УДК 004.832.2
doi: 10.21685/2307-4205-2023-3-2

ОБЕСПЕЧЕНИЕ НАДЕЖНОСТИ В ЖИЗНЕННОМ ЦИКЛЕ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ОТВЕТСТВЕННОГО НАЗНАЧЕНИЯ

М. Ю. Михеев[1], О. В. Прокофьев[2], А. Е. Савочкин[3], И. Ю. Семочкина[4]

[1, 2, 3, 4] Пензенский государственный технологический университет, Пенза, Россия
[1] mix1959@gmail.com, [2] prokof_ow@mail.ru, [3] aebrat@mail.ru, [4] ius1961@gmail.com

Аннотация. *Актуальность и цели.* За последние несколько лет произошло резкое расширение возможностей систем искусственного интеллекта (ИИ), что одновременно привело к новым рискам и потенциальным преимуществам. Автономизация систем, позволяющая перейти от поддержки принятия решений к самостоятельной выработке решения, предоставляет противоречивые результаты в областях ответственного применения в таких чувствительных сферах применения, как здоровье человека, его экологическая среда проживания, экономический и социальный статус. В области вооружений обсуждаются средства создания автономных систем нового поколения и связанной с ними концепции будущей «гипервойны». *Материалы и методы.* Из-за растущего использования ИИ во всем мире в перечисленных чувствительных областях возникает запрос на надежность при использовании таких автономных систем. Необходимо сформулировать риски и преимущества этой технологии, включая соблюдение фундаментальных этических принципов. Применение критически важных решений должно контролироваться человеком, несущим ответственность. Меры по обеспечению надежности автономной системы с ИИ должны быть предусмотрены на всех этапах жизненного цикла и только таким образом можно контролировать риски и создавать объяснимый и управляемый ИИ. *Результаты и выводы.* Авторами изложена концепция понятия «надежного» ИИ и описана реализация отдельных ее положений на этапах жизненного цикла автономной системы ответственного назначения.

Ключевые слова: надежность системы искусственного интеллекта, система ответственного назначения, принятие решений автономной системой

Финансирование: работа выполнена в рамках гранта Российского научного фонда № 23-21-10046, https://rscf.ru/project/23-21-10046/

Для цитирования: Михеев М. Ю., Прокофьев О. В., Савочкин А. Е., Семочкина И. Ю. Обеспечение надежности в жизненном цикле систем искусственного интеллекта ответственного назначения // Надежность и качество сложных систем. 2023. № 3. С. 12–20. doi: 10.21685/2307-4205-2023-3-2

ENSURING RELIABILITY IN THE LIFE CYCLE OF RESPONSIBLE ARTIFICIAL INTELLIGENCE SYSTEMS

M.Yu. Mikheev[1], O.V. Prokofiev[2], A.E. Savochkin[3], I.Yu. Semochkina[4]

[1, 2, 3, 4] Penza State Technological University, Penza, Russia
[1] mix1959@gmail.com, [2] prokof_ow@mail.ru, [3] aebrat@mail.ru, [4] ius1961@gmail.com

Abstract. *Background.* Over the past few years, there has been a dramatic expansion in the capabilities of artificial intelligence (AI) systems, which has simultaneously led to new risks and potential benefits. The autonomy of systems, which allows moving from decision support to self-development of a decision, provides conflicting results in areas of responsible application. Such sensitive areas of application as human health, its ecological living environment, economic and social status. In the field of armaments, the means of creating autonomous systems of a new generation and the concept of a future «hyperwar» associated with them are discussed. *Materials and methods.* Due to the growing use of AI around the world in these sensitive areas, there is a demand for reliability when using such autonomous systems. It is necessary to formulate the risks and benefits of this technology, including compliance with fundamental ethical principles. The application of critical decisions must be controlled by the person in charge. Measures to ensure the reliability of an autonomous system with AI must be provided at all stages of the life cycle, and only in this way it is possible to control risks and create explainable and manageable AI. *Results and conclusions.* The authors outlined the concept of the concept of «reliable» AI and described the implementation of its individual provisions at the stages of the life cycle of an autonomous system for responsible purposes.

Keywords: reliability of the artificial intelligence system, responsible assignment system, decision-making by an autonomous system

Financing: the study was supported by the Russian Science Foundation grant No. 23-21-10046, https://rscf.ru/project/23-21-10046/

For citation: Mikheev M.Yu., Prokofiev O.V., Savochkin A.E., Semochkina I.Yu. Ensuring reliability in the life cycle of responsible artificial intelligence systems. *Nadezhnost' i kachestvo slozhnykh sistem = Reliability and quality of complex systems.* 2023;(3):12–20. (In Russ.). doi: 10.21685/2307-4205-2023-3-2

