Научная статья
УДК 327.7
DOI: 10.20323/2658-428X-2025-2-27-59
EDN: LUMJEZ

# Направления интеграции инструментов OSINT в процессы обеспечения безопасности предприятий нефтегазового сектора

**Дмитрий Андреевич Медведев[1], Анастасия Евгеньевна Малых[2]✉**
[1]Кандидат политических наук, заведующий кафедрой (базовой) международного сотрудничества в сфере обеспечения безопасности, Российский государственный университет нефти и газа (НИУ) имени И. М. Губкина, г. Москва.
[2]Инженер Управления стратегического развития, Российский государственный университет нефти и газа (НИУ) имени И. М. Губкина, г. Москва
[1]Medvedev.d@gubkin.ru, https://orcid.org/0000-0002-8275-5188
[2]malykh.anastasia@mail.ru✉, https://orcid.org/0009-0001-3928-3445

***Аннотация.*** В статье представлен теоретический анализ роли OSINT (Open Source Intelligence или разведка по открытым источникам данных) как инструмента конкурентной разведки в сфере обеспечения комплексной безопасности нефтегазового предприятия с использованием научно-исследовательских данных российских и зарубежных ученых, аналитических и статистических материалов в отношении использования конкурентной разведки по открытым источникам с целью обеспечения защищенности объектов нефтегазовых предприятий от различных видов угроз. Актуальность исследования обуславливается геополитической напряженностью, недружественными действиями отдельных государств, включающих в себя беспрецедентное санкционное давление, напрямую влияющее на экономическую безопасность российских стратегически значимых компаний, а также рисками терроризма и диверсии в отношении критически важных объектов нефтегазового комплекса – нефтедобывающих и нефтеперерабатывающих предприятий, морских нефтегазовых скважин, магистральных газо- и нефтепродуктопроводов и т. д. На основании литературного обзора авторами было проведено исследование основных видов безопасности на нефтегазовых предприятиях, в рамках которых используются OSINT-данные, методологии OSINT и практических примеров использования данного инструментария. Кроме того, был проведен анализ значения OSINT при внедрении цифровых технологий, анализа уязвимостей критической информационной инфраструктуры и прогнозирования активности злоумышленников при угрозе физической и информационной безопасности объектов нефтегазового комплекса. Авторами были определены направления интеграции OSINT в сферу обеспечения защищенности объектов нефтегазового сектора и потенциал применения данного инструмента с целью мониторинга геополитических факторов обеспечения безопасности рассматриваемых объектов.

***Ключевые слова:*** OSINT; комплексная безопасность; нефтегазовая отрасль; конкурентная разведка; критически важные объекты; геополитика; международное сотрудничество

***Для цитирования:*** Медведев Д. А., Малых А. Е. Направления интеграции инструментов OSINT в процессы обеспечения безопасности предприятий нефтегазового сектора // Социально-политические исследования. 2025. № 2 (27). С. 59–74. http://dx.doi.org/10.20323/2658-428X-2025-2-27-59. https://elibrary.ru/LUMJEZ.

Original article

## Directions of OSINT tools integration into oil and gas sector security processes

**Dmitriy A. Medvedev[1], Anastasia E. Malykh[2]✉**

[1]Candidate of political sciences, head of department of (basic) international cooperation in the field of security, Gubkin Russian state university of oil and gas (NRU), Moscow.
[2]Engineer, Strategic development department, Gubkin Russian state university of oil and gas (NRU), Moscow
[1]Medvedev.d@gubkin.ru, https://orcid.org/0000-0002-8275-5188
[2]malykh.anastasia@mail.ru✉, https://orcid.org/0009-0001-3928-3445

***Abstract.*** The article presents a theoretical analysis of the role of OSINT (Open Source Intelligence) as a tool for competitive exploration in the field of ensuring the integrated security of an oil and gas enterprise using research data from russian and foreign scientists, analytical and statistical materials regarding the use of competitive exploration from open sources in order to ensure the protection of oil and gas facilities from various types of threats. The relevance of the study is determined by geopolitical tensions, unfriendly actions of individual states, including unprecedented sanctions pressure that directly affects the economic security of russian strategically important companies, as well as the risks of terrorism and sabotage in relation to critical oil and gas facilities – oil producers and refineries, offshore oil and gas wells, gas and oil product trunk pipelines, etc. Based on the literature review, the authors conducted a study of the main types of safety at oil and gas enterprises, which use OSINT data, OSINT methodologies and practical examples of the use of this tool. In addition, an analysis of the value of OSINT in the introduction of digital technologies, an analysis of vulnerabilities in critical information infrastructure and forecasting the activity of criminals in the event of a threat to the physical and information security of oil and gas facilities was carried out. The authors identified areas of OSINT integration in the sphere of ensuring the security of oil and gas facilities and the potential for using this tool in order to monitor geopolitical factors to ensure the safety of the facilities under consideration.

