

УДК 004.056

Романова Елена Юрьевна, доцент кафедры математических методов обеспечения безопасности систем факультета комплексной безопасности ТЭК, РГУ нефти и газа (НИУ) имени И.М. Губкина, г. Москва

Косинов Артем Александрович, студент, РГУ нефти и газа (НИУ) имени И.М. Губкина, г. Москва

Рулев Степан Анатольевич, студент, РГУ нефти и газа (НИУ) имени И.М. Губкина, г. Москва

Хабиров Денис Рустамович, студент, РГУ нефти и газа (НИУ) имени И.М. Губкина, г. Москва

Чесноков Степан Дмитриевич, студент, РГУ нефти и газа (НИУ) имени И.М. Губкина, г. Москва

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В АСПЕКТЕ КИБЕРБЕЗОПАСНОСТИ ТЭК: ОБЗОР

Аннотация

В статье приводится обзор новейших научных статей, рассматривающих различные современные информационные технологии, интегрированные в топливно-энергетический комплекс (ТЭК) в аспекте обеспечения кибербезопасности. В области топливно-энергетического комплекса разработка и понимание современных архитектур информационно-аналитических систем имеют критическое значение для противодействия кибератакам. Изучение новейших математических методов и моделей процессов ТЭК необходимо для совершенствования систем кибербезопасности данных и сетей. Изучение новейших разработок мониторинга передачи данных в производственных процессах ТЭК позволяет проводить анализ угроз и уязвимостей, разрабатывать систему кибербезопасности данных и сетей.

Annotation

This article provides a review of scientific papers examining various modern information technologies integrated into the fuel and energy complex (FEC) from a cybersecurity perspective. In the fuel and energy sector, the development and understanding of modern architectures for information and analytical systems are critical for countering cyberattacks. Studying the latest mathematical methods and models of FEC processes is essential for improving data and network cybersecurity systems. Studying the latest developments in data transmission monitoring in FEC production processes enables threat and vulnerability analysis and the development of data and network cybersecurity systems.

Ключевые слова: мониторинг ТЭК, мониторинг и информационная безопасность ТЭК, искусственный интеллект ТЭК, математическое моделирование ТЭК,.

Key words: monitoring of the fuel and energy sector, monitoring and information security oil and gas, artificial intelligence in the fuel and energy sector, mathematical modeling and monitoring in the fuel and energy sector.

Нефтегазовая отрасль в значительной степени опирается на информационно-технологические инновации. Интегрируя передовые аналитические инструменты и создавая комплексные структуры управления данными в правовом поле, организации могут эффективно снижать риски безопасности, обеспечить безопасность и целостность цифровых сред, улучшать протоколы кибербезопасности.

Анализ современных рисков и угроз в области информационной безопасности предприятий ТЭК проведен в [1]. Автор отмечает такие проблемы, как: недостаточное разделение сетей при современных тенденциях на микросегментации, концепции нулевого доверия; проблему «размывания» функций управления, что ведет к избыточным каналам связи с защищаемыми объектами; отечественные решения не всегда предоставляют набор функциональности, аналогичный конкурирующим иностранным вендорам

систем информационной защиты; предприятия ТЭК генерируют данные, нетипичные для многих средств защиты.

Интеграция традиционного математического моделирования и современных методов искусственного интеллекта представляет собой перспективный подход к снижению рисков и совершенствованию протоколов безопасности в нефтегазовой отрасли. Важнейшую роль занимает обеспечение информационной безопасности информационных баз, Интернета вещей, эксплуатационной эффективности предприятий ТЭК.

Важнейшая роль нефтегазовой отрасли в экономике делает ее подверженной растущим киберугрозам, нацеленным на критически важные операционные технологии и информационные системы. В обзоре [2] многосторонне рассматривается проблема кибербезопасности нефтегазовой отрасли. Выявлены критические уязвимости, оцениваются существующие меры кибербезопасности, Проблемы отрасли разделены на технологические, организационные и нормативные сегменты. Конвергенция информационных и операционных технологий создает сложный ландшафт кибербезопасности, их взаимосвязанность может приводить к каскадным эффектам из единой точки отказа, значительно усиливая потенциальное воздействие кибератак.