Введение

Важность искусственного интеллекта (ИИ) резко возросла за последние годы. В это же время этический аспект ИИ недостаточно исследован в сферах ответственного применения, в частности, в военной сфере [1]. Противоречивые аспекты использования методов ИИ в качестве компонента систем вооружения – это сложная область исследований, связанная с созданием непредсказуемых рисков. Тем не менее имеется потенциальная возможность повысить точность и масштабируемость воздействия оружия, что ведет к потенциальной минимизации ненужного ущерба или жертв, спасению человеческих жизней и ресурсов. Поэтому следует определить наиболее насущные аспекты для исследований и разработок, необходимых в этой области, чтобы гарантировать ответственное, безопасное и контролируемое использование этой технологии, а также прозрачность поведения этих систем. Реализация этих аспектов имеет основополагающее значение для приемлемости систем вооружения на базе ИИ. Кроме того, системы искусственного интеллекта любой степени сложности могут быть жизненно важной частью глобальной системы, включающей множество различных сенсорных и активных технических подсистем, а также людей. Кроме того, диапазон применения простирается от тактического уровня решений в конкретной ситуации до стратегического уровня, направленного на ситуационную осведомленность и комплексную поддержку принятия решений. Особый вопрос – аспект квалификации (оценки) и тестирования систем ИИ. Текущее состояние техники не дает определения процедур тестирования, специфичных для ИИ, не вызывает доверия и не гарантирует предсказуемость [1]. Это приводит к противоречиям между разработчиками и производителями вооруженных систем искусственного интеллекта с одной стороны, операторов (военных) с другой стороны и исследовательским сообществом посередине. Это поднимает вопрос о надежности как соответствии и предсказуемости систем ИИ, которые можно гарантировать при любых обстоятельствах. Определение концепции надежного ИИ также связано с необходимым и достаточным уровнем самостоятельности действий системы ИИ. Чем больше статические правила и ограниченная свобода системы ИИ, тем больше предсказуемость и последовательность результатов. С другой стороны, большая свобода для системы ИИ может повысить ее универсальность и полезность, а также увеличивает объем ответственности разработчика и оператора. Здесь ни оптимальный компромисс, ни лучшая практика не ясны и не требуют дальнейших исследований.

Целью данного исследования является формирование понятия надежности применительно к автономным системам ответственного назначения, управляемым искусственным интеллектом, а также методы и средства обеспечения надежности во время выполнения этапов жизненного цикла систем.

Материалы и этапы исследования

В результате обзора [1–12] авторами выявлено, что наибольшее внимание исследователей привлечено к автономным вооружениям, которые далее использованы в качестве характерного примера разрабатываемых систем ответственного назначения.

Ниже представлена выявленная «эталонная» структура жизненного цикла. Он состоит из четырех фаз (этапов): разработка, управление, подготовка миссии и применение. Эти четыре этапа предназначены для охвата всего процесса: от разработки военных систем искусственного интеллекта до их использования и обеспечения отслеживаемости. Процессу присущи этапы регулирования, адаптации и обратной связи. Первая фаза – это этап разработки. Для обеспечения надежности должны использоваться адекватные процессы, методы и приемы, аналогичные известным из техники безопасности. Для обеспечения ключевых свойств систем военного назначения с компонентами ИИ ключевые требования (в частности, связанные с надежностью) разрабатываемой системы должны быть проанализированы, корректно сформулированы и представлены в форме системной архитектуры. Вторая фаза – квалификационная оценка, которая в контексте ответственного применения должна

проводиться независимой экспертизой с персоналом, обученным в том числе в области права и этики, и сосредоточена конкретно на критических точках в приложениях ИИ (фаза управления). Поскольку каждая военная миссия имеет уникальные требования к системе ИИ, на третьем этапе рассматривается адаптация к конкретной миссии. Начиная с определения цели миссии на языке системы и в соответствии с правилами взаимодействия с системой, этот этап может быть описан как «установка параметров». Приложения ИИ были полностью обучены и проверены на предыдущих этапах, поэтому этот этап адаптации относится к настройкам параметров для конкретных целей миссии, доступных ресурсов и условий окружающей среды. Эта адаптация должна быть сделана специалистами, работающими на стадии применения (военными операторами). Последний, четвертый этап – развертывание и использование полученной системы ИИ. Здесь основными заинтересованными сторонами являются две военные роли: оператор системы вооружений ИИ и контролирующий орган, занимающийся планированием и анализом операций. Компоненты ИИ системы действуют как помощь оператору оружия с возможностью явного объяснения, почему система сделала тот или иной вывод или нет.

Результаты

Архитектура четырех фаз описана более подробно ниже.

