ПРОБЛЕМА УСТОЙЧИВОСТИ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ В УСЛОВИЯХ ВЫСОКОГО УРОВНЯ АВТОМАТИЗАЦИИ

Э. М. Исмайлов[1,а], **Т. В. Гавриленко**[1,2,б]

[1] *Сургутский филиал федерального государственного автономного учреждения «Федеральный научный центр Научно-исследовательский институт системных исследований Национального исследовательского центра «Курчатовский институт», г. Сургут, Российская Федерация*

[2] *Сургутский государственный университет, г. Сургут, Российская Федерация*

[а] *ORCID: https://orcid.org/0009-0003-9913-3283, trol.8@inbox.ru*

[б] *ORCID: https://orcid.org/0000-0002-3243-2751, taras.gavrilenko@gmail.com*

Аннотация: вследствие быстрого скачкообразного развития научно-технического прогресса и меняющейся геополитики возникает острая необходимость изучения и активного внедрения новых методов управления и защиты энергетической инфраструктуры, так как используемые технические решения в данной области не всегда могут обеспечить необходимый уровень надежности и безопасности. Применяемые для этого системы и программы в разных секторах экономики, являющиеся сегодня передовыми, могут мгновенно потерять актуальность из-за появления методов их взлома и невозможности их своевременного усовершенствования. В статье рассматриваются технологии на основе искусственного интеллекта, внедрение которых может обеспечить комплексный подход к вопросам управления и защиты энергетического сектора страны. Представлен анализ технологий на базе искусственного интеллекта, внедрение которых может обеспечить защиту от внешних воздействий на критическую инфраструктуру страны.

Ключевые слова: критическая информационная инфраструктура, энергетика, контроль, искусственный интеллект.

Для цитирования: Исмайлов Э. М., Гавриленко Т. В. Проблема устойчивости критической инфраструктуры в условиях высокого уровня автоматизации. *Успехи кибернетики*. 2025;6(2):75–79.

Поступила в редакцию: 16.02.2025. *В окончательном варианте: 17.05.2025*.

SUSTAINABILITY OF HIGHLY AUTOMATED CRITICAL INFRASTRUCTURE

E. M. Ismailov[1,a], **T. V. Gavrilenko**[1,2,b]

[1] *Surgut Branch of Scientific Research Institute for System Analysis of the National Research Centre "Kurchatov Institute", Surgut, Russian Federation*

[2] *Surgut State University, Surgut, Russian Federation*

[a] *ORCID: https://orcid.org/0009-0003-9913-3283, trol.8@inbox.ru*

[b] *ORCID: https://orcid.org/0000-0002-3243-2751, taras.gavrilenko@gmail.com*

Abstract: we examined the need for new approaches to managing and protecting energy infrastructure in the context of rapid scientific and technological advancement and evolving geopolitical conditions. The technical solutions currently employed in this sector fail to ensure the required level of reliability and security. New systems and programs introduced across various economic sectors quickly become obsolete due to the continuous emergence of novel methods for bypassing protective mechanisms and the inherent difficulty in promptly detecting such threats.

Keywords: critical IT infrastructure, power industry, monitoring, artificial intellegence.

Cite this article: Ismailov E. M., Gavrilenko T. V. Sustainability of Highly Automated Critical Infrastructure. *Russian Journal of Cybernetics*. 2025;6(2):75–79.

Original article submitted: 16.02.2025. *Revision submitted: 17.05.2025*.

Введение

С 2014 года на Российскую Федерацию активно накладываются разного рода санкции, которые в том числе ограничивают доступ к технологиям, кроме этого, в последнее время стремительно растет количество кибератак из-за рубежа, а также атак телефонных мошенников с применением профессиональных психологических подходов, которые могут нанести серьезный ущерб не только личной безопасности граждан, но и предприятиям критической инфраструктуры, сотрудники которых также подвергаются указанному воздействию. Однако при должном внимании к этим проблемам усилия,

направленные на их решение, могут не только обезопасить важные для страны объекты, но и дать мощный толчок развитию собственной научной и технической базы.

Ввиду сложившихся обстоятельств многие зарубежные предприятия, которые обеспечивали техническое оснащение и программное обеспечение для защиты объектов критической инфраструктуры, заявили о закрытии своих дочерних компаний и прекращении любого сотрудничества с Россией. Как следствие, информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, работающие практически во всех секторах экономики (энергетика, оборонная промышленность, банковская сфера, транспорт, связь и т. д.), остались без программной и технической поддержки со стороны зарубежных производителей, чье оборудование и программное обеспечение используется в том числе и на объектах критической информационной инфраструктуры страны (КИИ), а это значит, что все отрасли КИИ стали более уязвимы перед несанкционированным вмешательством в работу их систем.