***Key words:*** OSINT; integrated security; oil and gas industry; competitive intelligence; critical facilities; geopolitics; international cooperation

***For citation***: Medvedev D. A., Malykh A. E. Directions of OSINT tools integration into oil and gas sector security processes. *Social and political researches*. 2025;2(27): 59–74. (In Russ). http://dx.doi.org/10.20323/2658-428X-2025-2-27-59. https://elibrary.ru/LUMJEZ.

## Введение

В контексте обеспечения технологического суверенитета основой развития топливно-энергетического комплекса будет являться инновационное развитие традиционных отраслей ТЭК: нефтегазовой отрасли, электроэнергетики, угольной и горно-обогатительной отрасли при создании и внедрении технологий на основании научно-технологических разработок и фундаментальных исследований [Жданеев, 2022]. Среди достижений нефтегазовой отрасли за последние годы ученые выделяют цифровизацию и автоматизацию процессов добычи и переработки нефти и газа, результатом которых является оптимизация процессов добычи углеводородов и значительное снижение эксплуатационных затрат. При этом отмечается, что компании нефтегазового сектора, обладающие суверенитетом в сфере технологической независимости, менее уязвимы к внешним воздействиям политического и экономического характера [Горбашко, 2024; Волошин, 2023].

Так, одним из важнейших вопросов развития нефтегазовой отрасли является обеспечение устойчивого функционирования и комплексной безопасности предприятий, включая надежность топливо- и энергоснабжения, комплексную автоматизацию процессов и ИТ-системы с целью предотвращения наступления нежелательных событий на опасных производственных объектах [Подготовка к обеспечению … , 2021], безопасность на объектах критической инфраструктуры.

Активное развитие и популяризация аналитических инструментов, позволяющих собирать, структурировать и использовать данные из открытых источников в интернете привели к интеграции методов «разведки по открытым источникам» (*анг. open source intelligence, далее – OSINT*) в деятельности многих компаний частного сектора.

Отметим, что, как правило, *к инструментарию OSINT относится следующее:*

– структурирование индексируемой поисковыми ресурсами информации и использование специальных запросов, использование специализированных каталогов и поисковых систем, веб-скрейпинг открытой информации в интернете (не относящейся к персональным данным пользователей);

– поиск по фото- и видеоизображениям (IMINT), включая реверсивный (обратный) поиск, выявление и проверка метаданных файлов, оценка достоверности цифровых изображений;

– сбор и анализ геопространственной информации на основе изображений и иных данных

(GEOINT), работа со специальными базами картографической информации (например, Openstreetmap);

– сбор и систематизация открытой информации в социальных сетях, блогах, форумах, а также визуализация связей, построение социальных графов;

– использование веб-архивов, а также кэшированных данных веб-страниц, доступных в интернете;

– средства анализа доменов и IP-адресов;

– иные способы сбора и анализа информации из открытых источников.

Указанные методы стали внедряться и в процессы управления и обеспечения защиты промышленных предприятий по всему миру [Шармаев, 2022]. Вместе с этим динамичность внедренческих процессов происходит на фоне отсутствия однозначного толкования термина, а также определения совокупности инструментов, которые составляют методическую базу разведки по открытым источникам.

На текущий момент на международном уровне за OSINT не закреплена однозначная дефиниция, а применение инструментария OSINT не обеспечивается международной договорной базой. В ряде документов Организации Объединенных Наций упоминается термин, технически трактовка которого воспринимается как «сбор и анализ общедоступных данных из различных источников для проведения расследований» [Организация Объединенных Наций]. К таким источникам относятся веб-сайты, социальные сети, онлайн-базы данных, сайты электронной коммерции, блоги, форумы, платформы для обмена сообщениями, правительственные порталы и даже даркнет.

На национальном уровне лишь в некоторых странах приняты регламентирующие документы, например, в США опубликована Стратегия OSINT на период с 2024 по 2026 гг. При этом данная Стратегия рассматривает OSINT с позиции разведывательных данных, полученных исключительно на основе общедоступной или коммерческой информации, которая затрагивает определенные приоритеты, требования или пробелы в разведывательных данных [The IC OSINT … ].

Тем не менее, в соответствии с докладом экспертов американского центра RAND, опубликованным в 2025 году, OSINT постепенно становится основным инструментом современной аналитики, системной методологией, подразумевающей под собой, в том числе технологии вероятностного прогнозирования с учетом коллективного опыта [Доклад RAND … ]. Отмечается, что вероятностное краудсорсинговое прогнозирование может компенсировать пробелы в сборе данных, дополняя традиционные методы сбора разведывательной информации. Кроме того, объем разведывательных данных к получению доступа по применению инструментария OSINT не поименован, что позволяет сделать вывод о расширительном толковании сфер использования таких данных для цели обеспечения безопасности как

предприятий, так и в целом государств.