В организационном сегменте основное внимание уделяется культуре кибербезопасности, включая обеспечение соблюдения политики и обучение сотрудников. В технологическом сегменте отмечается, что устаревшие технологии (например, системы управления бурением, добычей и транспортировкой), которые изначально не были разработаны для противостояния текущим угрозам кибербезопасности являются проблемой обеспечения кибербезопасности. Также риски приносит интеграция Интернета вещей и облачных вычислений в существующую инфраструктуру отрасли.

Современный цифровой ландшафт переживает взрывной рост объёмов данных и эволюцию аналитических технологий. Это создаёт двойственный эффект: с одной стороны — колоссальные возможности для бизнеса, с другой

— принципиально новые угрозы для кибербезопасности. В эпоху больших данных кибербезопасность — это не просто технология, а стратегический актив. В [3] обосновывается необходимость совершенствования протоколов кибербезопасности для защиты конфиденциальной информации и обеспечения целостности цифровых инфраструктур. Подчеркивается, что интеграция технологий искусственного интеллекта в системы кибербезопасности требует комплексного и дальновидного подхода, решения проблем конфиденциальности данных, ошибок алгоритмов и потребности в квалифицированных специалистах по кибербезопасности.

В условиях постоянно меняющегося ландшафта киберугроз необходимы всеобъемлющие системы повышения устойчивости, обеспечение безопасности и целостности цифровой среды организаций. Авторы исследования [4] разработали комплексную и адаптивную систему снижения угроз, способную противостоять сложным киберугрозам. Ключевые рекомендации включают внедрение передовых технологий, непрерывное обучение, расширение обмена информацией об угрозах, внедрение многоуровневой стратегии защиты и проведение регулярных аудитов безопасности.

Управление рисками в контексте обеспечения кибербезопасности является темой многих исследований. Так, в [5] подытожен успешный опыт ПАО «Газпром» в управлении рисками.

Пространственные данные в режиме реального времени являются важнейшей частью систем управления активами и выполнения операций в нефтегазовой отрасли. Интеграция геоинформационных систем технологиями Интернета вещей (IoT), дистанционного зондирования, управления и сбора данных обеспечивает эффективность принятия управленческих решений, операционной эффективности и безопасности. В статье [6] рассматриваются теоретические основы применения пространственных данных в реальном времени в секторах ТЭК. Подчеркивается, что системы данных в реальном времени уязвимы для кибератак, что ставит под угрозу как непрерывность

работы, так и целостность данных. Кибератаки на системы реального времени вызывают нарушения работы, кражу конфиденциальной информации, нанесение экологического и финансового ущерба. Обеспечение безопасности этих систем требует надежных мер, таких как шифрование, многофакторная аутентификация и непрерывный мониторинг сети. Кроме того, необходима модернизация устаревших подсистем, не имеющих адекватные функции безопасности, децентрализованный характер систем данных в режиме реального времени также затрудняет внедрение единых протоколов кибербезопасности для всех компонентов. Устранение этих рисков требует проактивного подхода. Авторы предлагают использовать технологию блокчейн для решения проблем кибербезопасности. Определения и оценки типов, частоты и серьезности возникновения рисков, характерных для нефтегазового сектора Нигерии, способов управления ими в этом секторе являлись целью исследования [7]. Отмечается, что риски, связанные с этим бизнесом, сложны и дорогостоящи, поэтому эта отрасль избегает страхования, потенциальные страховые премии могут быть слишком высокими.

Важность исследования факторов, определяющих уровень энергетической безопасности России в условиях неустойчивой системы коммуникации между странами в мировом пространстве подчеркивается в [8]. Важным фактором работоспособности и безопасности энергосистемы становится защита энергетической инфраструктуры от киберугроз. Авторы предлагают следующий регламент оценки уровня энергетической безопасности: анализ уровня развития и защищенности информационных систем ТЭК; оценка разнообразия источников энергоснабжения; анализ уровня резерва и запасов энергоресурсов; оценка финансовой устойчивости; мониторинг политических и геополитических рисков.