В итоге промышленный шпионаж приобретает более циничный характер, направленный не только на кражу финансовой и интеллектуальной собственности, но и на разные виды диверсий с целью нанесения максимально возможного ущерба механизмам и технологическим процессам.

Указанные обстоятельства влекут за собой технические, политические, военные, юридические, коммерческие, производственные и иные виды рисков, реализация которых может привести к тяжелейшим последствиям для жизни и здоровья граждан и экономики страны [1, 2].

Общеизвестным примером внешнего вмешательства в объекты КИИ и последствий таких воздействий являются события в Венесуэле и Иране.

Венесуэла

В 2019 году Венесуэла подверглась кибератаке, в ходе которой вышла из строя самая большая в стране гидроэлектростанция.

По словам министра информации страны Хорхе Родригеса, «кибератака стала причиной самого масштабного в истории Венесуэлы отключения электроэнергии». Атака была направлена на автоматическую систему контроля ГЭС «Гури», которая контролировала процесс выработки электроэнергии. В ходе данной кибератаки пропало электроснабжение таких важных секторов КИИ, как больницы, банки и т.д. [3].

Иран

В 2010 году в Иране в ходе кибератаки с применением компьютерного червя Stux.net, причинен вред объектам ядерной промышленности – заводам по обогащению урана и АЭС, что нанесло огромный урон ядерной программе Ирана [4], развитие которой было отброшено на многие годы назад.

Основной задачей вредоносного червя было испортить все обратные связи между системами управления на базе программно-логического комплекса и системами мониторинга текущего состоянии установок по обогащению урана.

При этом необходимо отметить, что в приведенных выше примерах были атакованы системы управления на базе программно-логического комплекса от ведущих производителей и их системы защиты продемонстрировали свою неэффективность перед внешним вмешательством.

Очевидно, что существует острая необходимость защитить объекты КИИ, это важно для обеспечения безопасности государства и стабильности ключевых сфер жизнедеятельности.

Состояние проблемы

Перспективным направлением для решения данной задачи представляется применение технологии искусственного интеллекта (ИИ) и ее активное внедрение в сектор КИИ.

Федеральный закон Российской Федерации от 24.04.2020 № 123-ФЗ дает определение искусственному интеллекту: комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получить при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру (в том числе информационные системы, информационно-телекоммуникационные сети, иные технологические средства обработки информации), программное обеспечение (в том числе то, в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений [5].

В рамках управления системами безопасности на сегодняшний день технологии ИИ применяются, например, в системах видеонаблюдения и контроля безопасности путем сбора данных с камер видеонаблюдения, охранных систем и их передачи в адрес оператора [5].

Перспективной сферой применения ИИ являются предприятия среднего и малого бизнеса. Облачные системы ML Space от Sber Cloud, Azure от Microsoft и Auto ML от Google предоставляют все необходимые инструменты для создания собственных алгоритмов с целью автоматического ответа на запрос или прогнозирования спроса [6]. Такие компании могут стать активными участниками создания и внедрения искусственного интеллекта в секторе КИИ.

Сегодня для управления любым сектором экономики используют комплекс аппаратных и программных средств. При разделении любого крупного процесса управления на подпроцессы мы увидим, что существует точечное управление (локальное по месту) и обширное (общее управление из операторной). Процессы такого масштаба необходимо рассматривать как динамические системы с изменяющимися во времени параметрами. На рисунке 1 (модель черного ящика) представлена упрощенная система управляемого объекта (S), например насоса по перекачке нефтепродукта, с входящими (U (t), V(t)) и выходящим (Y(t)) векторными параметрами.