**Методы исследования**

В ходе исследования был проведен комплексный анализ международного опыта использования инструментов OSINT для защиты предприятий нефтегазового комплекса от различных видов информационных угроз. В рамках системной методологии была выявлена роль OSINT в рамках обеспечения экономической и финансовой, информационной и кадровой безопасности, а также физической защищенности объектов нефтегазовых предприятий и социально- и международно-политических условий функционирования данных объектов. Для определения основных направлений использования анализа данных по открытым источникам были проведены интервью с представителями компаний, использующих OSINT в целях обеспечения комплексной безопасности предприятий. Также структурно-функциональный анализ использовался для определения интеграции OSINT в стратегии безопасности объектов нефтегазовой отрасли и защиты от киберугроз.

**Результаты исследования**

На сегодняшний день в рамках информационно-аналитического обеспечения защищенности нефтегазовых предприятий инструменты OSINT могут применяться разнообразно.

Как показывает анализ практической деятельности, основные направления обеспечения безопасности, в которых используются методы OSINT на предприятиях:

– экономическая и финансовая безопасность организации (в этом случае инструменты дополняются специальными средствами, например, отслеживание криптовалютных операций);

– информационная безопасность и защищенность информационных систем организации;

– кадровая безопасность и риски, связанные с неблагонадежностью сотрудников;

– социально-политические и международно-политические условия функционирования предприятия (особенно в условиях односторонних рестрикций, применяемых к российский нефтегазовым предприятия);

– физическая защищенность объектов.

Практические примеры внедрения в систему комплексной безопасности OSINT для снижения кадровых рисков касаются, как правило, верификации информации о потенциальных кандидатах на вакантные должности, однако дополняются возможностями анализа деятельности сотрудников для снижения рисков инсайдерских атак.

В рамках противодействия физическим угрозам предприятий могут быть использованы методы OSINT, касающиеся обеспечения анализа геоданных и анализа социальных сетей [Медведев, 2025]. В частности, в рамках анализа уязвимостей конкретного предприятия информация из открытых источни-

ков геопространственных данных позволяет оценить потенциальные угрозы, составить перечень рисков, связанных с потенциальными сценариями нападения на предприятие.

Инструментарий OSINT в отношении социальных сетей ориентирован на сбор и систематизацию данных о цифровом следе, который представляет собой уникальный набор отслеживаемых цифровых действий, коммуникаций, сохраняющихся в интернет или на цифровых устройствах. В более широком смысле, данные цифрового следа включают свидетельства о любой активности пользователей. Так, цифровой след включает в себя не только непосредственно записи о действиях, но и свидетельства о любой активности, например, геоданные.

В свою очередь, экономическая составляющая безопасности предприятия усиливается с помощью OSINT-инструментов за счет применения разведки по открытым источникам для проверки надежности контрагента или выявления научно-технической политики конкурентов [Елкина, 2021]. Например, Управление по финансовому регулированию и надзору Великобритании в своем Руководстве по борьбе с финансовыми преступлениями утверждает, что финансовые организации должны интегрировать OSINT в рабочие процессы EDD, используя его проверки из открытых источников в интернете в дополнение к коммерчески доступным базам данных [Blackdot Solutions … ].

По данным экспертов, в качестве операторов OSINT-данных выступают государственные органы и негосударственные организации, международные акторы, бизнес-корпорации и преступные организации [Янгаева, 2022].

Также в связи с внедрением инновационных цифровых технологий на объектах нефтегазовой отрасли, одним из наиболее актуальных вопросов остается безопасность цифровой инфраструктуры [Трофимов, 2023]. Уязвимость критической информационной инфраструктуры к информационным угрозам порождает необходимость совершенствования подходов к обеспечению информационной безопасности [Ярош, 2020].

В отношении информационных угроз инструментарий OSINT, в частности инструмент Shodan, позволяет оперативно выявлять подключенные к интернету устройства SCADA-систем, анализировать их уязвимости и мониторить активность потенциальных злоумышленников. Интеграция данных OSINT в математические модели, такие как процесс Хокса, позволяет уточнить интенсивность киберугроз и повысить точность прогнозирования атак. Применение таких подходов способствует переходу к адаптивным моделям управления безопасностью, способным учитывать временные характеристики угроз и оперативно реагировать на их изменения [Самарин, 2022].