Разработка и понимание современных архитектур информационно-аналитических систем ТЭК имеют критическое значение для противодействия кибератакам. Изучение новейших математических методов и моделей

процессов ТЭК необходимо для совершенствования систем обеспечения кибербезопасности как данных, так и сетей.

Обзор применений математических моделей в нефтегазовой отрасли приведен в работе [17]. Там же разработана математическая модель нефтяного месторождения, приведены примеры расчетов пластового давления при различных режимах добычи в заданных скважинах.

Управление производственными объектами оптимизируются с помощью стратегий оптимизации как на основе искусственного интеллекта, так и на основе традиционного математического моделирования. Анализ современных рисков и угроз в области информационной безопасности предприятий является актуальным направлением для обеспечения кибербезопасности предприятий ТЭК.

В исследовании [10] рассмотрено современное промышленное применение экспертных систем, обсуждены возможности экспертных систем в таких областях, как оценка рисков, анализ решений, промышленная классификация и диагностика неисправностей. В целом, исследование выявило актуальность и важность интеграции экспертных систем в промышленную автоматизацию.

Однако для достижения интеграции необходимо решить ряд вопросов: проблемы качества данных, кибербезопасности и необходимость обучения сотрудников новым навыкам. В статье [11] обсуждаются возможности, преимущества, проблемы и перспективы прогнозной аналитики и генеративного искусственного интеллекта в нефтегазовой отрасли. а также их возможности для изменений и создания ценности. Модели генеративного искусственного интеллекта имитируют реальные сценарии эксплуатации скважин, что позволяет выявить оптимальную стратегию бурения, добычи и технического обслуживания, повышая тем самым эффективность и безопасность эксплуатации.

В статье [12] рассматриваются преобразования нефтегазовой отрасли в связи с использованием методов искусственного интеллекта и машинного

обучения для разведки, оптимизации размещения скважин на анализе исторических геологических данных и данных в режиме реального времени. Кроме того, с помощью стратегий на основе искусственного интеллекта оптимизируются управление запасами, добыча углеводородов и энергоэффективность. К перспективным направлениям применения методов искусственного интеллекта в нефтегазовой отрасли авторы относят: передовые автономные системы (буровые установки, грузовики, роботизированные инспекционные комплексы и дроны для мониторинга и сбора данных в режиме реального времени); цифровые двойники и моделирование физических активов; интеграцию с блокчейном для повышения безопасности данных, прозрачность и прослеживаемость в нефтегазовом секторе; управление разработкой месторождений нового поколения благодаря методам геологического моделирования и аналитике данных в режиме реального времени; совершенствование моделирования месторождений, оптимизации операций по повышению нефтеотдачи и эффективному управлению сложными месторождениями; усовершенствования в области мониторинга окружающей среды и безопасности.

Как технологии искусственного интеллекта трансформируют сектор управления нефтегазовыми проектами рассматривается в [13].

Авторы отмечают преимущества новых технологий в процессе принятия решений с помощью предиктивной аналитики и динамического планирования проектов. Отмечают и сложности, так как для эффективной работы требуются точные входные данные, регулярное обновление, зависимость от технологий и обеспечения конфиденциальности и безопасности данных.

В статье [14] для оптимизации процессов улавливания и хранения углеводородов в нефтегазовой отрасли предлагается концепция, объединяющая методы обработки данных с геологической информацией. Для определения оптимальных геологических формаций хранения, обнаружения месторождений, прогнозирования выбросов и их влияния на окружающую

среду применяются алгоритмы машинного обучения, анализ геопространственных данных и прогнозное моделирование. , исследование направлено на определение.

Концепции предиктивной аналитики и прогнозного технического обслуживания на основе методов искусственного интеллекта посвящена работа [15]. Анализ данных, собранных с различных датчиков и оборудования, согласно этой методике применяется для прогнозирования возможных неисправностей оборудования, позволяют выявлять проблемы на ранних стадиях, что позволяет принять меры до возникновения сбоя. Точность моделей машинного обучения повышается за счет взаимодействия с устройствами Интернета вещей для предоставления данных в режиме реального времени и непрерывного мониторинга.