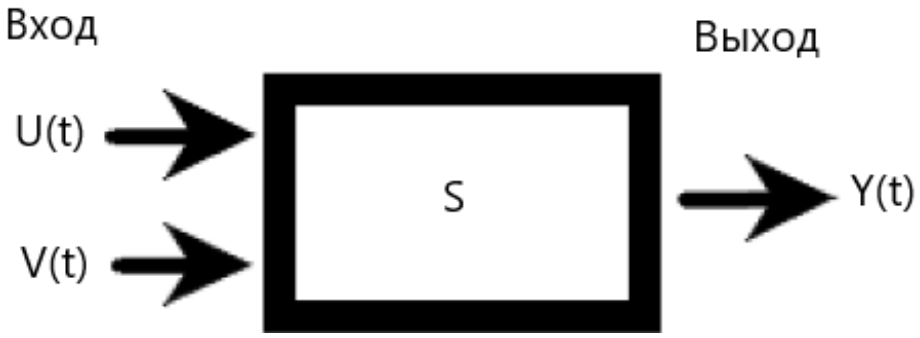

Рис. 1. *Модель черного ящика*

Рассматривая векторный выход системных параметров Y(t), мы понимаем, что это может быть реакция системы на управление в нормальном режиме работы по входящему каналу U(t) или неуправляемому каналу V(t) при вмешательстве с целью нанесения вреда системе, в которой объект (S) служит исполнительным органом. При этом существует вероятность множественных возможных значений (X) и элементов упорядоченного множества (T), моментов времени (t). Таким образом, вероятность событий $T \rightarrow X$, $X(t) \in X^T$, $t \in T$.

На сегодняшний день велика вероятность того, что при внешнем воздействии или активации вируса в системе управления и мониторинга параметров персонал при удаленном нахождении от объекта управления не сможет распознать (услышать, увидеть), что объект больше не поддается регулированию и, по сути, является неуправляемой системой, что может привести к негативным последствиям. Существует нерешенная задача по созданию саморазвивающейся модели, которая сможет в режиме реального времени проводить самообучение, тем самым являясь гарантом оперативного пресечения негативных воздействий и при необходимости — возвращения системы в штатный режим работы.

Проведя анализ часто применяемого электрооборудования, систем управления и передачи данных, можно выдвинуть предположение, что ИИ был бы востребован как дополнительная (автономная) система мониторинга состояний электрооборудования, систем контроля и передачи данных [7–10], а также для сравнения значений сигналов, которые приходят от электрооборудования по сетям контроля и передачи данных в контроллер и от него — на верхний уровень, с сигналами, которые получает ИИ от тех же датчиков, что и система управления [11]. При возникновении разницы между приходящим и уходящим сигналом контроллера ИИ мог бы мгновенно формировать реестр ошибочных сигналов и передавать его оператору, тем самым давая возможность оперативному персоналу объекта КИИ предпринять необходимые действия для проверки и устранения неисправностей. На рисунке 2 представлена разработанная нами схема высокой автоматизации, в которую встроен ИИ, условные обозначения и изображения рисунка 2 представлены на рисунке 3.

Применение ИИ может позволить сформировать независимый контур сбора и анализа параметров состояния систем объекта КИИ, в том числе на базе оценки больших данных о косвенных

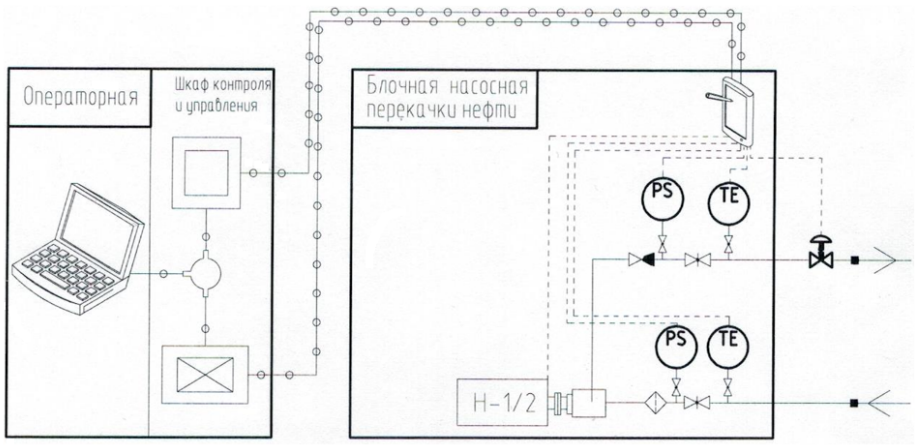

Рис. 2. *Схема высокой автоматизации*

УСЛОВНЫЕ ОБОЗНАЧЕНЯ И ИЗОБРАЖЕНИЯ

Обозначение и изображение	Характеристика
	Интерфейс передачи данных (ETHERNET)
	Интерфейс передачи данных (RS-485)
	Нефтепровод технологический
	Клапан регулирующий с электроприводом
	Направление выхода жидкости
	Направление входа жидкости
	Задвижка ручная
	Комбинированный клапан
PS	Датчик давления
TE	Датчик температуры
	Сетчатый фильтр
H-1/2	Насосный агрегат
	Станция управления насосной (по месту)
	Клапан обратный
	Рабочее место оператора
	Контроллер
	Искусственный интеллект
	Маршрутизатор

Рис. 3. *Условные обозначения и изображения*

признаках работы основного оборудования, например, таких как небольшие отклонения от обычных значений температуры оборудования, потребления электроэнергии и т.п. [12]. Такой дополнительный, внешний по отношению к основным системам контур безопасности позволит снизить уязвимость объектов КИИ к вредоносным воздействиям, являясь вспомогательной надстройкой к существующим программам, сетям и оборудованию.