Еще одно возможное применение средств разведки по открытым источникам в сфере информацион-

ной безопасности предприятия – сбор и синтез фрагментов похищенных данных. Злоумышленники часто размещают часть утекших данных в качестве демонстрации наличия потери информациии организацией. Как отмечает OSINT-специалист Д. Мередит, «используя средства разведки по открытым источникам, специалисты по кибербезопасности выявляют и анализируют фрагменты похищенных данных, чтобы определить масштабы и характер взлома» [Мередит, 2025].

Инструменты разведки по открытым источникам могут также быть использованы для верификации информации, разоблачения фейковых сообщений, искаженных изображений, целью которых является введение сотрудников или руководства организации в заблуждение. Инструменты OSINT, такие как theHarvester, используются для отслеживания фишинговых атак до их реализации против организации [Мередит, 2025]. Другой способ верификации информации, в частности, изображений, используемых в разведке по открытым источникам – реверсивный поиск, позволяющий обнаружить, когда и где ранее в интернете данное изображение использовалось и как оно выглядело изначально.

По данным экспертов процесс анализа данных разведки по открытым источникам составляет, как правило, следующий аналитический цикл:

1) определение целей разведывательной деятельности;

2) определение соответствующих инструментов и осуществление сбора открытых данных;

3) обработка и фильтрация собранных данных исходя из целей деятельности;

4) анализ и структуризация информации, выявление связей, проверка гипотез, верификация данных;

5) обзор результатов;

6) отчетность и обратная связь [Rajamäki & Tiitta, 2024].

При этом критически важным аспектом этапа сбора данных является применение специализированного инструментария OSINT. Отмечается высокая эффективность таких инструментов, как Maltego (для визуализации связей и автоматизированного сбора данных из различных типов источников) и SpiderFoot (для автоматического сканирования и агрегации информации о доменах, IP-адресах, почтовых серверах и т. д.). Дополнением к ним служат общедоступные ресурсы, такие как поисковые системы для обнаружения индексируемой технической информации и данных о сотрудниках, а также геосервисы для анализа инфраструктуры организации.

Исследование экспертов позволяет сделать вывод об эффективности внедрения и интеграции OSINT в систему Cyber Threat Intelligence (CTI) компании при обеспечении перехода от реактивной к проактивной модели безопасности [Палеев, 2022; Перов, 2024]. Кроме того, такая система представляет

собой основу мониторинга угроз деятельности организации, включая выявление уязвимостей (например, случайно опубликованных конфиденциальных данных, информации об устаревшем ПО) до их получения злоумышленниками. Также в рамках данной интеграции, представляется возможным моделировать сценарии реализации киберугроз (“Red Teaming”), используя те же источники и инструменты OSINT (такие как Maltego и SpiderFoot для анализа цифровых следов сотрудников), которые доступны киберпреступникам для подготовки целевых фишинговых атак или атак социальной инженерии. Выявление этих данных силами самой организации позволяет своевременно принимать меры по работе с уязвимостями и повышать осведомленность персонала.

Важно отметить, что внедрение формализованного процесса OSINT с использованием специализированного инструментария является критически важным элементом для усиления киберустойчивости организаций вне зависимости от направления основной деятельности. Оно способствует проактивному управлению угрозами, снижению операционных и репутационных рисков, а также укреплению системы управления непрерывностью функционирования компании. Перспективными направлениями для развития возможностей OSINT в целях обеспечения корпоративной безопасности является мониторинг угроз в Dark Web, изучение влияния искусственного интеллекта на эффективность и риски OSINT-процессов, включая автоматизацию анализа данных. В качестве будущих направлений интеграции OSINT с другими технологиями выделяются: искусственный интеллект, машинное обучение и блокчейн-форензика, что позволит выявлять, к примеру, подозрительные транзакции с криптовалютой, киберуязвимости, дезинформацию в медиапространстве [Szymoniak, 2025]. Также с помощью OSINT прогнозируется создание более защищенных от несанкционированного доступа систем цифровой идентификации.

Отметим, что в компаниях финансового сектора и сфере консалтинга все более релевантным становится набор персонала с компетенциями в сфере OSINT-аналитики. Так, в компании «Сбербанк» для специалиста по информационной безопасности необходимы навыки аналитической обработки информации по методологии OSINT, для специалиста компании «Ингосстрах» также дополнительным требованием указывается анализ киберугроз с применением инструментов OSINT, в обязанности специалиста по управлению киберрисками компании «Деловые решения и технологии» входит анализ информации о компании на основе открытых источников (OSINT). Эксперты также отмечают необходимость инвестирования компаний в обучение специалистов лучшим практикам OSINT-аналитики для распознавания актуальных угроз, работы с автоматизированными

данными с учетом этических и правовых факторов [Szymoniak, 2025].