Фаза разработки. На рис. 1 показаны компоненты системы вооружения на основе ИИ на этапе разработки. Основным элементом является система хранения ИИ. Он содержит основу «морального поведения» и отвечает за объяснимость системы вооружения ИИ. С одной стороны, этот модуль определяет общий язык для всех участников, чтобы указать недвусмысленные правила взаимодействия, а также возможности системы в машиночитаемой и интерпретируемой человеком форме. Язык всегда состоит из грамматики и словаря. Поскольку системы ИИ будут широко использовать алгоритмы машинного обучения, используемые обучающие данные должны храниться централизованно в дополнение к моделям для классических подходов ИИ. Алгоритмы ИИ системы описаны в модуле приложения ИИ. В архитектуре определены четыре группы компонентов ИИ и механизм этических правил. Сенсорные приложения на основе ИИ для обнаружения, классификации, анализа интересующего объекта и вывода о поведении позволяют обнаруживать внешние критически важные обстоятельства. Управление ресурсами на основе ИИ позволяет оптимизировать использование ресурсов системы вооружения. Модули выводов и рассуждений обеспечат улучшенное понимание ситуации. Анализ целей и последствий должен соответствовать правилам боя с возможностями оружия. Эти четыре возможности полагаются на механизм этических правил, чтобы проверять свое поведение на соответствие к набору этических правил. Это гарантирует, что этические принципы используются для внедрения и выполнения компонентов ИИ в системе ИИ.

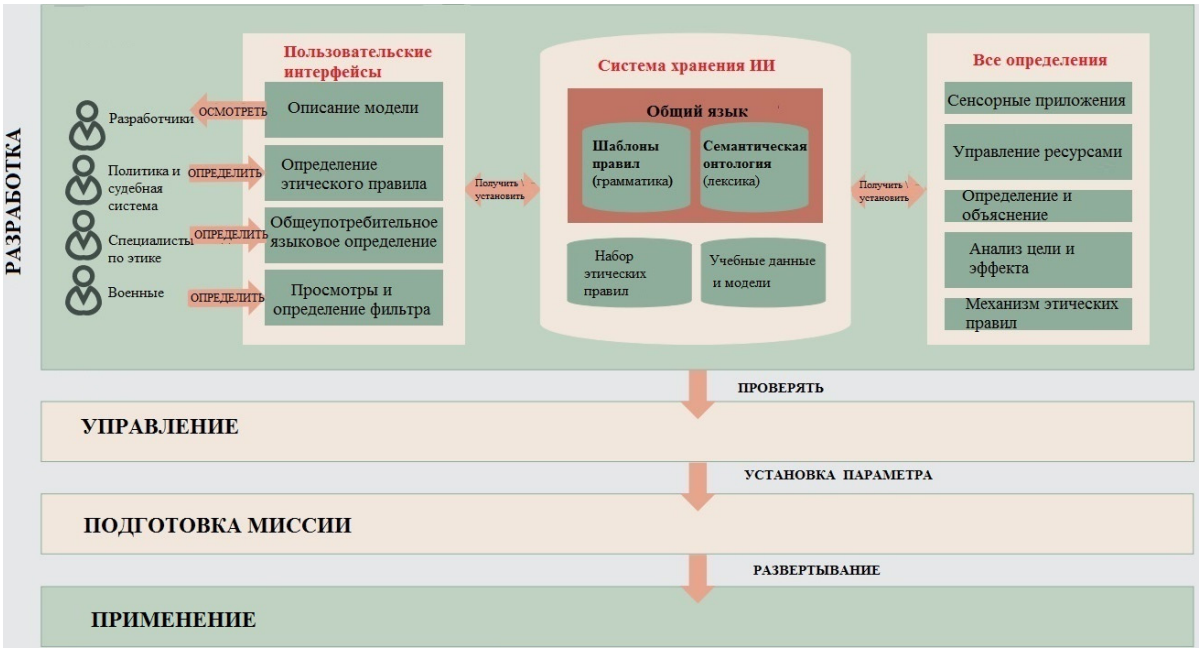

Рис. 1. Фаза разработки системы ответственного назначения на основе ИИ

Чтобы определить и изучить содержимое системы хранения ИИ, необходимы пользовательские интерфейсы. Для каждой группы участников должны быть доступны разные представления для ввода и изучения этических правил, определения общего языка и получения объяснений системных предложений с использованием технологии XAI (интерпретируемого ИИ). Адекватные процессы, методы и технологии для обеспечения надежности должны быть установлены на этапе разработки, что обеспечивает инженерная структура надежности. Такая структура может соответствовать инженерным подходам и руководящим принципам для систем с высокой степенью интеграции (например, техниками безопасности и стандартами безопасности) и должна охватывать всю фазу разработки. Конечным пунктом деятельности по разработке доверия является случай обеспечения доверия, всесторонняя аргументация надежности всей системы. Аргументация включает в себя все соответствующие требования надежности, а также достаточные доказательства, подтверждающие, что система отвечает всем этим требованиям.

Фаза управления. Следующим шагом после разработки является этап управления (рис. 2), на котором определяют элементы системы вооружения на основе ИИ, подлежащие квалификационной оценке.

