



AKTUAR MOLIYA VA BUXGALTERIYA HISOBI ILMIY JURNALI

Vol. 5 Issue 02 | pp. 327-334 | ISSN: 2181-1865

Available online <https://finance.tsue.uz/index.php/afa>

АСПЕКТЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА РЫНКЕ НЕФТЕГАЗОВОЙ ОТРАСЛИ УЗБЕКИСТАНА



Абдуллаева Дилора Куйсуновна

Ташкентский международный университет
финансового управления

и технологий негосударственное высшее учебное
заведение, к.э.н., доц., Доцент каф. «Экономика и управление»

E-mail: d.abdullayeva@tift.uz

Annotatsiya: Neft va gaz bozorida sun'iy intellektning kiberxavfsizligi so'nggi paytlarda tobora muhim ahamiyat kasb etmoqda, chunki korporatsiyalar katta miqdordagi nozik ma'lumotlarni qayta ishlaydi va bu ma'lumotlarni tarmoqlar bo'ylab uzatadi. Kiberxavfsizlik ma'lumotlarni ruxsatsiz kirishdan himoya qilishga qaratilgan. Bu, ayniqsa, masofadan turib ishlashda to'g'ri keladi. Maqolada so'nggi paytlarda ro'y bergan kiberbuzilishlar kiberxavfsizlik mahsulotlariga talabning oshishiga olib kelgani haqida so'z boradi.

Kalit so'zlar: sun'iy intellekt, raqamlashtirish, kiberxavfsizlik, kiberbuzarliklar, axborot texnologiyalari

Аннотация: Кибербезопасность искусственного интеллекта на рынке нефтегазовой отрасли в последнее время становится все более важной, поскольку корпорации обрабатывают огромные объемы конфиденциальной информации и передают эти данные по сетям. Кибербезопасность фокусируется на защите данных от несанкционированного доступа. Это особенно актуально при удаленной работе. В статье рассматривается, что в последнее время случаи кибервзломов привели к увеличению спроса на продукты кибербезопасности.

Ключевые слова: искусственный интеллект, цифровизация, кибербезопасность, кибервзломы, информационные технологии

Abstract: Artificial intelligence cybersecurity in the oil and gas market has become increasingly important in recent years as corporations process huge amounts of sensitive information and transmit this data over networks. Cybersecurity focuses on protecting data from unauthorized access. This is especially true when working remotely. The article considers that in recent times, cases of cyber hacks have increased the demand for cybersecurity products.

Keywords: artificial intelligence, digitalization, cybersecurity, cyber hacks, information technology.

Введение

Актуальность темы исследования определяется тем, что нефть и газ являются уникальными товарами, не имеющих заменителей в энергетическом секторе не только Узбекистана, но и всего мира, особенно с учетом геополитической ситуации в

мире и возможностей внедрения искусственного интеллекта на рынке нефтегазовой отрасли, о чем свидетельствуют следующие цифры: искусственный интеллект на рынке нефти и газа оценивался в 2023 году в 2 034,9 млн долларов США, и к 2027 году он достигнет 3 669,8 млн долларов США, что означает среднегодовой темп роста в 10,81% в течение прогнозируемого периода (2023-2027 годы).

Свою нишу в сегментации рынка нефтегазовых стран-участников имеет Узбекистан. Как неотложная поставлена задача удвоения доли цифровых услуг в ВВП Узбекистана в ближайшие два года и планируется привлечь около 2,5 млрд долларов инвестиций на развитие цифровой инфраструктуры.

Искусственный интеллект на рынке нефтегазовой отрасли Узбекистана при этом становится мишенью для случаев кибервзломов, что увеличило спрос на продукты кибербезопасности.

По оценкам компании Cybersecurity Ventures прогнозируются высокие темпы роста кибератак, около 12–15% в годовом исчислении до 2025 года, что выше 8–10%, прогнозируемых другими отраслевыми аналитиками.

Материалы и методы исследования

На сегодняшний день компании нефтегазового сектора экспериментируют с технологиями искусственного интеллекта для повышения эффективности и доходов. Используя искусственный интеллект в нефтегазовых операциях, корпорации заинтересованы в разработке и создании передовых аналитических решений для управления бурением на суше и на дне океана.