Помимо этого, не менее важным аспектом обеспечения комплексной безопасности ТЭК является устойчивое развитие нефтегазовой отрасли, которое сопряжено с рядом рисков: волатильность цен на энергоресурсы, установление потолка цен на нефтепродукты недружественными странами (price cap), увеличение количества трудноизвлекаемых запасов, потеря рынков сбыта, недостаток инноваций и технологий, ограничение доступа к иностранному капиталу, санкционное давление, введение эмбарго и т. д. [Противодействие угрозам … , 2023]. В данном контексте инструментарий OSINT используется для оценки и минимизации санкционных рисков, позволяет провести комплексную комплаенс-проверку контрагента на предмет санкционных связей, а также выявить конечных бенефициаров, в том числе по внешнеэкономическим сделкам.

Особую актуальность применение OSINT приобретает в рамках современного международного взаимодействия, при котором интенсивный обмен данными способствует формированию единого информационного пространства и увеличению доступности рядовых пользователей в интернете к огромному массиву разнородной информации о большинстве организаций. Так, известно, что системы онлайн-мониторинга водного и воздушного транспорта (например, flightradar24, marinetraffic) используются аналитиками для выявления актуальных транспортно-логических маршрутов конкурентов, сбора данных о направлениях сбыта продукции и основных партнерах.

Действительно, «международное сотрудничество в нефтегазовой отрасли стимулирует внедрение единых протоколов обработки информации» [Качелин, 2023, с. 95], а также создает платформу для большей информационной открытости взаимодействия. Вместе с очевидными положительными эффектами эти процессы порождают и дополнительные риски. Как отмечает Ю. В. Боровский, современные энергетические отношения требуют «гибких механизмов адаптации к изменяющимся геополитическим реалиям» [Боровский, 2023], что подчеркивает необходимость интеграции OSINT в стратегии безопасности крупных транснациональных компаний, которые часто являются основной целью рестрикционного давления в рамках текущих геополитических процессов.

Важно отметить, что использование инструментов OSINT позволяет компаниям нефтегазового сектора выявлять угрозы на ранних стадиях, анализируя открытые данные: от новостных агрегаторов до социальных сетей и спутниковых снимков. Например, мониторинг данных из открытых источников помогает предупредить кибератаки на системы управления производством, а анализ геополитических трендов – спрогнозировать риски срыва поставок. Я. А. Ворожеина и

соавторы указывают, что «геополитическая безопасность России напрямую связана с устойчивостью ее энергетической инфраструктуры» [Геополитическая безопасность … , 2023, с. 155], что делает OSINT критически важным для оценки региональных конфликтов и санкционных рисков.

Кроме того, OSINT способствует оперативному реагированию на инциденты. Так, в 2022 г. некоторые европейские компании использовали спутниковые данные для отслеживания перемещения танкеров в условиях санкций, что позволило оптимизировать логистику [Крюков, 2022]. Подобные примеры демонстрируют, как апробация инструмента анализа данных по открытым источникам становится основой для осуществления стратегических решений.

В то же время эффективность инструментов OSINT в информационно-аналитическом обеспечении безопасности предприятий нефтегазового сектора может быть усилена с помощью механизмов трансграничного сотрудничества. Так, страны СНГ, как отмечает А. Ю. Грачев, активно развивают правовые механизмы совместного мониторинга объектов ТЭК, включая обмен аналитикой на базе OSINT [Грачев, 2022]. Подобные инициативы снижают риски террористических актов и техногенных катастроф, обеспечивая оперативную обработку открытых данных.

Кроме того, проекты в рамках БРИКС, такие как разработка альтернативных систем платежей, опираются на OSINT с целью минимизации рисков санкционного давления [Российский и мировой ТЭК … , 2024; Мурашко, 2023]. Данный пример демонстрирует, как международное взаимодействие интегрирует открытые данные в инструментарий экономической безопасности.

**Заключение**

Несмотря на высокий потенциал, в случае применения OSINT в международном контексте наблюдается ряд сложностей. В первую очередь, требуется тщательная проверка данных на предмет фейкового характера информации. Во-вторых, национальный правовой режим данных, подлежащих обмену на международном уровне, может иметь существенные различия, что затрудняет сотрудничество стран в данной сфере. Е. А. Осадченко отмечает, что «энергетическая безопасность РФ зависит от согласованности международно-правовых норм» [Осадченко, 2024, с. 85], что актуально для регулирования OSINT.

Как подчеркивает А. В. Новак, «надежность энергоснабжения невозможна без инновационных подходов к безопасности» [Новак, 2021, с. 10]. В данном контексте OSINT становится связующим звеном между технологическим прогрессом и перспективами международного взаимодействия в обеспечении комплексной безопасности нефтегазовых предприятий.