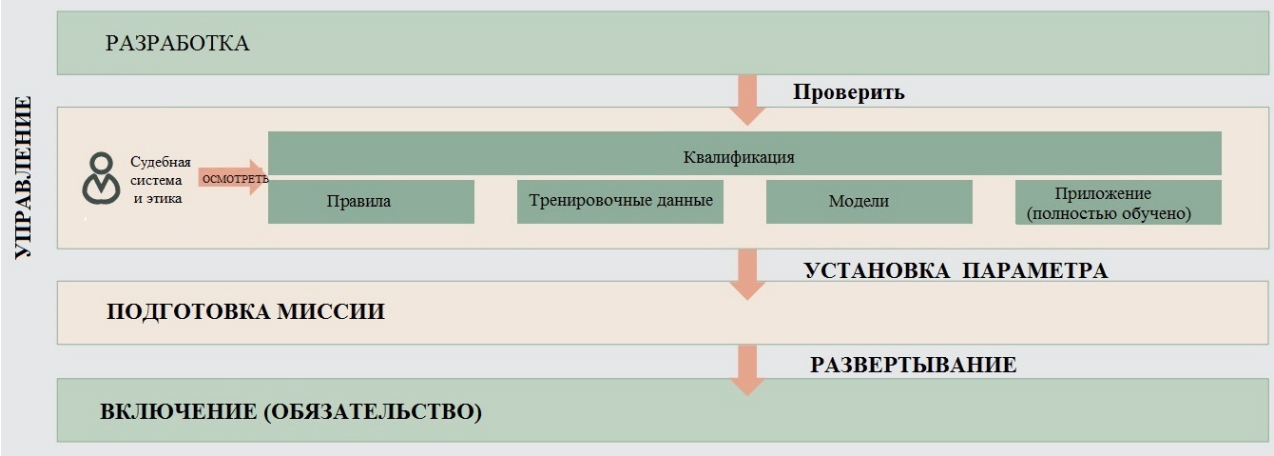

Рис. 2. Фаза управления системой на основе ИИ

Рассматриваемая система вооружения на основе ИИ на этом этапе полностью разработана, а это означает, что все части машинного обучения полностью обучены, а модели и правила стабилизированы. Результирующие алгоритмы являются статическими, но могут содержать параметры для конкретных настроек; это будет подробно описано в третьей фазе. Этот этап служит для проверки соблюдения правил применения и этических норм. Ключевым элементом этой проверки является случай обеспечения доверия, который обеспечивает общую аргументацию надежности, подкрепленную доказательствами и взаимосвязанную со всеми соответствующими артефактами разработки. Доказательства будут включать результаты тестов, но также будут и независимые тесты, проводимые квалификационными органами. Модули, подлежащие независимому тестированию, – это содержимое систем хранения ИИ (правила, тестовые и обучающие данные) и приложения ИИ с обработчиком правил.

Фаза подготовки миссии. Каждая военная миссия предъявляет уникальные требования к операциям, например, к миротворческой, гуманитарной или боевой миссии. На этапе подготовки миссии (рис. 3) цель миссии должна быть указана с использованием общего языка.

Настройка параметров для алгоритмов (например, условия окружающей среды) и корректировка системы правил (например, правила взаимодействия для конкретных задач, различные приоритеты) подготовят систему к участию в миссии. Генератор правил миссии устанавливает параметры для системы ИИ в соответствии с целью миссии. Это необходимо проверить, чтобы устранить ошибки и несоответствия между целью миссии, правилами и доступными ресурсами, которые можно использовать для достижения цели миссии. Общий шаблон параметризации должен быть адекватно отражен в случае гарантии доверия, чтобы гарантировать надежность в любом возможном контексте миссии.