Анализ ситуации на нефтегазовом рынке выявил следующие ключевые тенденции искусственного интеллекта :

- Цифровые двойники нефтегазовых компаний делают процессы разведки и добычи более эффективными и оптимизированными. Цифровая модель месторождений и карьеров представляет собой виртуальную объемную копию месторождения, которая позволяет наблюдать за процессами, протекающими при разработке, прогнозировать результаты работы, вносить корректировки по мере эксплуатации.
- Благодаря интеграции программного обеспечения искусственного интеллекта нефтегазовые компании потенциально получают важную информацию для улучшения своих бизнес-результатов в предшествующих процессах. Этот процесс может включать в себя передачу в программное обеспечение отобранных записей данных и информации из источников данных, включая структурированные документы, PDF-файлы, рукописные заметки, аудио- или видеофайлы.
- В соответствии с Парижским соглашением нефтегазовые компании обязали достичь нулевых выбросов углерода к 2050 году, чтобы минимизировать свой углеродный след, что вызывает необходимость использования технологии искусственного интеллекта для профилактического обслуживания оборудования, чтобы уменьшить экологический ущерб. Искусственный интеллект позволяет нефтегазовым корпорациям предвидеть и устранять вероятные неисправности оборудования до того, как они произойдут.
- Компания Baker Hughes, занимающаяся энергетическими технологиями, и AIQ, совместное предприятие по искусственному интеллекту Национальной

нефтяной компании Абу-Даби (ADNOC) с Group 42, объявили о заключении соглашения о стратегическом сотрудничестве для создания передовых аналитических решений в мировой нефтегазовой промышленности.

- «Цифровое месторождение - это не что иное, как эволюция и объединение технологий бурения, разведки, цифрового управления процессами и производствами добычи нефти и газа в сочетании с современными коммуникационными технологиями». Искусственный интеллект используется для оптимизации добычи с помощью компьютерного зрения для более быстрого анализа сейсмических и подземных данных, минимизация времени простоя для профилактического обслуживания нефтегазового оборудования, понимание пласта и моделирование для прогнозирования рисков добычи нефти при сокращении времени обслуживания и расходов.
- Искусственный интеллект использует наземную систему управления InForce, которая сочетает в себе гидравлическую энергию для активации скважинных инструментов и логику управления для управления интеллектуальной системой скважин.. В частности, управляет функциями системы для более сложных конфигураций закачивания и в основном используется там, где удаленные операции должны выполняться через существующую SCADA(Например, компания Baker Hughes).
- Технологии искусственного интеллекта используются нефтегазовыми компаниями в оцифровке записей и автоматизации анализа собранных геологических данных и карт, что способствует выявлению проблем, таких как коррозия трубопровода или сбои в работе оборудования.

Однако по мере того, как в нефтегазовой отрасли появляется все больше сетевых технологий, компании сталкиваются с проблемами и новыми рисками кибербезопасности и пониманием того, что требуется для борьбы с ними, опираясь при этом на основы кибербезопасности.(рис 1)

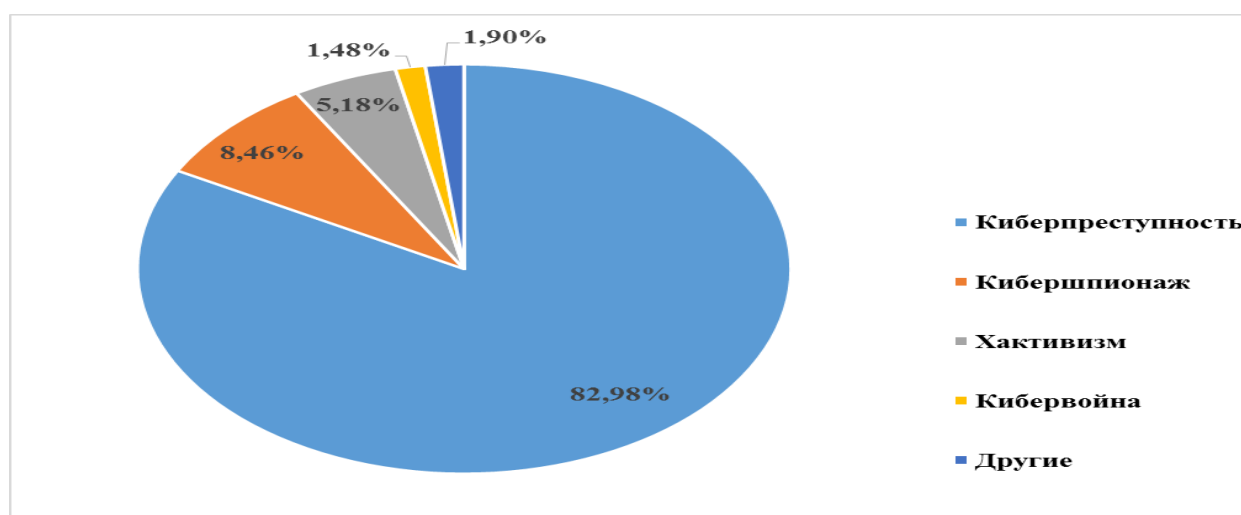


Рис 1. Распределение видов кибератак на нефтегазовые компании за девять месяцев 2024 года¹.