В области топливно-энергетического комплекса цифровые технологии мониторинга технического состояния производственных объектов с применением методов искусственного интеллекта могут быть подвергнуты кибератакам. Изучение новейших разработок мониторинга позволяет проводить анализ угроз и уязвимостей, разрабатывать систему кибербезопасности данных и сетей.

В [16] приведен обзор методов обнаружения утечек из нефте- и газопроводов. Методы подразделены на три категории в зависимости от их технических характеристик: аппаратные, программные и интеллектуальные. Отмечаются важность исследований уязвимости и надежности каналов беспроводной связи между координатором сети и узлами датчиков.

Статья [17] посвящена аспектам цифровизации с целью обеспечения надежной эксплуатации оборудования и систем магистральной транспортировки газа. Приводятся примеры разработки цифровых моделей систем транспортировки газа.

Статья [18] посвящена системе автоматизированного непрерывного мониторинга и контроля безопасности газовоздушной среды и параметров временных герметизирующих устройств при проведении работ на линейной

части магистрального газопровода. Изучение новейших разработок мониторинга передачи данных в производственных процессах ТЭК позволяет проводить анализ угроз и уязвимостей, разрабатывать систему кибербезопасности данных и сетей.

Предприятия ТЭК в значительной степени опираются на ИТ-инновации при управления бизнес-процессами, что требует обработки больших объемов данных, получением ценной информации и принятием своевременных решений на ее основе. Так как принятие решений на основе больших данных требует глубокого понимания контекстуальных факторов, влияющих на эти решения, ряд работ проводят соответствующие исследования. В работе [19] авторами из Омара факторы рассматриваются с использованием новой концепции "Технология-организация-среда", в которой представлены технологические, организационные и экологические факторы. Двадцать факторов были сгруппированы в три: качество данных, профессионализм сотрудников и организационные стратегии, из которых первый признан самым важным.

Изучение новейших разработок мониторинга технического состояния производственных объектов и управление рисками позволяет проводить анализ угроз и уязвимостей, разрабатывать систему кибербезопасности данных и сетей.

Изучение причин аварий и оценки типов рисков и уязвимостей, присутствующих в нефтегазовом секторе важны для построения информационных систем мониторинга и защиты данных и сетей, выявления возможных направлений атак. Обеспечение информационной безопасности данных и систем управления рисками ТЭК является важной составляющей обеспечения кибербезопасности.

Быстро меняющийся ландшафт киберугроз должен быть обеспечен надежными и адаптирующимися к динамичному характеру проблем цифровой безопасности стратегиями защиты сетей. В [20] предложена методика разработки комплексной системы предотвращения угроз, объединяющей

передовые методологии в области кибербезопасности, управления рисками и анализа угроз. Предлагаемый многоуровневый механизм защиты объединяет информацию об угрозах в режиме реального времени со сложными стратегиями реагирования на инциденты, предлагает упреждающие и реактивные меры. Важными элементами платформы являются системы обнаружения аномалий, обучение сотрудников и непрерывные мониторинг безопасности.

Математическое моделирование в нефтегазовой отрасли позволяет анализировать и прогнозировать возникновение и развитие опасных как производственных, так и информационно-технологических событий, явлений и процессов.

Так в работе [21] на основе дифференциальных уравнений диффузии и теплопереноса построена математическая модель определения кольцевого давления в газовых гибких трубах большой протяженности.

В статье [22] рассматриваются объективные качественные и количественные показатели, характеризующие состояние охраны труда и безопасность нефтепереработки. Подчеркивается, что важным аспектом является выявление, анализ и контроль рисков, включая информационно-технологические крупномасштабных аварий. Поэтому необходимо внедрять меры контроля и сертифицировать все возможные риски в проектной документации для их предотвращения.