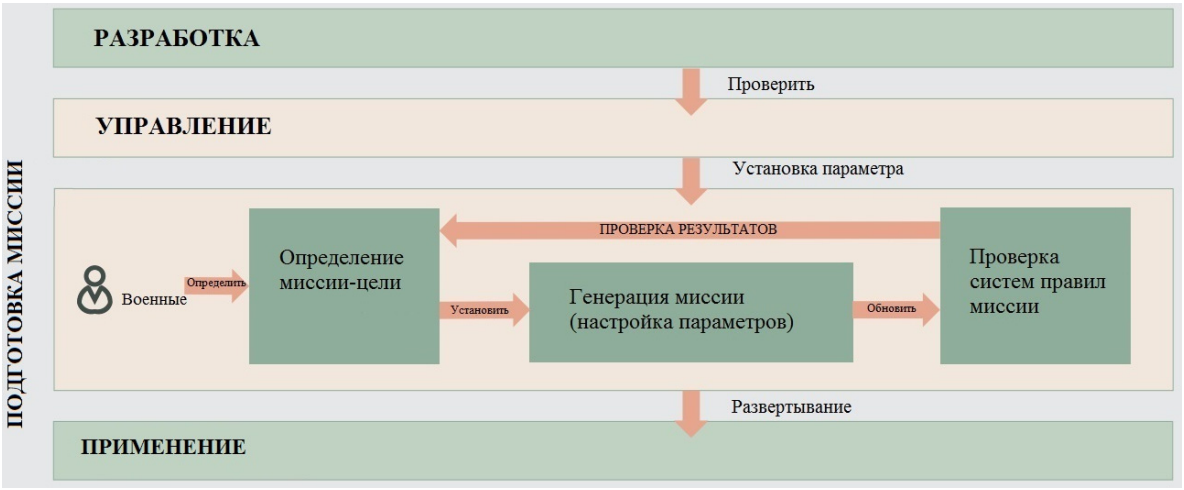

Рис. 3. Фаза подготовки миссии

Фаза применения. Этот этап (рис. 4) охватывает использование системы ИИ в конкретной миссии. Адаптация для миссии (настройка параметров) и, таким образом, цель миссии и механизм правил инкапсулированы в набор данных правил для конкретной миссии. Основываясь на этом, пользователю помогают четыре модуля. Сенсорные приложения освобождают пользователя от обработки необработанных данных. Качество обнаружения, классификации и отслеживания результатов будет повышено за счет использования алгоритмов анализа данных, объединения выводов и рассуждений на основе ИИ. Интеллектуальное управление ресурсами поддерживает пользователя, оптимизируя потенциальные ресурсы оружия. Самым амбициозным подходом является помощь в анализе целей и результатов.

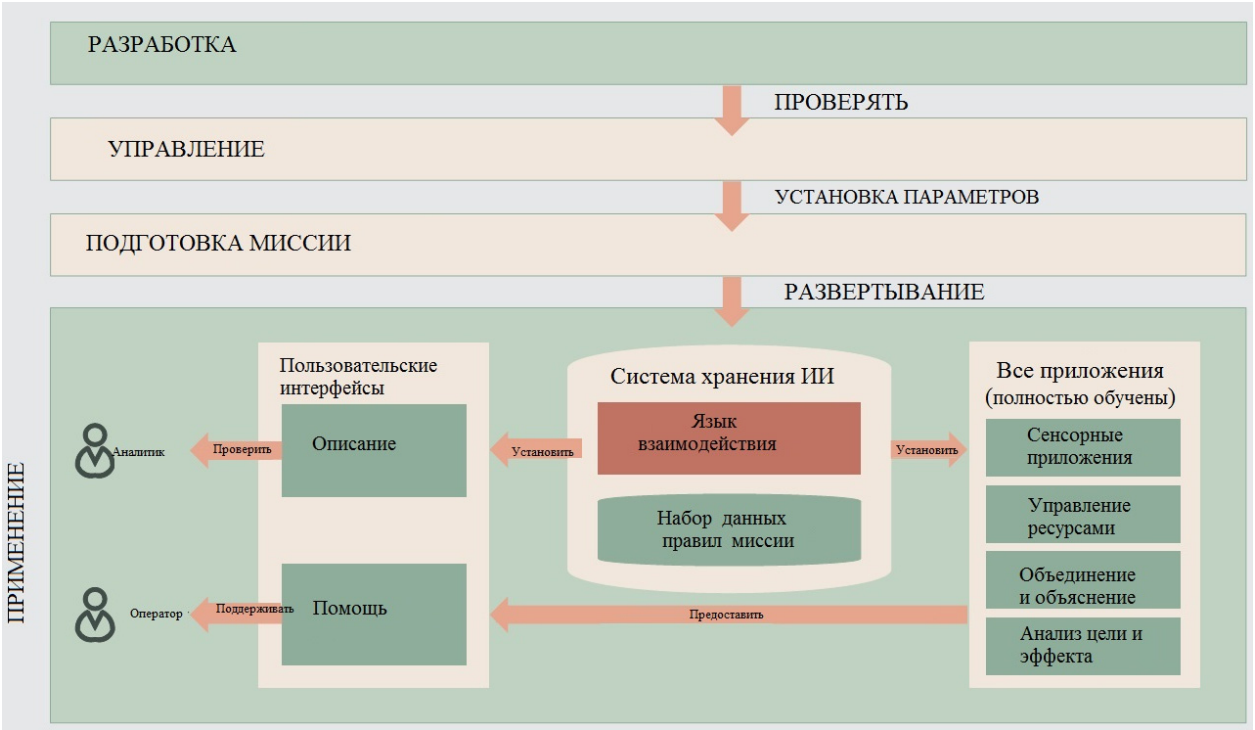

Рис. 4. Фаза применения

Помимо пользовательского интерфейса для оператора, который просто включает или отключает функции, должен быть специальный пользовательский интерфейс, поддерживающий проверку предложения ИИ, спрашивая, почему система сделала предложение применить оружие со специальной параметризацией или нет. Объяснения ИИ являются ключом к этому. С другой стороны, пользователь должен быть определенным образом обучен взаимодействию с системой. Скорее всего

(в зависимости от фактического применения) будут соответствующие предположения в случае обеспечения надежности, и тогда ключевым моментом является то, что предположения всегда остаются в силе.