¹ www.honeywellprocess.com/en-US/news-and-events/Pages/pr-12062017-honeywell-survey-shows-low-adoption-of-industrial-cyber-security-measures.aspx

Различные типы кибератак, такие как неправомерное использование инсайдерской информации, атаки на веб-приложения и физический риск/потеря имущества, имеют отношение и к нефтегазовой отрасли. Последствия атак могут носить масштабный и техногенный характер: от задержек поставок, снижения добычи до влияния на жизни, здоровье людей и окружающую среду

В терминах модели зрелости безопасности искусственного интеллекта нефтегазового сектора таких как интернет вещей, а также модели зрелости цифровых двойников (IIC Digital Twin Consortium IoT SMM), речь идет о практиках домена «Укрепление безопасности». Реализация этих практик на предприятиях нефтегазовой промышленности может требовать различных затрат в зависимости от того, к какой категории это предприятие относится.

Графики кибератак, опубликованных за девять месяцев 2024 года насчитывает 946 событий (10,51 событий в день), что заметно меньше (почти 30%) по сравнению с аналогичным периодом прошлого года.

По прогнозам искусственный интеллект на рынке нефти и газа будет расти в среднем на 10,81% в течение следующих 5 лет.

Азиатско-Тихоокеанский регион демонстрирует самый высокий среднегодовой темп роста искусственного интеллекта на рынке нефти и газа в 2018–2028 годах.

При этом рынок нефтегазовой безопасности растет со среднегодовым темпом роста 4,65% в течение следующих 5 лет. Более того, кибератаки в этом секторе вызвали значительные сбои во всей сети, включая восходящие, промежуточные и нисходящие процессы.

Поэтому компании внедряют эффективные решения в области кибербезопасности для борьбы с ними.

Анализ рынка нефтегазовой безопасности

Рынок нефтегазовой безопасности оценивался в 26,34 млрд долларов США в 2023 году и, как ожидается, достигнет 34,59 млрд долларов США к 2026 году и будет расти со среднегодовым темпом роста 4,65% в течение прогнозируемого периода 2021-2026 годов.

Анализ рынка нефтегазовой безопасности выявил следующие тенденции, обуславливающие актуальность возникновения спроса на вопросы нефтегазовой безопасности, к которым можно отнести:

- Растущий спрос на энергию и истощение энергетических ресурсов в последние годы заставили компании, а также правительства разработать планы мер по обеспечению безопасности в нефтегазовой отрасли.
- Увеличение расходов нефтяных и газовых компаний на безопасность сетевых и операционных технологий, а также растущая тенденция к управлению безопасностью и уязвимостями способствовали росту рынка нефтегазовой безопасности. Кроме того, растущая тенденция использования в отрасли собственных устройств (BYOD) создает дополнительные проблемы для инфраструктуры безопасности.
- Внедрение новых технологий значительно повышает эффективность, так как трубопроводные сети нефтяной и газовой промышленности простираются на

обширную территорию, и в условиях нынешнего конкурентного рынка экономически нецелесообразно использовать человеческие ресурсы для ее защиты. Это привело к спросу на систему цифрового экономического надзора с выполнением требований того, что продукты и компоненты оборудования, установленные в основной отрасли, должны соответствовать стандартам пожаробезопасности и взрывобезопасности.

- Мобильные веб-устройства наблюдения в таких сценариях обеспечивают удаленное наблюдение из централизованного или назначенного места и помогают оптимизировать безопасность. Стареющая инфраструктура подталкивает к необходимости наблюдения из соображений безопасности.
- Функции кибербезопасности, обеспечиваемые сетевой связью из-за простоты эксплуатации будут гибкими, но ожидается, что также несут с собой аспект уязвимости. Суровые погодные условия, экстремальные рабочие температуры, опасные процессы и т. д. делают рынок сложным, поскольку требуют соблюдения множества отраслевых стандартов и стандартов безопасности для продуктов, которые будут использоваться в отрасли, и влияют на рыночную среду. Все эти факторы имеют решающее значение для стимулирования спроса на кибербезопасность в течение прогнозируемого периода.

