УДК 331.4

Агаларян Н.Н.
Ведущий эксперт Центр компетенций
технологического развития ТЭК
при Минэнерго России
Мухаметсафин Б.И., *магистрант кафедры*
«Мировая экономика»
ФГБОУ ВО «Дипломатическая академия МИД России»
Россия, Москва

ПРОМЫШЛЕННАЯ БЕЗОПАСНОСТЬ В ЭПОХУ ЦИФРОВИЗАЦИИ: КАК ЭНЕРГЕТИКА СПРАВЛЯЕТСЯ С НОВЫМИ УГРОЗАМИ

В статье рассматриваются актуальные направления развития промышленной безопасности в условиях стремительной цифровизации энергетического сектора. Особое внимание уделяется трансформации подходов к управлению рисками на фоне внедрения технологий искусственного интеллекта (ИИ), промышленного интернета вещей (IIoT), цифровых двойников и автоматизированных систем мониторинга. Анализируются новые вызовы, связанные с ростом киберугроз, усилением нормативных требований и необходимостью адаптации устаревшей инфраструктуры. Приводятся примеры эффективных технологических решений и стратегий крупнейших мировых компаний.

Ключевые слова: *промышленная безопасность, энергетика, цифровизация, искусственный интеллект, IIoT, предиктивная аналитика, кибербезопасность.*

Современные тренды промышленной безопасности в нефтегазовой отрасли демонстрируют парадоксальную динамику: с одной стороны, цифровая трансформация открывает беспрецедентные возможности для

предотвращения аварий, с другой – создает принципиально новые риски. Объем мирового рынка решений по обеспечению безопасности в 2024 году составил 404,14 млрд долл. США[1], в то время как объем рынка нефтегазовой безопасности – 35,7 млрд долл. США, и, по прогнозам экспертов, к 2033 году он достигнет 54,2 млрд долл. США.[2] При этом, уровень аварийности остаётся высоким: частота серьёзных происшествий не демонстрирует устойчивого снижения, а совокупный ущерб отрасли от инцидентов в последние годы оценивается в миллионы долларов ежегодно. Согласно ежегодному отчету IBM «Cost of a Data Breach» за 2024 год, в 2023 году средний мировой ущерб от утечки данных вырос до 4,88 млн долл. США, а в промышленном секторе – 5,56 млн долларов США, что на 18% выше по сравнению с предыдущим годом.[3]

Среди ключевых угроз цифровой эпохи особое внимание специалистов привлекает усиливающаяся киберуязвимость производственной инфраструктуры. В 2024 году в России медианное число кибератак в месяц достигало порядка 10 тысяч, а общее количество инцидентов с высоким уровнем критичности приблизилось к 26 тысячам. При отсутствии своевременного реагирования примерно каждый пятый из таких инцидентов мог привести к финансовым потерям для российских компаний, превышающими 1 миллион рублей.

Особенно тревожна ситуация в сегменте критической информационной инфраструктуры (КИИ): на нее пришлось около 64% всех зафиксированных атак (см. рис. 1).[4] В числе основных целей атак – объекты нефтегазового

[1] Отчет об анализе размера, доли и тенденций мирового рынка решений по безопасности — обзор отрасли и прогноз до 2032 года. – URL: https://www.databridgemarketresearch.com/ru/reports/global-security-solutions-market (дата обращения: 02.05.2025).

[2] Verified Market Reports. Oil and Gas Security Market. – URL: https://www.verifiedmarketreports.com/product/oil-and-gas-security-market/ (дата обращения: 02.05.2025).

[3] Risk & Insurance. Global Average Cost of a Data Breach Reaches $4.88M in 2023. – URL: https://riskandinsurance.com/global-average-cost-of-a-data-breach-reaches-4-88m-in-2023/#:~:text=Business%20disruption%20and%20response%20costs,plugging%20talent%20gaps%2C%20IBM%20finds.&text=The%20global%20average%20cost%20of,Data%20Breach%20Report%20for%202024 (дата обращения:02.05.2025).