Обсуждение

Динамичные сценарии, возникающие в областях ответственного прнименения, в том числе в военной, включают в себя сочетание классических элементов деятельности с атаками в кибер- и информационной сфере, а также с развертыванием большого количества автоматически и автономно управляемых беспилотных систем. Из-за значительно возросшей динамики этого боя также используется термин «реакция на скорости машины». Целью военных является достижение военного превосходства и способности планировать и проводить операции точнее и быстрее, чем противник. Однако в определенный момент времени люди больше не могут самостоятельно контролировать эту динамичную обстановку во всех ее деталях. Техническая поддержка в мониторинге и оценке ситуации, планировании действий и, наконец, выполнении операции станет необходимостью. Здесь в игру вступают методы искусственного интеллекта. Использование искусственного интеллекта предлагает возможность обеспечить оперативное превосходство, начиная с мониторинга и оценки ситуации. В связи с оцифровкой области деятельности будет доступно все больше информации для оценки ситуации. Методы распознавания образов могут привести к тому, что эти процессы будут выполняться намного быстрее и точнее. В сочетании с методами целеуказания, захвата цели и управления огнем цикл «датчик–стрелок» может быть значительно ускорен. Повышение точности воздействия может привести к уменьшению побочного ущерба и послужить защите гражданское население. С помощью искусственного интеллекта будущие сражения можно проводить намного быстрее, точнее и с меньшими затратами [13]. Кроме того, такие технологии, как рои дронов, предлагают военный потенциал, который сегодня не существует в такой форме. Большой рой дронов – отличный пример, показывающий, что в какой-то момент с угрозой нельзя бороться, если в цепочке находится человек, который индивидуально выбирает цели для борьбы с ними. Эмерджентное поведение самоорганизующихся систем ИИ должно быть тщательно изучено, аналогично поведению естественного роя. Однако использование технологий из области искусственного интеллекта также сопряжено с рисками и проблемами. Во-первых, существуют риски, которые существуют и при использовании ИИ в менее ответственных областях, такие как вопросы честности и беспристрастности, необъяснимости или уязвимости перед манипуляциями и неправомерным использованием. Кроме того, особая проблема возникает в военной среде, когда технология ИИ используется в системах вооружения. Международное гуманитарное право определяет три важных принципа, которые необходимо учитывать при использовании оружия в конфликтах, кроме аспектов надежности и предосторожности. Это различие между гражданским населением и военными, соразмерность средств противостояния и оценка военной необходимости применения оружия. Это приводит к представлению о том, что люди должны иметь возможность осуществлять «эффективный контроль» при использовании оружия. Эффективный контроль здесь означает, что человек должен быть в состоянии понять и оценить всю ситуацию. Возникает вопрос, как обеспечить реальное осуществление эффективного контроля, какая информация должна быть доступна и как она должна быть представлена? Над всем этим стоит базовая потребность в доверии и, следовательно, концепция того, как установить надежность на всех уровнях этой очень сложной области применения.

Заключение

Концепция надежного ИИ в системах ответственного применения должна учитывать различные фазы (этапы) жизненного цикла системы вооружений с ИИ. Все этапы должны содержать меры для обеспечения надежности и ответственного использования ИИ. Ключевыми факторами использования ИИ являются общий язык, поставленная цель, анализ задач и последствий, а также гарантия надежности. В частности, модули на этапе управления (см. рис. 2) должны быть квалифицированы так же, как и система в целом. Правила должны быть проверены на правильность, обучающие данные на честный и реалистичный баланс, модели на правильность и уместность. Механизм правил должен быть протестирован на предмет обработки приоритетов и несоответствий.

Надежность – важное свойство для любой системы, а для тех, которые связаны со значительными рисками и тесно взаимодействуют с людьми-операторами, это особенно актуально. Однако из-за

неотъемлемых характеристик компонентов ИИ, особенно когда речь идет о машинном обучении, сложно обеспечить достоверность, особенно полную понятность. Более того, надежность касается не только технических свойств отдельных компонентов ИИ, но и свойств всей системы в ее общем контексте.

Надежные системы ответственного назначения с ИИ:

– должны быть законными, соответствовать всем применимым законам и правилам;

– должны быть этичными, обеспечивая соблюдение этических принципов и ценностей;

– должны быть надежными как с технической, так и с социальной точек зрения, поскольку даже при наличии добрых намерений системы ИИ могут нанести непреднамеренный вред.

Надежность, включающая в себя такие аспекты, как безопасность и защищенность, является более техническим аспектом, который в настоящее время также характеризуется многими проблемами. Изложенное должно послужить стимулом для разработчиков систем ответственного назначения, занимающихся вопросами обеспечения качества принимаемых решений [14, 15].

