i_n = \frac{q_n}{q_{Pn}} k_{Эn}$$

где:

kЭn показатель коэффициента веса пара-

метра события, причем

$$\sum_{i=1}^n k_{Эn} = 1.$$

В этом случае достоверность оценки ситуации, а значит, её влияние на эффективность принимаемого решения будет определяться выражением:

$$I = \sum_{i=1}^n i_n$$

При взаимодействии человека с ИИ нет необходимости пользоваться сложными формулами, тем не менее, они отражают общие принципы использования данных, генерируемых ИИ на современном уровне его развития. Анализируя выражения (1-4) можно определить основные принципы взаимодействия пользователя с ИИ:

специалисты дежурных служб реагирования на ситуации, вызывающие отклонения функционирования системы от штатного состояния должны иметь определённые алгоритмы взаимодействия с ИИ при возникновении конкретной ситуации;

при сборе данных о последствиях произошедшего события важно определить количество параметров n, как по данным ИИ, так и при докладах о ситуации с мест и данным автоматических датчиков:

при оценке ситуации необходимо определить факторы с наибольшей (критической) степенью влияния на обстановку kЭn;

при недостатке информации о параметрах сложившейся ситуации q, необходимым представляется поиск этой информации по косвенным признакам, в том числе на основе данных, предоставляемых ИИ.

При разработке алгоритмов взаимодействия человека с ИИ, для достижения целей системы защиты населения и территорий, необходимо будет опираться на существующую нормативно-правовую базу.

В этой связи необходимо четко определить правовой статус роли ИИ в общей системе поддержки принятия решений [2]. В таких системах, на любом уровне их функционирования, ответственность за принятое решение лежит на

руководителе, который полномочен принять решение. Это положение существенно повышает требования к информации, предоставляемой ИИ и квалификации лиц, разрабатывающих проекты решений. Требование к ИИ как к источнику информации основывается на принципах её достоверности и своевременности. В современной реальности ИИ, как самообучающаяся система, должен проводить анализ эффективности принятых решений по аналогичным ситуациям и проецировать их на запросы пользователей, в соответствии с имеющимися запросами. При этом нельзя не учитывать возможность злоумышленной атаки сгенерированными данными на модели ИИ, в результате которых они могут быть изменены под цели организаторов атаки. Требование своевременности информации может быть выполнено, только при доступе обработки ИИ данных датчиков параметров обстановки, что не всегда возможно по нормативно-правовым или техническим причинам. Поэтому любые данные ИИ должны подвергаться критическому анализу и подтверждаться данными реальной оперативной обстановки.

Оценивая возможности ИИ, многими авторами отмечаются его возможности по прогнозированию происшествий, влияющих на системы безопасности [3]. В области защиты населения и территорий от чрезвычайных особенно важными являются решения направленные на опережение проявления опасного фактора. Такие решения основаны на непрерывном мониторинге и обоснованных прогнозах возникновения угроз. Согласно выражению (2) эффективность таких решений будет зависеть от числа показателей реальной обстановки ПР, попавших в базу данных обработки ИИ. На объектовом и муниципальном уровнях, где число показателей сравнительно невелико, данные ИИ операторы дежурно-диспетчерских служб, могут соотнести с реальной обстановкой, в том числе используя накопленный профессиональный опыт. На более высоких уровнях функционирования систем безопасности, осмыслить оператором, все показатели, принятые для анализа ИИ, не представляется возможным, что может привести к неэффективному и ошибочному решению.

Важным аспектом взаимодействия пользователя с ИИ является защита информации, ввиду нахождения баз данных и средств их обработки вне юрисдикции государства. Защита информации, согласно приказу Федеральной службы по техническому и экспортному контролю от 11.04.2025 № 117 предусматривает взаимодействие пользователя и ИИ в формате строго заданных шаблонов вопросов и ответов, при обеспечении контроля соответствия ответов, установ-

ленным оператором шаблонам [4]. Фактически аналогичные требования установлены и для взаимодействия в формате свободной текстовой формы, где устанавливаются допустимые тематики и ведётся контроль соответствия им запросов пользователей.

Анализируя вышеизложенное, следует заметить, что установленные шаблоны будут влиять на полноту и целостность данных, необходимых для принятия обоснованных решений. Учитывая возможности, предоставляемые ИИ, необходимо при разработке шаблонов, учитывать невозможность передачи на общедоступные серверы информации, которая может снизить общее состояние безопасности. Если рассматривать общение с ИИ, как два информационных потока – встречный от ИИ и направленный к ИИ от оператора, то первый необходимо подвергать критическому анализу, соотносясь с данными реальной обстановки, а второй завуалировано маскировать шаблонными запросами, имея целью максимально скрыть масштабы ущерба и реальное состояние защиты объекта.