[4] TAdviser. Число кибератак в России и мире. – URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A7%D0%B8%D1%81%D0%BB%D0%BE_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA_%D0%B2_%D0%A0%D0%BE%D1%81%

комплекса, как на уровне систем управления технологическими процессами, так и в системах физической безопасности. Угроза исходит не только от индивидуальных злоумышленников, но и от организованных хакерских группировок, в том числе предположительно аффилированных с государственными структурами, таких как CyberAv3ngers.

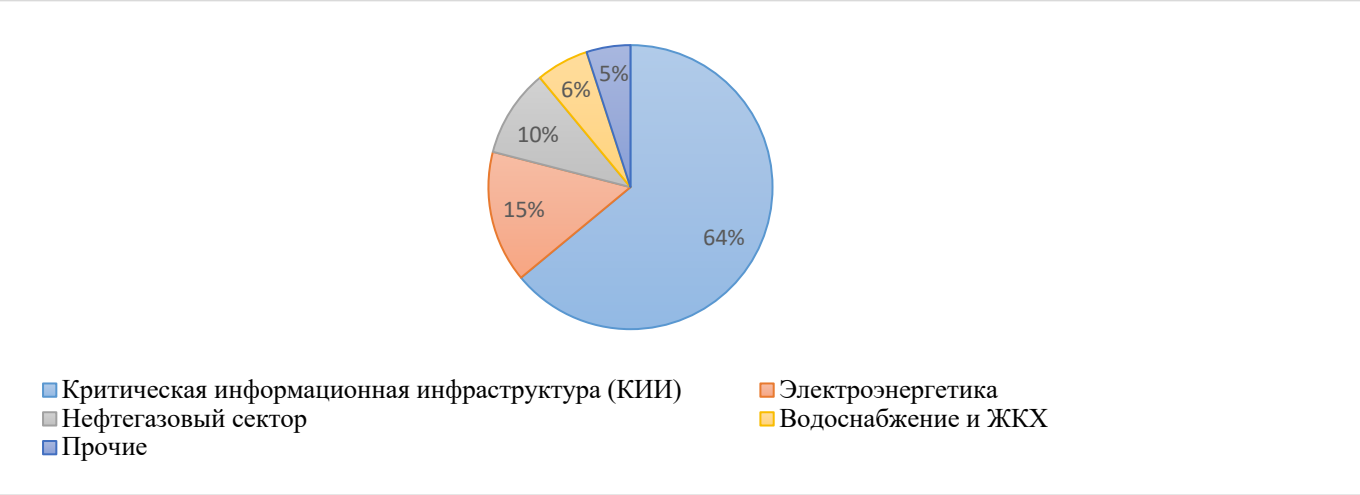

Рис. 1. Распределение кибератак по секторам энергетики в России в 2024 году[5]

Положительным примером противодействия киберугрозам стали действия RED Security SOC, центра круглосуточного мониторинга и реагирования на киберугрозы с более 8,6 млрд анализируемых событий в сутки, благодаря которым в 2024 году удалось предотвратить совокупный ущерб на сумму порядка 26 миллиардов рублей.[6] Кроме того, RED Security SOC выделило топ-3 наиболее атакуемых отрасли за 2024 год (см. рис. 2), что позволило сфокусировать усилия на защите наиболее уязвимых сегментов. Данный пример подчёркивает критическую значимость проактивной цифровой защиты и необходимость постоянного развития механизмов реагирования.

D1%81%D0%B8%D0%B8_%D0%B8_%D0%B2_%D0%BC%D0%B8%D1%80%D0%B5#:~:text=%D0%A1%D0%BE%D0%B2%D0%BE%D0%BA%D1%83%D0%BF%D0%BD%D1%8B%D0%B9%20%D1%83%D1%89%D0%B5%D1%80%D0%B1%20%D0%BE%D1%82%20%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D0%B8%2C%20%D0%BA%D0%BE%D1%82%D0%BE%D1%80%D1%8B%D0%B9,%D0%BE%D0%B1%D1%89%D0%B5%D0%B3%D0%BE%20%D1%87%D0%B8%D1%81%D0%BB%D0%B0%20%D0%B8%D0%BD%D1%86%D0%B8%D0%B4%D0%B5%D0%BD%D1%82%D0%BE%D0%B2%20%D0%B7%D0%B0%20%D0%B3%D0%BE%D0%B4. (дата обращения: 03.05.2025).