Заключение

Таким образом, система управления на базе ИИ дает возможность дополнительного мониторинга состояния существующих систем без вмешательства в действующую программу управления электрооборудованием, при этом оперативный персонал получает полностью автономную систему наблюдения, которая по косвенным параметрам с датчиков позволяет обнаружить и пресечь любые внешние воздействия на системы управления на объекте.

Алгоритмы ИИ предоставляют в режиме реального времени возможность анализировать ключевые параметры работы оборудования, и при их отклонении от штатных показателей система на базе ИИ оказывает интеллектуальную поддержку оператору в форме актуальных алгоритмов, направленных на стабилизацию производственного процесса и его возвращение к штатному режиму работы.

Эффективным решением для обеспечения информационной и промышленной безопасности будет внедрение в существующие системы защиты и управления КИИ технологий на основе искусственного интеллекта. В этой связи разработка интеллектуальных моделей для применения в управлении КИИ представляется одной из наиболее актуальных задач.

ЛИТЕРАТУРА

1. Востров В. А., Гавриленко Т. В., Исмайлов Э. М. Некоторые аспекты разработки интеллектуальной модели для финансового риск-менеджмента нефинансовых организаций. *Успехи кибернетики*. 2023;4(4):74-80. DOI: 10.51790/2712-9942-2023-4-4-07.
2. Wen L., Li X., Gao L., Zhang Y. A New Convolutional Neural Network-Based Data-Driven Fault Diagnosis Method. *IEEE Transactions on Power Delivery.* 2017;65(7):5990-5998. DOI: 10.1109/TIE.2017.2774777.
3. Мадуро заявил об атаках на энергосистему Венесуэлы изнутри. *Информационное агентство Интерфакс.* Режим доступа: https://www.interfax.ru/world/653598.
4. Ромашкина Н. П., Махукова А. В. Компьютерная вредоносная атака на ядерную программу Ирана. *Информационные войны*. 2013;(4):40–50.
5. О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных». *Федеральный закон от 24.04.2020 № 123-ФЗ.* Режим доступа: http://www.kremlin.ru/acts/bank/45475.
6. Облачные сервисы: что это такое, какими они бывают и кому полезны. *Skillbox Media.* Режим доступа: https://skillbox.ru/media/code/oblachnye-servisy-chto-takoe-kakimi-byvayut-i-komu-polezny/.
7. Masa'd F. M., Al-maaitah T. A., Al-maaitah D. A., Qawasmeh E. F., Qatawneh N. A. Harnessing Artificial Intelligence for Human Resources Management: Tools, Advantages, and Risks in the Energy Sector. *E3S Web of Conferences*. 2024;541(4). DOI: 10.1051/e3sconf/202454102004.
8. Lee H. J., Ahn B. S., Park Y. M. A Fault Diagnosis Expert System for Distribution Substations. *IEEE Transactions on Power Delivery.* 2000;15(1):92-97. DOI: 10.1109/61.847234.
9. Sun J., Qin S. Y., Song Y. H. Fault Diagnosis of Electric Power Systems Based on Fuzzy Petri Nets. *IEEE Transactions on Power Delivery.* 2004;19(4):2053-2059. DOI: 10.1109/TPWRS.2004.836256.
10. Yongli Z., Limin H., Jinling L. Bayesian Networks-Based Approach for Power Systems Fault Diagnosis. *IEEE Transactions on Power Delivery.* 2006;21(2):634-639. DOI: 10.1109/TPWRD.2005.858774.
11. Iqbal R., Maniak T., Doctor F., Karyotis C. Fault Detection and Isolation in Industrial Processes Using Deep Learning Approaches. *IEEE Transactions on Power Delivery.* 2019;15(5):3077-3084. DOI: 10.1109/tii.2019.2902274.
12. Lo N. G., Flaus J. M., Adrot O. Review of Machine Learning Approaches in Fault Diagnosis Applied to IoT Systems. *International Conference on Control, Automation and Diagnosis*. 2019:1-6. DOI: 10.1109/ICCAD46983.2019.9037949.