Таким образом, по результатам исследования авторами было выявлено следующее:

1) инструментарий OSINT имеет значительный потенциал к дальнейшему внедрению в процессы информационно-аналитического обеспечения комплексной безопасности нефтегазовых предприятий, позволяя минимизировать различные виды рисков, возникающих в ходе их функционирования, в особенности в случае применения на объектах автоматизированных систем управления. Также прогнозируется будущее интеграции OSINT с технологиями машинного обучения, искусственного интеллекта, блокчейн-форензики;

2) при этом на данный момент отсутствует единый подход к дефиниции OSINT на международно-правовом уровне наряду с толкованием сферы применения данного инструмента. Таким образом, инструменты OSINT широко используются в различных сферах: от маркетинговых исследований и корпоративной безопасности до выявления нарушений санкционных режимов отдельными странами. Отсутствует также и полный перечень видов инструментов, методик и способов разведки по открытым источникам, несмотря на некоторые попытки со стороны экспертного и научного сообщества по систематизации указанной деятельности;

3) основные виды безопасности нефтегазовых объектов, в рамках которых могут быть использованы OSINT-данные: экономическая и финансовая безопасность, информационная безопасность, кадровая безопасность, социально-политические и международно-политические условия функционирования предприятий, физическая защищенность объектов;

4) определены направления интеграции OSINT в обеспечение безопасности объектов нефтегазового комплекса, в частности, использование открытых данных для формирования моделей прогнозирования частоты кибератак на предприятия.

**Библиографический список**

1. Боровский Ю. В. Россия и Евросоюз: смена тренда в энергетических отношениях // Российский социально-гуманитарный журнал. 2023. № 3. DOI 10.18384/2224-0209-2023-3-1323. EDN VUNYMU.

2. Волошин В. И. Технологический фактор развития российского нефтегазового комплекса // Российский внешнеэкономический вестник. 2023. № 7. С. 7–23. DOI 10.24412/2072-8042-2023-7-7-23. EDN MPDLGT.

3. Геополитическая безопасность России: к постановке проблемы / Я. А. Ворожеина, А. П. Клемешев, Н. А. Комлева [и др.] // Балтийский регион. 2023. Т. 15, № 1. С. 153–169. DOI 10.5922/2079-8555-2023-1-9. EDN YGFCOQ.

4. Горбашко Е. А. Технологический суверенитет как фактор конкурентоспособности нефтегазовых компаний Российской Федерации / Е. А. Горбашко, В. И. Бородин // Экономика и управление. 2024. Т. 30, № 9. С. 1100–1110. DOI 10.35854/1998-1627-2024-9-1100-1110. EDN QXXKHW.

5. Грачев А. Ю. Международное сотрудничество стран СНГ в сфере правового обеспечения безопасности объектов топливно-энергетического комплекса // Международное сотрудничество евразийских государств: политика, экономика, право. 2022. № 1. С. 21–29. EDN FMKHXA.

6. Доклад RAND «Mitigating Emerging Human Intelligence Challenges with Forecasting». URL: https://www.rand.org/pubs/commentary/2025/06/mitigating-emerging-human-intelligence-challenges-with.html (дата обращения: 24.04.2025).

7. Елкина О. С. Внутренние угрозы энергетической безопасности и пути их нейтрализации / О. С. Елкина, С. Е. Елкин, В. А. Сырчин // Теоретическая экономика. 2021. № 10(82). С. 56–70. DOI 10.52957/22213260_2021_10_56. EDN UBVJRB.

8. Жданеев О. В. Обеспечение технологического суверенитета отраслей ТЭК Российской Федерации // Записки Горного института. 2022. Т. 258. С. 1061–1078. DOI 10.31897/PMI.2022.107. EDN QBQUEX.

9. Качелин А. С. Международное сотрудничество как фактор научно-технологического развития в нефтегазовой отрасли России // ЭТАП: экономическая теория, анализ, практика. 2023. № 1. С. 85–110. DOI 10.24412/2071-6435-2023-1-85-110. EDN UKBXCO.

10. Крюков В. А. ТЭК Китая и России в контексте перехода на траекторию низкоуглеродного развития / В. А. Крюков, Я. В. Крюков // Пространственная экономика. 2022. Т. 18, № 3. С. 141–167. DOI 10.14530/se.2022.3.141-167. EDN OELQST.

11. Медведев Д. А. Информационно-аналитическое описание газоперерабатывающего завода как типового объекта топливного сектора инфраструктуры зарубежных стран на основе открытых источников / Д. А. Медведев, Р. А. Полончук // Экономика и управление: проблемы, решения. 2025. Т. 3, № 2(155). С. 62–69. DOI 10.36871/ek.up.p.r.2025.02.03.007. EDN BALPNZ.