[5] См выше

[6] RED Security. RED Security SOC. – URL: https://redsecurity.ru/services/red-soc (дата обращения: 03.05.2025).

Рис. 2. Топ 3 атакуемых отрасли за 2024 год[7]

На этом фоне в отрасли промышленной безопасности наблюдается стремительная технологическая трансформация. Одним из ключевых решений становятся цифровые двойники (Digital Twins), применение которых позволяет снизить вероятность аварий на 30-40% благодаря точному моделированию процессов и оперативному выявлению отклонений[8]. Мировой опыт подтверждает эффективность данной технологии: например, компания Boeing зафиксировала 40-процентное улучшение показателей качества с первого раза благодаря применению цифровых двойников для прогнозирования производительности различных компонентов.[9]

Дополнительные преимущества обеспечивает внедрение предиктивного обслуживания, основанного на анализе больших данных и машинном обучении. Согласно оценкам McKinsey, подобные решения позволяют снизить количество аварийных отказов на 70% и сократить затраты на техническое обслуживание до 30%. Высокую эффективность демонстрируют также системы прогнозирования на базе ИИ. Так, модель Deep Transformer Pro показала точность прогнозирования отказов трансформаторов до более чем 90%, что привело к снижению количества неплановых отключений на 50% и сокращению затрат на ремонт на 40%.

[7] См выше

[8] РБК. Цифровые двойники: как они предотвращают аварии и снижают издержки. – URL: https://companies.rbc.ru/news/XeiwGxNYnr/tsifrovyie-dvojniki-kak-oni-predotvraschayut-avarii-i-snizhayut-izderzhki/ (дата обращения: 03.05.2025).

[9] Royale International. Digital Twins Need Time Critical Solutions. – URL: https://www.royaleinternational.com/2024/02/digital-twins-need-time-critical-solutions/ (дата обращения: 04.05.2025).

На российском рынке эта модель активно внедряется ведущими энергетическими компаниями: «Энергосбыт» применяет модель для прогнозирования отказов трансформаторов, «Интер РАО» – для оптимизации плана технического обслуживания трансформаторов, а «Россети» – для мониторинга состояния трансформаторов на своей обширной сети.[10] Кроме того, внедрение дистанционного мониторинга с использованием беспилотных летательных аппаратов (БПЛА) существенно сокращает затраты на инспекции. Профессиональные программы инспекции с применением дронов позволяют снизить расходы на проверки до 60%, одновременно повышая качество и скорость выявления дефектов до 97%.[11]

Крупнейшие международные нефтегазовые корпорации, такие как BP, Shell и ExxonMobil, активно инвестируют в развитие цифровой безопасности, включая разработку квантовых алгоритмов и участиев передовых технологических инициативах, таких как IBM Q Network (IoT World Today, 2022)[12], что особенно актуально в условиях роста киберугроз и ужесточения международных стандартов.

На Ближнем Востоке, в частности в Саудовской Аравии и ОАЭ, цифровая трансформация осуществляется в рамках масштабных национальных программ, таких как Saudi Vision 2030 и UAE Energy Strategy 2050, предусматривающих интеграцию технологий IIoT, цифровых двойников и ИИ для повышения эффективности управления рисками и мониторинга критически важных объектов.

США и Канада традиционно демонстрируют высокий уровень интеграции передовых цифровых решений в промышленную безопасность. К примеру, компании Shell и Chevron активно используют комплексные ИИ-платформы и

[10] Искусственный интеллект в прогнозировании отказов трансформаторов: Neurotech Deep Learning Deep Transformer Pro Model Prognosis. – URL: https://shtykatyrka.ru/iskusstvennyy-intellekt-v-prognozirovanii-otkazov-transformatorov-neurotech-deep-learning-deep-transformer-pro-model-prognosis-dlya-povysheniya-nadezhnosti (дата обращения: 04.05.2025).