Список литературы

1. Rise of artificial intelligence in military weapons systems / ed. by J. Beyerer, P. Martini. Fraunhofer Group for Defense and Security VVS, 2020. URL: www.vvs.fraunhofer.de
2. Boulanin V., Saalman L., Topychkanov P. et al. Artificial Intelligence, Strategic Stability and Nuclear Risk. 2020. URL: https://www.sipri.org/sites/default/files/2020-06/artificial_intelligence_strategic_stability_and_nuclear_risk.pdf
3. Integrating Cybersecurity and Critical Infrastructure. National, Regional and International Approaches / ed. by L. Saalman. 2018. URL: https://www.sipri.org/sites/default/files/2018-04/integrating_cybersecurity_0.pdf
4. The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk. Vol. I. Euro-Atlantic Perspectives / ed. by V. Boulanin. 2020. URL: https://www.sipri.org/publications/2020/other-publications/artificial-intelligence-strategic-stability-and-nuclear-risk
5. Boulanin V., Verbruggen M. Mapping the Development of Autonomy in Weapon Systems. 2020. URL: https://www.sipri.org/sites/default/files/2018-04/integrating_cybersecurity_0.pdf
6. Boulanin V., Bruun L., Goussac N. Autonomous Weapon Systems And International Humanitarian Law. Identifying Limits and the Required Type and Degree of Human–Machine Interaction. 2021. URL: https://www.sipri.org/sites/default/files/2021-06/2106_aws_and_ihl_0.pdf
7. Saalman L., Su F., Saveleva Dovgal L. Cyber Posture Trends in China, Russia, the United States and the European Union. 2022. URL: https://www.sipri.org/sites/default/files/2022-12/2212_cyber_postures_0.pdf
8. Boulanin V. Mapping the development of autonomy in weapon systems. A primer on autonomy. 2017. URL: https://www.sipri.org/sites/default/files/Mapping-development-autonomy-in-weapon-systems.pdf
9. Boulanin V., Goussac N., Bruun L., Richards L. Responsible Military Use of Artificial Intelligence. Can the European Union Lead the Way in Developing Best Practice? 2020. URL: https://www.sipri.org/publications/2020/other-publications/responsible-military-use-artificial-intelligence-can-european-union-lead-way-developing-best
10. Boulanin V., Brockmann K., Richards L. Responsible Artificial Intelligence Research and Innovation for International Peace and Security. 2020. URL: https://www.sipri.org/sites/default/files/2020-11/sipri_report_responsible_artificial_intelligence_research_and_innovation_for_international_peace_and_security_2011.pdf
11. Bromley M., Maletta G. The Challenge of Software and Technology Transfers to Non-Proliferation Efforts // Implementing and Complying with Export Controls. 2018. URL: https://www.sipri.org/publications/2018/other-publications/challenge-software-and-technology-transfers-non-proliferation-efforts-implementing-and-complying
12. Turell J., Su F., Boulanin V. Cyber-incident Management Identifying and Dealing with the Risk of Escalation // IPRI Policy. 2020. № 55. URL: https://www.sipri.org/publications/2020/sipri-policy-papers/cyber-incident-management-identifying-and-dealing-risk-escalation
13. Бабкин А. В., Подольский А. Г., Прокофьев О. В., Савочкин А. Е. Роль информационно-аналитической системы мониторинга цен в влиянии на научную и научно-техническую продукцию военного назначения в обеспечении экономической безопасности государства // Надежность и качество сложных систем. 2022. № 4. С. 110–119.
14. Михеев М. Ю., Прокофьев О. В., Семочкина И. Ю. Методологии построения систем поддержки принятия решений в многоаспектной области применения // Труды Международного симпозиума Надежность и качество. 2022. Т. 1. С. 18–22.
15. Иванов А. И., Кубасов И. А. Сильный искусственный интеллект: повышение качества нейросетевых решений с переходом к обработке входных данных большого объема // Надежность и качество сложных систем. 2021. № 1. С. 9–16. doi: 10.21685/2307-4205-2021-1-1

References

1. Beyerer J., Martini P. (ed.). *Rise of artificial intelligence in military weapons systems*. Fraunhofer Group for Defense and Security VVS, 2020. Available at: www.vvs.fraunhofer.de