12. Мередит Дейл Д27 OSINT. Руководство по сбору и анализу открытой информации в интернете. Астана : Спринт Бук, 2025. 224 с.

13. Мурашко М. М. Российская стратегия импортозамещения в ТЭК // Геоэкономика энергетики. 2023. Т. 22, № 2. С. 18–39. DOI 10.48137/26870703_2023_22_2_18. EDN CGWZMO.

14. Новак А. В. Задача ТЭК России – надежное снабжение потребителей страны и мира // Энергетическая политика. 2021. № 2(156). С. 6–17. DOI 10.46920/2409-5516_2021_2156_6. EDN MSLPVF.

15. Организация Объединенных Наций: официальный сайт. URL: https://www.unodc.org/unodc/frontpage/2025/March/using-open-source-intelligence-to-investigate-human-trafficking-and-migrant-smuggling.html (дата обращения: 24.04.2025).

16. Осадченко Е. А. Место энергетической безопасности в системе безопасности Российской Федерации // Вестник Омского университета. Серия: Экономика. 2024. Т. 22, № 3. С. 83–91. DOI 10.24147/1812-3988.2024.22(3).83-91. EDN GFFCRN.

17. Палеев Д. Л. Пути укрепления энергетической безопасности России в условиях обострения геополитической ситуации / Д. Л. Палеев, М. В. Черняев // Экономические системы. 2022. Т. 15, № 4. С. 154–164. DOI 10.29030/2309-2076-2022-15-4-154-164. EDN ORLTKI.

18. Перов А. В. Процессы трансформации российской энергетики: геополитическое измерение // Геоэкономика энергетики. 2024. Т. 25, № 1. С. 111–124. DOI 10.48137/26870703_2024_25_1_111. EDN MJFCRA.

19. Подходы к обеспечению безопасности на нефтегазовых предприятиях / А. С. Кравцов, В. А. Седельникова, К. А. Чижов [и др.] // Московский экономический журнал. 2021. № 9. DOI 10.24411/2413-046X-2021-10573. EDN UKNVMY.

20. Противодействие угрозам и рискам устойчивого развития нефтегазовой отрасли как стратегическое направление обеспечения экономической безопасности РФ / Ю. А. Чугаева, А. А. Лютынская, А. Р. Ашалян, Е. Е. Ткаля // Естественно-гуманитарные исследования. 2023. № 1(45). С. 303–309. EDN QNWORI.

21. Самарин И. В. Обеспечение информационной безопасности АСУ ТП с использованием метода предиктивной защиты // Программные продукты и системы. 2022. № 3. С. 111–118. DOI: 10.15827/2311-6749.22.3.111.

22. Российский и мировой ТЭК: угрозы и перспективы повышения экономической безопасности / Ю. А. Чугаева, А. Л. Унанов, М. С. Боженов, М. З. Тхагушев // Естественно-гуманитарные исследования. 2024. № 2(52). С. 283–286. EDN GKEPZR.

23. Трофимов С. Е. Государственное регулирование нефтегазового комплекса в условиях цифровизации мировой экономической системы // Управленческие науки. 2023. Т. 13, № 1. С. 71–82. DOI 10.26794/2304-022X-2023-13-1-71-82. EDN ESQTLH.

24. Шармаев В. И. Обеспечение информационной безопасности с помощью разведки по открытым источникам (OSINT) / В. И. Шармаев, Я. А. Андреева, К. А. Василевский // Вопросы защиты информации. 2022. № 2(137). С. 45–50. DOI 10.52190/2073-2600_2022_2_45. EDN KRYLPB.

25. Янгаева М. О. OSINT. Получение криминалистически значимой информации из сети Интернет / М. О. Янгаева, Н. О. Павленко // Алтайский юридический вестник. 2022. № 2(38). С. 131–135. EDN HDISPM.

26. Ярош А. С. Цифровая экономика и безопасность КИИ ТЭК / А. С. Ярош, А. В. Житников // Вестник научного центра по безопасности работ в угольной промышленности. 2020. № 3. С. 68–72. EDN CRHHVQ.

27. Blackdot Solutions: официальный сайт. URL: https://blackdotsolutions.com/wp-content/uploads/2022/10/The-Guide-to-OSINT-for-Financial-Crime-Investigators.pdf (дата обращения: 24.04.2025).

28. Rajamäki, Jyri & Tiitta, Krista. Implementation of OSINT for Improving an International Finance Sector Organization’s Cybersecurity. International Conference on Cyber Warfare and Security. 19. 612-616. 202410.34190/iccws.19.1.1977.