[11] Averroes.ai. Mastering Drones for Utility Inspection: Use Cases, Cost & Tips. – URL: https://averroes.ai/blog/mastering-drones-for-utility-inspection-use-cases-cost-tips (дата обращения: 06.05.2025).

[12] IoT World Today. Quantum Computing Summit Austin 2022: Air Force Gives Quantum Update. – URL: https://www.iotworldtoday.com/industry/quantum-computing-summit-austin-2022-air-force-gives-quantum-update (дата обращения: 04.05.2025).

инструменты предиктивной аналитики. Примером может служить программное обеспечение (ПО) PIPA Pre-Incident Planning Software for safety professionals от Shell. Оно обеспечивает широкий спектр аналитических выходных данных – от простых графиков, демонстрирующих масштабы возможных последствий инцидентов, до детализированных планов аварийного реагирования с указанием зон риска, требований к защите и обоснований применяемых решений.

Согласно данным консалтинговой компании DNV, к 2025 году около 47% нефтегазовых компаний планируют активно использовать технологии ИИ для управления рисками. Однако внедрение таких решений сопряжено с рядом трудностей: дефицит квалифицированных специалистов, высокие затраты на внедрение, а также сложности интеграции ИИ-решений в устаревшие технологические и производственные платформы, без снижения их операционной эффективности.

Эксперты DNV подчеркивают, что успешная цифровая трансформация требует не только передовых технологий, но и устойчивой экосистемы партнерств, включающей взаимодействие между технологическими компаниями, отраслевыми операторами и регулирующими органами. Только при согласованных действиях всех участников возможно комплексное раскрытие потенциала цифровизации в целях повышения промышленной безопасности.[13]

Дополнительным драйвером цифровой трансформации выступает ужесточение нормативно-правовых требований в сфере информационной и промышленной безопасности. На международном уровне основу таких требований формируют стандарты ISO/IEC 27001[14], а также методология NIST Cybersecurity Framework (CSF)[15], которые задают структуру для построения

[13] DNV. AI Spells Opportunity and Manageable Risk for the Oil and Gas Industry. – URL: https://www.dnv.com/article/ai-spells-opportunity-and-manageable-risk-for-the-oil-and-gas-industry/ (дата обращения: 08.05.2025).
[14] ISO. ISO/IEC 27001 Information Security Management. – URL: https://www.iso.org/standard/27001 (дата обращения: 07.05.2025).
[15] NIST. Cybersecurity Framework. – URL: https://www.nist.gov/cyberframework (дата обращения: 06.05.2025).

систем управления информационной безопасностью. В России ключевым регуляторным документам относятся Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ[16], Федеральный закон «О промышленной безопасности опасных производственных объектов» от 21.07.1997 № 116-ФЗ [17] и Распоряжение Правительства Российской Федерации от 12 марта 2024 г. № 581-р Об утверждении стратегического направления в области цифровой трансформации топливно-энергетического комплекса до 2030 года [18] , дополненные подзаконными актами, разработанными Минэнерго России, а также национальной версией международного стандарта – ГОСТ Р ИСО/МЭК 27001-2012 [19] . Специфические отраслевые рекомендации, в частности, по обеспечению кибербезопасности технологических систем в нефтегазовом секторе, закреплены в документах, таких как API Standard 1164[20].

Для эффективного обеспечения промышленной безопасности в условиях ускоренной цифровизации энергетического сектора необходим переход от точечных инициатив к целостной стратегии цифровой устойчивости, что предполагает не только внедрение технологий ИИ, цифровых двойников и IIoT, но и глубокую трансформацию корпоративного подхода к управлению рисками. Ключевыми элементами такой стратегии должны стать проактивное прогнозирование инцидентов, построение надежной системы кибербезопасности с опорой на международные и национальные стандарты, развитие внутренней экспертизы и технологических партнерств, а также