Эффективность решения, сгенерированного ИИ, также будет зависеть от адекватности модели, на основе которой оно предлагалось. Обычно она основывается на возможностях сил и средств, которые можно привлечь для восстановления функционирования нарушенной системы. Часто их состав и возможности могут быть предметом защиты информации, и в связи с этим необходимо четкое разделение в запросах к ИИ, информации способной нанести ущерб системе со стороны внешних сил и информации исключающей такую возможность. Например, запрос о возможном времени расчистки определённого количества завалов, группировкой техники, может дать представление не только о составе этой группировки, но и степени поражения объекта, что может быть крайне нежелательным в определенных условиях. При этом запрос о возможностях конкретной единицы техники по вывозу массы завалов, не дает представления о разрушениях.

Рассматривая использование ИИ для информационной поддержки принятия решений, нельзя не сказать о его возможности самообучаться и предлагать решения на основе опыта восстановления функционирования нарушенных систем [5]. Его возможности в этом случае имеют смысл использовать для оценки принимаемых решений. Он может представить определенные (открыто распространяемые) документы, издаваемые для защиты населения от воздействия неблагоприятных факторов в аналогичной ситуации. Также с его помощью можно проводить мониторинг социальных сетей, в которых имелось

обсуждение последствий происшествия и реагирование на него органов управления. Для оценки применения ИИ в практике информационной поддержки принятия решений по обеспечению безопасности важно иметь анализ его применения в реальной обстановке. Имея определенные модели реагирования на происшествия и шаблоны обращений к ИИ, можно довольно точно оценить его составляющую в объеме информации, принятой к сведению при обосновании соответствующих решений. В этой связи необходима оценка возможностей ИИ в предоставлении информации в сроки, регламентированные руководящими документами.

Оценивая уровень современного развития ИИ и тенденции его использования в различных видах деятельности можно сделать следующие выводы:

возможности ИИ в обязательном порядке должны быть использованы при принятии решений в области;

возможности ИИ при подготовке принятия решений, целесообразно использовать на локальном уровне, на более высоких уровнях, можно получить неоправданный риск больших ошибок;

при разработке алгоритмов взаимодействия человека с ИИ, необходимо учитывать его главное достоинство – быстроту получения информации, с учетом критического её осмысления;

должностные лица органов управления, отвечающих за сбор информации о текущей обстановке, должны иметь утверждённые алгоритмы, взаимодействия с ИИ;

важной частью этого взаимодействия являются мероприятия защиты информации.

Список литературы:

[1] Указ Президента РФ от 15.02.2024 N 124 "О внесении изменений в Указ Президента Российской Федерации от 10 октября 2019 г. N 490 "О развитии искусственного интеллекта в Российской Федерации" и в Национальную стратегию, утвержденную этим Указом" /п.4.

[2] Минбалеев А. В. Понятие «искусственный интеллект» в праве // Вестник Удмуртского университета. Серия «Экономика и право». 2022. Т. 32, № 6. С. 1094–1099.

[3] Газизов, А. Р. Роль искусственного интеллекта в улучшении обнаружения угроз / А. Р. Газизов, Р. Э. Хагуш // Педагогический вестник. – 2025. – № 36. – С. 13-15. – EDN ATQZCK.

[4] Приказ ФСТЭК России от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» /п.60.

[5] Ищейнов В.Я. Применение искусственного интеллекта в информационной безопасности/ Журнал Делопроизводство – 2024, № 2, с. 90–93.

References:

[1] Decree of the President of the Russian Federation No. 124 dated February 15, 2024, "On Amendments to Decree of the President of the Russian Federation No. 490 dated October 10, 2019, 'On the Development of Artificial Intelligence in the Russian Federation' and to the National Strategy Approved by Said Decree," Clause 4.

[2] Minbaleev A. V. The Concept of "Artificial Intelligence" in Law // Bulletin of Udmurt University. Series "Economics and Law." 2022. Vol. 32, No. 6. P. 1094–1099.

[3] Gazizov, A. R. The Role of Artificial Intelligence in Improving Threat Detection / A. R. Gazizov, R. E. Khagush // Pedagogical Bulletin. – 2025. – No. 36. – P. 13–15. – EDN ATQZCK.

[4] Order of the FSTEC of Russia No. 117 dated April 11, 2025, "On Approval of Requirements for the Protection of Information Contained in State Information Systems and Other Information Systems of State Bodies, State Unitary Enterprises, and State Institutions" / Clause 60.

[5] Ishcheynov V.Ya. Application of Artificial Intelligence in Information Security / *Deloproizvodstvo* Journal – 2024, No. 2, pp. 90–93.