Нефтегазовая отрасль характеризуется высокой сложностью производимых работ. Возможные аварии представляют значительный риск для жизни людей, экономической стабильности и окружающей среды. Поэтому решающее значение имеет анализ и предотвращение аварий. В [23] на основе вторичных данных Международной ассоциации производителей нефти и газа (IOGP) исследованы причины аварий и инцидентов на нефтяных и газовых скважинах, вызванные человеческим фактором: ненадлежащий надзор, неадекватная оценка рисков, неадекватные рабочие процедуры, недостаточная квалификация, неисправная система оповещения и

недостаточная информированность. Проанализировано, как методы искусственного интеллекта используются в этом секторе для снижения рисков и совершенствования протоколов безопасности в нефтегазовой отрасли.

Список литературы

1. Силантьев А. О. Особенности информационной безопасности в нефтедобывающих компаниях: аспект импортозамещения // Молодой ученый. 2024. № 37(536). С. 9-12.
2. Pothana Prasad, Ramaseri-Chandra Ananth, Gokapai Vasanth Cybersecurity in the oil and gas sector: vulnerabilities, solutions, and future directions // 2024 Cyber Awareness and Research Symposium (CARS), Grand Forks, ND, USA. 2024. PP. 1-7
3. L. K. Nwobodo, Ch. S. Nwaimo, A. E. Adegbola Enhancing cybersecurity protocols in the era of big data and advanced analytics // GSC Advanced Research and Reviews. 2024. 19(03). PP. 203–214.
4. H. Balisane, Eh. Egho-Promise, E. Lyada, F. Aina Towards improved threat mitigation in digital environments: a comprehensive framework for cybersecurity enhancement // International Journal of Research - GRANTHAALAYAH May 2024 12(5), PP. 108–123.
5. Дроздова Д.В. Управление рисками в рамках обеспечения кибербезопасности предприятий ТЭК // Теория и практика современной науки. 2024. №7 (109)
6. Kirti Vasdev Real-time spatial data in oil and gas asset management and operations // Journal of Oil, Petroleum and Natural Gas Research, December 24, 2024
7. Asika, Kenneth-Rex Chibuzor, Udo-Orji, Chidinma Okatta, Aloysius Uzoma Risk management in the oil and gas sector, analytical discourse: a case of Shell Petroleum Development (SPDC) Company Nigeria // International Journal of Operational Research in Management, Social Sciences & Education Volume 10 Number 2 November, 2024.

8. Кулагина Н А., Голованова Н Б., Графов Ю Г. Диагностика национальной и экономической безопасности в энергетическом секторе России в условиях цифровых трансформаций на основе аналитической обработки информационных массивов сведений // Вестник Академии знаний. 2024. №2 (61).
9. Новожилов И. М., Шишкина А. В. Математическое моделирование при разработке нефтяного месторождения // Конференция: XXVII Международная конференция по мягким вычислениям и измерениям (SCM'2024) 22-24 мая. 2024. Санкт-Петербург, СПбГЭТУ «ЛЭТИ».
10. Xianzhe Yang, Changsheng Zhu Industrial expert systems review: a comprehensive analysis of typical applications // IEEE Access, July 2024.
11. Sridevi Kakolu, Muhammad Ashraf Faheem Predictive analytics and generative ai in oil & gas: transforming wellbore stability and hazard detection // Iconic research and engineering journals. Volume 8 Issue 1. PP. 635-649.
12. Ganesh Shankar Gowekar How oil and gas industry are transforming with ai and ml // World Journal of Advanced Research and Reviews, 2024, 23(03). PP. 1234–1238.
13. Ali F. AlShehab, Mustafa S. AlSaigh The integration of artificial intelligence in the oil and gas project management sector // International Journal of Management and Commerce Innovations Vol. 12, Issue 1, PP: 196-199.
14. Wags Numoipiri Digitemie, Ifeanyi Onyedika Ekemezie Enhancing carbon capture and storage efficiency in the oil and gas sector: an integrated data science and geological approach // Engineering Science & Technology Journal Volume 5, Issue 3, PP. 924-934.
15. Ganesh Shankar Gowekar Artificial intelligence for predictive maintenance in oil and gas operations // World Journal of Advanced Research and Reviews, 2024, 23(03). PP. 1228–1233.
16. Sumayh S. Aljameel, Dina A. Alabbad, Dorieh Alomari, Razan Alzannan, Shatha Alismail, Fatimah Aljubran, Atta-ur Rahman Oil and gas pipelines leakage detection approaches: a systematic review of literature // International

Journal of Safety and Security Engineering Vol. 14, No. 3, June, 2024. PP. 773-786.