2. Boulanin V., Saalman L., Topychkanov P. et al. *Artificial Intelligence, Strategic Stability and Nuclear Risk*. 2020. Available at: https://www.sipri.org/sites/default/files/2020-06/artificial_intelligence_strategic_stability_and_nuclear_risk.pdf
3. Saalman L. (ed.). *Integrating Cybersecurity and Critical Infrastructure. National, Regional and International Approaches*. 2018. Available at: https://www.sipri.org/sites/default/files/2018-04/integrating_cybersecurity_0.pdf
4. Boulanin V. (ed.). *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk. Vol. I. Euro-Atlantic Perspectives*. 2020. Available at: https://www.sipri.org/publications/2020/other-publications/artificial-intelligence-strategic-stability-and-nuclear-risk
5. Boulanin V., Verbruggen M. *Mapping the Development of Autonomy in Weapon Systems*. 2020. Available at: https://www.sipri.org/sites/default/files/2018-04/integrating_cybersecurity_0.pdf
6. Boulanin V., Bruun L., Goussac N. *Autonomous Weapon Systems And International Humanitarian Law. Identifying Limits and the Required Type and Degree of Human–Machine Interaction*. 2021. Available at: https://www.sipri.org/sites/default/files/2021-06/2106_aws_and_ihl_0.pdf
7. Saalman L., Su F., Saveleva Dovgal L. *Cyber Posture Trends in China, Russia, the United States and the European Union*. 2022. Available at: https://www.sipri.org/sites/default/files/2022-12/2212_cyber_postures_0.pdf
8. Boulanin V. *Mapping the development of autonomy in weapon systems. A primer on autonomy*. 2017. Available at: https://www.sipri.org/sites/default/files/Mapping-development-autonomy-in-weapon-systems.pdf
9. Boulanin V., Goussac N., Bruun L., Richards L. *Responsible Military Use of Artificial Intelligence. Can the European Union Lead the Way in Developing Best Practice?* 2020. Available at: https://www.sipri.org/publications/2020/other-publications/responsible-military-use-artificial-intelligence-can-european-union-lead-way-developing-best
10. Boulanin V., Brockmann K., Richards L. *Responsible Artificial Intelligence Research and Innovation for International Peace and Security*. 2020. Available at: https://www.sipri.org/sites/default/files/2020-11/sipri_report_responsible_artificial_intelligence_research_and_innovation_for_international_peace_and_security_2011.pdf
11. Bromley M., Maletta G. The Challenge of Software and Technology Transfers to Non-Proliferation Efforts. *Implementing and Complying with Export Controls*. 2018. Available at: https://www.sipri.org/publications/2018/other-publications/challenge-software-and-technology-transfers-non-proliferation-efforts-implementing-and-complying
12. Turell J., Su F., Boulanin V. Cyber-incident Management Identifying and Dealing with the Risk of Escalation. *IPRI Policy*. 2020:(55). Available at: https://www.sipri.org/publications/2020/sipri-policy-papers/cyber-incident-management-identifying-and-dealing-risk-escalation
13. Babkin A.V., Podol'skiy A.G., Prokof'ev O.V., Savochkin A.E. The role of the information and analytical price monitoring system in influencing scientific and scientific-technical military products in ensuring the economic security of the state. *Nadezhnost' i kachestvo slozhnykh system = Reliability and quality of complex systems.* 2022;(4):110–119. (In Russ.)
14. Mikheev M.Yu., Prokof'ev O.V., Semochkina I.Yu. Methodologies for building decision support systems in a multidimensional field of application. *Trudy Mezhdunarodnogo simpoziuma Nadezhnost' i kachestvo = Proceedings of the International Symposium Reliability and Quality*. 2022;1:18–22. (In Russ.)
15. Ivanov A.I., Kubasov I.A. Strong artificial intelligence: improving the quality of neural network solutions with the transition to processing large-volume input data. *Nadezhnost' i kachestvo slozhnykh system = Reliability and quality of complex systems.* 2021;(1):9–16. (In Russ.). doi: 10.21685/2307-4205-2021-1-1

Информация об авторах / Information about the authors

Михаил Юрьевич Михеев
доктор технических наук, профессор, заведующий кафедрой информационных технологий и систем,
Пензенский государственный технологический университет
(Россия, г. Пенза, проезд Байдукова/ ул. Гагарина, 1а/11)
E-mail: mix1959@gmail.com

Олег Владимирович Прокофьев
кандидат технических наук, доцент, доцент кафедры информационных технологий и систем,
Пензенский государственный технологический университет
(Россия, г. Пенза, проезд Байдукова/ ул. Гагарина, 1а/11)
E-mail: prokof_ow@mail.ru

Mikhail Yu. Mikheev
Doctor of technical sciences, professor,
head of the sub-department of information technology and systems,
Penza State Technological University
(1a / 11 Baidukova passage/ Gagarina street, Penza, Russia)

Oleg V. Prokofiev
Candidate of technical sciences, associate professor,
associate professor of the sub-department of information technology and systems,
Penza State Technological University
(1a / 11 Baidukova passage/ Gagarina street, Penza, Russia)

Александр Евгеньевич Савочкин
кандидат технических наук,
доцент кафедры прикладной информатики,
Пензенский государственный
технологический университет
(Россия, г. Пенза, проезд Байдукова/
ул. Гагарина, 1а/11)
E-mail: aebrat@mail.ru

Ирина Юриевна Семочкина
кандидат технических наук, доцент, доцент кафедры
информационных технологий и систем,
Пензенский государственный
технологический университет
(Россия, г. Пенза, проезд Байдукова/
ул. Гагарина, 1а/11)
E-mail: ius1961@gmail.com

Aleksandr E. Savochkin
Candidate of technical sciences, associate professor
of the sub-department of applied informatics,
Penza State Technological University
(1a / 11 Baidukova passage/ Gagarina street,
Penza, Russia)

Irina Yu. Semochkina
Candidate of technical sciences, associate professor,
associate professor of the sub-department
of information technology and systems,
Penza State Technological University
(1a / 11 Baidukova passage/ Gagarina street,
Penza, Russia)

**Авторы заявляют об отсутствии конфликта интересов /
The authors declare no conflicts of interests.**

Поступила в редакцию/Received 15.06.2023
Поступила после рецензирования/Revised 17.07.2023
Принята к публикации/Accepted 14.08.2023