[16] КонсультантПлюс. Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры». – URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 05.05.2025).
[17] КонсультантПлюс.О промышленной безопасности опасных производственных объектов: федер. закон РФ от 21.07.1997 № 116-ФЗ – URL: https://www.consultant.ru/document/cons_doc_LAW_15234/ (дата обращения: 06.05.2025).
[18] КонсультантПлюс.Распоряжение Правительства Российской Федерации от 12 марта 2024 г. № 581-р Об утверждении стратегического направления в области цифровой трансформации топливно-энергетического комплекса до 2030 года. – URL: https://www.garant.ru/products/ipo/prime/doc/408610169/ (дата обращения: 06.05.2025).
[19] ГОСТ Р ИСО/МЭК 27001-2012. – URL: https://gostassistent.ru/doc/ec4dfe5d-a428-4404-8613-32edc5826be9 (дата обращения: 07.05.2025).
[20] API Standard 1164. Important Standards Announcements. – URL: https://www.api.org/products-and-services/standards/important-standards-announcements/1164 (дата обращения: 05.05.2025).

интеграция экологических аспектов в систему промышленного мониторинга. Важно не просто применять цифровые решения, а выстраивать вокруг них устойчивую инфраструктуру и культуру безопасности, способную адаптироваться к быстро меняющимся угрозам и требованиям. Только такой подход позволит компаниям не только минимизировать количество инцидентов и убытки, но и укрепить доверие со стороны государства, общества и международных рынков.

Библиографический список

1. API Standard 1164. Important Standards Announcements. – URL: https://www.api.org/products-and-services/standards/important-standards-announcements/1164 (дата обращения: 05.05.2025).
2. Averroes.ai. Mastering Drones for Utility Inspection: Use Cases, Cost & Tips. – URL: https://averroes.ai/blog/mastering-drones-for-utility-inspection-use-cases-cost-tips (дата обращения: 06.05.2025).
3. DNV. AI Spells Opportunity and Manageable Risk for the Oil and Gas Industry. – URL: https://www.dnv.com/article/ai-spells-opportunity-and-manageable-risk-for-the-oil-and-gas-industry/ (дата обращения: 08.05.2025).
4. DNV GL. Energy Transition Outlook 2024: Safety and Digitalization. – URL: https://sun-connect.org/wpcont/uploads/DNV_ETO_2024_Main_Report_b-compressed.pdf (дата обращения: 05.05.2025).
5. ГОСТ Р ИСО/МЭК 27001-2012. – URL: https://gostassistent.ru/doc/ec4dfe5d-a428-4404-8613-32edc5826be9 (дата обращения: 07.05.2025).
6. IBM Security X-Force. Threat Intelligence Index 2023: Energy Sector Analysis. – URL: https://secure-iss.com/wp-content/uploads/2023/02/IBM-Security-X-Force-Threat-Intelligence-Index-2023.pdf (дата обращения: 05.05.2025).

7. International Energy Agency (IEA). Energy Cybersecurity 2023. – URL: https://www.iea.org/reports/world-energy-outlook-2023 (дата обращения: 06.05.2025).
8. ISO. ISO/IEC 27001 Information Security Management. – URL: https://www.iso.org/standard/27001 (дата обращения: 07.05.2025).
9. Zhdaneev, O. V. Technological and institutional priorities of the oil and gas complex of the Russian Federation in the term of the world energy transition / O. V. Zhdaneev, K. N. Frolov // International Journal of Hydrogen Energy. – 2024. – Vol. 58. – P. 1418-1428. – DOI 10.1016/j.ijhydene.2024.01.285.
10. Бравков, П. В. К вопросу о непрерывности ведения бизнеса предприятий нефтегазовой отрасли России. Часть 1 / П. В. Бравков, О. В. Жданеев, В. С. Чубоксаров // Стандарты и качество. – 2020. – № 8. – С. 88-94.
11. Жданеев, О. В. Оценка уровня локализации продукции при импортозамещении в отраслях ТЭК / О. В. Жданеев // Экономика региона. – 2022. – Т. 18, № 3. – С. 770-786. – DOI 10.17059/ekon.reg.2022-3-11.
12. КонсультантПлюс. Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры». – URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 05.05.2025).
13. КонсультантПлюс. О промышленной безопасности опасных производственных объектов: федер. закон РФ от 21.07.1997 № 116-ФЗ. – URL: https://www.consultant.ru/document/cons_doc_LAW_15234/ (дата обращения: 06.05.2025).
14. КонсультантПлюс. Распоряжение Правительства Российской Федерации от 12 марта 2024 г. № 581-р Об утверждении стратегического направления в области цифровой трансформации топливно-энергетического комплекса до 2030 года. – URL: https://www.garant.ru/products/ipo/prime/doc/408610169/ (дата обращения: 06.05.2025).