17. Лучкин Н. А., Земенкова М. Ю., Квасов И. Н. Сквозные цифровые технологии для обеспечения надежности и безопасности систем магистрального транспорта газа // Тюменский научный журнал. 2024. №2
18. Яхина Э. Н., Шарафутдинова Г. М. Автоматизированная система контроля загазованности и параметров временных герметизирующих устройств на магистральных газопроводах // Сетевое издание «Нефтегазовое дело». 2024. № 2. С. 130–140.
19. Abir S. Al-Harrasi, Haitham Y. Adarbah, Ali Al-Badi, Abdul K. Shaikh, Hafidh Al-Shihi, Alyaa Al-Barrak Exploring the adoption of big data analytics in the oil and gas industry: a case study // Journal of Business, Communication & Technology, 3(2), PP. 1-16.
20. Halima Kure, Abimbola Sangodoyin, Folayo Aina, Emmanuel Lyada The effectiveness of a comprehensive threat mitigation framework in networking: a multi-layered approach to cyber security // International Research Journal of Computer Science, Volume 11, Issue 5. 2024. PP. 529-538.
21. Xiang-An Lu, Liang-Liang Jiang, Jian-Sheng Zhang, Min-Gui Wang Securing offshore resources development: a mathematical investigation into gas leakage in long-distance flexible pipes // Petroleum Science Volume 21, Issue 4, August. 2024. PP. 2734-2744.
22. Bogopolsky V. O., Bagirov A. A., Shirinov M. M. Assessment of operational risks in the oil and gas industry // Nafta-Gaz. 2024. No. 8. PP. 520–525.
23. Asharul Khan, Majid Al Busafi, Amjed Al Thuhli, Sajjad Siddiqui Accident and incident analysis in the oil and gas sector using artificial intelligence and machine learning // The 15th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2024) October 28-30, 2024, Leuven, Belgium.

References

1. Silantyev A. O. Features of information security in oil producing companies: an aspect of import substitution // Young scientist. 2024. No. 37 (536). P. 9-12.
2. Pothana Prasad, Ramaseri-Chandra Ananth, Gokapai Vasanth Cybersecurity in the oil and gas sector: vulnerabilities, solutions, and future directions // 2024 Cyber Awareness and Research Symposium (CARS), Grand Forks, ND, USA. 2024. PP. 1-7
3. L. K. Nwobodo, Ch. S. Nwaimo, A. E. Adegbola Enhancing cybersecurity protocols in the era of big data and advanced analytics // GSC Advanced Research and Reviews. 2024. 19(03). PP. 203–214.
4. H. Balisane, Eh. Egho-Promise, E. Lyada, F. Aina Towards improved threat mitigation in digital environments: a comprehensive framework for cybersecurity enhancement // International Journal of Research - GRANTHAALAYAH May 2024 12(5), PP. 108–123.
5. Drozdova D.V. Risk management in the framework of ensuring cybersecurity of fuel and energy complex enterprises // Theory and practice of modern science. 2024. No. 7 (109)
6. Kirti Vasdev Real-time spatial data in oil and gas asset management and operations // Journal of Oil, Petroleum and Natural Gas Research, December 24, 2024
7. Asika, Kenneth-Rex Chibuzor, Udo-Orji, Chidinma Okatta, Aloysius Uzoma Risk management in the oil and gas sector, analytical discourse: a case of Shell Petroleum Development (SPDC) Company Nigeria // International Journal of Operational Research in Management, Social Sciences & Education Volume 10 Number 2 November, 2024.
8. Kulagina N. A., Golovanova N. B., Grafov Yu. G. Diagnostics of national and economic security in the energy sector of Russia in the context of digital transformations based on analytical processing of information arrays // Bulletin of the Academy of Knowledge. 2024. No. 2 (61).