Конкурентная среда на рынке искусственного интеллекта на рынке нефти и газа сильно сконцентрирован из-за высоких первоначальных инвестиций. Одними из ключевых игроков на рынке безопасности являются Cisco, ABB, Microsoft и новые игроки с новыми разработками на рынке включают в себя:

- Корпорация Chevron, занимающаяся разведкой, добычей и транспортировкой сырой нефти и природного газа, повысила свою производительность благодаря облачным сервисам Microsoft, повышающим безопасность. Chevron создала безопасное современное цифровое рабочее место с Microsoft Office 365 и OneDrive для своих сотрудников по всему миру. На сегодняшний день Chevron сократила расходы на хранение, перенесла более 800 терабайт данных в OneDrive.

- Компания BP развернула Microsoft 365, чтобы улучшить взаимодействие с пользователем и безопасность. BP переносит свою рабочую среду на Microsoft 365 Enterprise E5, чтобы воспользоваться преимуществами платформенного подхода и защитить обширный цифровой периметр от кибератак.

Результаты и их обсуждение Нефтегазовая промышленность Узбекистана является одной из ведущих и перспективных направлений деятельности, так как обеспечивает не только поддержание роста экономики, но и позволяет сохранить энергетическую независимость: быть крупным поставщиком нефти, реализовывать проекты и привлекать иностранные инвестиции в имеющиеся активы.

Преимуществом является и геополитическое расположение - многие территории Узбекистана, в процентном соотношении около 60% от общего их числа, открыты и перспективны для добычи нефти и газа.

Поэтому Узбекистан богат углеводородным сырьем, так, нефть и газ считаются главными ресурсами для последующей переработки и производства топлива. За весь период проведения разведывательных работ в Узбекистане открыто более 246

месторождений нефти и газа. Нельзя не отметить и значительное влияние нефтегазового сектора на объем ВВП. Так, на нефтегазовую отрасль Узбекистана приходится около 16% ВВП страны, а в доходной части бюджета ее доля составляет более 20%.

Рынок нефтедобычи Узбекистана – достаточно высококонкурентный, поэтому здесь технологии Индустрии 4.0 начали применять одними из первых. Цифровые двойники месторождений, цифровое бурение, аналитика массивов Big Data, предиктивные модели – все это позволяет снизить издержки на разведку, добычу, переработку и повысить эффективность.

Рост цифровизации нефтегазовой отрасли Узбекистана, а также растущий спрос на энергию и истощение энергетических ресурсов сделал ее подверженной кибератакам, что заставило правительство и компании разработать меры по обеспечению безопасности в нефтегазовой отрасли.

Искусственный интеллект оказался эффективным вложением в нефтегазовую отрасль Узбекистана для улучшения различных процессов от диагностики котлов до фактического бурения. Такие приложения, как цифровой керн – это цифровые модели столбиков породы, которые извлекают из скважин в процессе геологоразведки, чтобы исследовать нефтеносный пласт, а также профилактическое обслуживание для восходящего, среднего и нисходящего потоков.

Кроме того, из-за сохранения опасений по поводу воздействия производства энергии на окружающую среду, нефтегазовые компании активно ищут инновационные подходы для достижения своих бизнес-целей при одновременном снижении воздействия на окружающую среду.

Рост цифровизации нефтегазовой отрасли сделал ее крупной мишенью для киберпреступников, так по статистике Kaspersky ICS CERT в нефтегазовом сегменте количество заблокированного вредоносного программного обеспечения увеличилось на 5.9 пунктов, что привело к таким последствиям как отказ в обслуживании, вредоносное программное обеспечение и фишинг (рис.2).