15. IoT World Today. Quantum Computing Summit Austin 2022: Air Force Gives Quantum Update. – URL: https://www.iotworldtoday.com/industry/quantum-computing-summit-austin-2022-air-force-gives-quantum-update (дата обращения: 04.05.2025).
16. RED Security. RED Security SOC. – URL: https://redsecurity.ru/services/red-soc (дата обращения: 03.05.2025).
17. Risk & Insurance. Global Average Cost of a Data Breach Reaches $4.88M in 2023. – URL: https://riskandinsurance.com/global-average-cost-of-a-data-breach-reaches-4-88m-in-2023/#:~:text=Business%20disruption%20and%20response%20costs,plugging%20talent%20gaps%2C%20IBM%20finds.&text=The%20global%20average%20cost%20of,Data%20Breach%20Report%20for%202024 (дата обращения: 02.05.2025).
18. РБК. Цифровые двойники: как они предотвращают аварии и снижают издержки. – URL: https://companies.rbc.ru/news/XeiwGxNYnr/tsifrovyie-dvojniki-kak-oni-predotvraschayut-avarii-i-snizhayut-izderzhki/ (дата обращения: 03.05.2025).
19. Royale International. Digital Twins Need Time Critical Solutions. – URL: https://www.royaleinternational.com/2024/02/digital-twins-need-time-critical-solutions/ (дата обращения: 04.05.2025).
20. Искусственный интеллект в прогнозировании отказов трансформаторов: Neurotech Deep Learning Deep Transformer Pro Model Prognosis. – URL: https://shtykatyrka.ru/iskusstvennyy-intellekt-v-prognozirovanii-otkazov-transformatorov-neurotech-deep-learning-deep-transformer-pro-model-prognosis-dlya-povysheniya-nadezhnosti (дата обращения: 04.05.2025).
21. TAdviser. Число кибератак в России и мире. – URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A7%D0%B8%D1%81%D0%BB%D0%BE_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%

D0%B8_%D0%B8_%D0%B2_%D0%BC%D0%B8%D1%80%D0%B5#:~:text=%D0%A1%D0%BE%D0%B2%D0%BE%D0%BA%D1%83%D0%BF%D0%BD%D1%8B%D0%B9%20%D1%83%D1%89%D0%B5%D1%80%D0%B1%20%D0%BE%D1%82%20%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D0%B8%2C%20%D0%BA%D0%BE%D1%82%D0%BE%D1%80%D1%8B%D0%B9,%D0%BE%D0%B1%D1%89%D0%B5%D0%B3%D0%BE%20%D1%87%D0%B8%D1%81%D0%BB%D0%B0%20%D0%B8%D0%BD%D1%86%D0%B8%D0%B4%D0%B5%D0%BD%D1%82%D0%BE%D0%B2%20%D0%B7%D0%B0%20%D0%B3%D0%BE%D0%B4 (дата обращения: 03.05.2025).

22. Verified Market Reports. Oil and Gas Security Market. – URL: https://www.verifiedmarketreports.com/product/oil-and-gas-security-market/ (дата обращения: 02.05.2025).
23. Отчет об анализе размера, доли и тенденций мирового рынка решений по безопасности — обзор отрасли и прогноз до 2032 года. – URL: https://www.databridgemarketresearch.com/ru/reports/global-security-solutions-market (дата обращения: 02.05.2025).