9. Novozhilov I. M., Shishkina A. V. Mathematical modeling in the development of an oil field // Conference: XXVII International Conference on Soft Computing and Measurements (SCM'2024) May 22-24, 2024. St. Petersburg, ETU "LETI".
10. Xianzhe Yang, Changsheng Zhu Industrial expert systems review: a comprehensive analysis of typical applications // IEEE Access, July 2024.
11. Sridevi Kakolu, Muhammad Ashraf Faheem Predictive analytics and generative ai in oil & gas: transforming wellbore stability and hazard detection // Iconic research and engineering journals. Volume 8 Issue 1. PP. 635-649.
12. Ganesh Shankar Gowekar How oil and gas industry are transforming with ai and ml // World Journal of Advanced Research and Reviews, 2024, 23(03). PP. 1234–1238.
13. Ali F. AlShehab, Mustafa S. AlSaigh The integration of artificial intelligence in the oil and gas project management sector // International Journal of Management and Commerce Innovations Vol. 12, Issue 1, PP: 196-199.
14. Wags Numoipiri DigiTemie, Ifeanyi Onyedika Ekemezie Enhancing carbon capture and storage efficiency in the oil and gas sector: an integrated data science and geological approach // Engineering Science & Technology Journal Volume 5, Issue 3, PP. 924-934.
15. Ganesh Shankar Gowekar Artificial intelligence for predictive maintenance in oil and gas operations // World Journal of Advanced Research and Reviews, 2024, 23(03). PP. 1228–1233.
16. Sumayh S. Aljameel, Dina A. Alabbad, Dorieh Alomari, Razan Alzannan, Shatha Alismail, Fatimah Aljubran, Atta-ur Rahman Oil and gas pipelines leakage detection approaches: a systematic review of literature // International Journal of Safety and Security Engineering Vol. 14, No. 3, June, 2024. PP. 773-786.

17. Luchkin N. A., Zemenkova M. Yu., Kvasov I. N. End-to-end digital technologies for ensuring the reliability and safety of gas main transportation systems // Tyumen Scientific Journal. 2024. No. 2.
18. Yakhina E. N., Sharafutdinova G. M. Automated system for monitoring gas contamination and parameters of temporary sealing devices on main gas pipelines // Online publication "Oil and Gas Business". 2024. No. 2. P. 130–140.
19. Abir S. Al-Harrasi, Haitham Y. Adarbah, Ali Al-Badi, Abdul K. Shaikh, Hafidh Al-Shihi, Alyaa Al-Barrak Exploring the adoption of big data analytics in the oil and gas industry: a case study // Journal of Business, Communication & Technology, 3(2), PP. 1-16.
20. Halima Kure, Abimbola Sangodoyin, Folayo Aina, Emmanuel Lyada The effectiveness of a comprehensive threat mitigation framework in networking: a multi-layered approach to cyber security // International Research Journal of Computer Science, Volume 11, Issue 5. 2024. PP. 529-538.
21. Xiang-An Lu, Liang-Liang Jiang, Jian-Sheng Zhang, Min-Gui Wang Securing offshore resources development: a mathematical investigation into gas leakage in long-distance flexible pipes // Petroleum Science Volume 21, Issue 4, August. 2024. PP. 2734-2744.
22. Bogopolsky V. O., Bagirov A. A., Shirinov M. M. Assessment of operational risks in the oil and gas industry // Nafta-Gaz. 2024. No. 8. PP. 520–525.
23. Asharul Khan, Majid Al Busafi, Amjed Al Thuhli, Sajjad Siddiqui Accident and incident analysis in the oil and gas sector using artificial intelligence and machine learning // The 15th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2024) October 28-30, 2024, Leuven, Belgium.