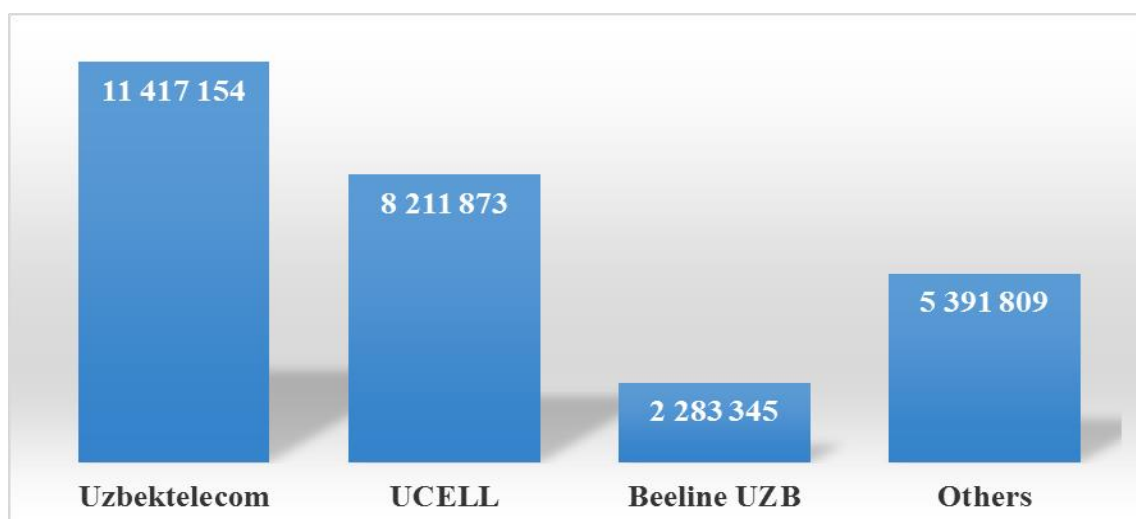


Рис. 2. - Меры кибербезопасности в разрезе операторов связи Узбекистана в 2024 году²

Растущий спрос на энергию и истощение энергетических ресурсов в последние годы выявило необходимость компаниям, а также правительству разработать ряд мер по обеспечению безопасности в нефтегазовой отрасли.

Заключение Система кибербезопасности рынке нефти и газа Узбекистана должна органично встраиваться в общую бизнес-стратегию предприятия и учитываться при модернизации производственных активов. Ее задача - не только минимизировать риски киберугроз, но и обеспечивать компаниям дополнительные преимущества: например, способствовать повышению производительности и безопасности техпроцессов.

Актуальным является то, чтобы специалисты, создающие систему кибербезопасности, были способны играть на опережение - предвидеть будущие угрозы и влиять на ход событий, - а не просто реагировали на действия киберпреступников, что предполагает использование новых методов обнаружения угроз и обмена информацией о них.

Важно помнить о влиянии человеческого фактора на успешность кибератак и проводить мероприятия для повышения бдительности и осведомленности в сфере кибербезопасности, а также обучение по противодействию атакам методами социальной инженерии.

В первую очередь, необходимо определить возможные события, которые недопустимы для функционирования этого бизнеса, и регулярно проводить верификацию таких событий на практике с помощью тестирования на проникновение или размещения цифровых двойников на киберполигонах.

Такой подход поможет выстроить систему комплексной защиты и мониторинга, которые не позволят злоумышленникам нанести ущерб организации и ее клиентам. Из-за тенденции к нарушению основной деятельности нефтегазовых компаний Узбекистана с помощью различного вредоносного программного обеспечения (шифровальщики, вайперы) решение о создании резервного копирования позволит быстро восстановиться, если атака все-таки достигла своей цели.

Как результат, нефтегазовым компаниям Узбекистана стоит изучить свои информационные активы, определить слабые места и возможные киберугрозы.

Список использованной литературы:

1. Application of machine learning and artificial intelligence in oil and gas industry / A. Sircar, K. Yadav, K. Rayavarapu [et al.] // Petroleum Research. – 2021. – Vol. 6, Issue 4. – P. 379–391. – DOI: 10.1016/j.ptlrs.2021.05.009

² www.honeywellprocess.com/en-US/news-and-events/Pages/pr-12062017-honeywell-survey-shows-low-adoption-of-industrial-cyber-security-measures.aspx

2. Koroteev D., Tekic Z. Artificial intelligence in oil and gas upstream: Trends, challenges, and scenarios for the future // Energy and AI. – 2021. – Vol. 3. – DOI: 10.1016/j.egyai.2020.100041
3. Applications of artificial intelligence in oil and gas development / Hong Li, Haiyang Yu, Nai Cao [et al.] // Archives of Computational Methods in Engineering. – 2020. – Vol. 28, Issue 3. – P. 937–949. – DOI: 10.1007/s11831-020-09402-8
4. www.honeywellprocess.com/en-US/news-and-events/Pages/pr-12062017-honeywell-survey-shows-low-adoption-of-industrial-cyber-security-measures.aspx

Copyright: © 2025 by the authors. This work is licensed under a Creative Commons Attribution-4.0 International License (CC - BY 4.0)