29. Szymoniak, Sabina; Foks, Kacper; and Pyrkosz-Dziubczyk, Aleksandra “Application of OSINT Methods in Ensuring Cybersecurity”, IPSI Transactions on Internet Research, vol. 20(2), pp. 38-49, 2025. https://doi.org/10.58245/ipsi.tir.2502.05.

30. The IC OSINT Strategy 2024-2026. URL: https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf (дата обращения: 24.04.2025).

**Reference list**

1. Borovskij Ju. V. Rossija i Evrosojuz: smena trenda v jenergeticheskih otnoshenijah = Russia and the European Union: a change in trend in energy relations // Rossijskij social'no-gumanitarnyj zhurnal. 2023. № 3. DOI 10.18384/2224-0209-2023-3-1323. EDN VUNYMU.

2. Voloshin V. I. Tehnologicheskij faktor razvitija rossijskogo neftegazovogo kompleksa = Technological factor of development of the Russian oil and gas complex // Rossijskij vneshnejekonomicheskij vestnik. 2023. № 7. S. 7–23. DOI 10.24412/2072-8042-2023-7-7-23. EDN MPDLGT.

3. Geopoliticheskaja bezopasnost' Rossii: k postanovke problemy = Geopolitical security of Russia: to the formulation of the problem / Ja. A. Vorozheina, A. P. Klemeshev, N. A. Komleva [i dr.] // Baltijskij region. 2023. T. 15, № 1. S. 153–169. DOI 10.5922/2079-8555-2023-1-9. EDN YGFCOQ.

4. Gorbashko E. A. Tehnologicheskij suverenitet kak faktor konkurentosposobnosti neftegazovyh kompanij Rossijskoj Federacii = Technological sovereignty as a factor of competitiveness of oil and gas companies of the Russian Federation / E. A. Gorbashko, V. I. Borodin // Jekonomika i upravlenie. 2024. T. 30, № 9. S. 1100–1110. DOI 10.35854/1998-1627-2024-9-1100-1110. EDN QXXKHW.

5. Grachev A. Ju. Mezhdunarodnoe sotrudnichestvo stran SNG v sfere pravovogo obespechenija bezopasnosti ob#ektov toplivno-jenergeticheskogo kompleksa = International cooperation of the CIS countries in the field of legal support for the safety of fuel and energy facilities // Mezhdunarodnoe sotrudnichestvo evrazijskih gosudarstv: politika, jekonomika, pravo. 2022. № 1. S. 21–29. EDN FMKHXA.

6. Doklad RAND «Mitigating Emerging Human Intelligence Challenges with Forecasting» = Report RAND «Mitigating Emerging Human Intelligence Challenges with Forecasting». URL: https://www.rand.org/pubs/commentary/2025/06/mitigating-emerging-human-intelligence-challenges-with.html (data obrashhenija: 24.04.2025).

7. Elkina O. S. Vnutrennie ugrozy jenergeticheskoj bezopasnosti i puti ih nejtralizacii Internal threats to energy security and ways to neutralize them / O. S. Elkina, S. E. Elkin, V. A. Syrchin // Teoreticheskaja jekonomika. 2021. № 10(82). S. 56–70. DOI 10.52957/22213260_2021_10_56. EDN UBVJRB.

8. Zhdaneev O. V. Obespechenie tehnologicheskogo suvereniteta otraslej TJeK Rossijskoj Federacii = Ensuring the technological sovereignty of the fuel and energy sectors of the Russian Federation // Zapiski Gornogo instituta. 2022. T. 258. S. 1061–1078. DOI 10.31897/PMI.2022.107. EDN QBQUEX.

9. Kachelin A. S. Mezhdunarodnoe sotrudnichestvo kak faktor nauchno-tehnologicheskogo razvitija v neftegazovoj otrasli Rossii = International cooperation as a factor of scientific and technological development in the Russian oil and gas industry // JeTAP: jekonomicheskaja teorija, analiz, praktika. 2023. № 1. S. 85–110. DOI 10.24412/2071-6435-2023-1-85-110. EDN UKBXCO.

10. Krjukov V. A. TJeK Kitaja i Rossii v kontekste perehoda na traektoriju nizkouglerodnogo razvitija = Fuel and energy complex of China and Russia in the context of the transition to a low-carbon development trajectory / V. A. Krjukov, Ja. V. Krjukov // Prostranstvennaja jekonomika. 2022. T. 18, № 3. S. 141–167. DOI 10.14530/se.2022.3.141-167. EDN OELQST.

11. Medvedev D. A. Informacionno-analiticheskoe opisanie gazopererabatyvajushhego zavoda kak tipovogo ob#ekta toplivnogo sektora infrastruktury zarubezhnyh stran na osnove otkrytyh istochnikov = Information and analytical description of the gas processing plant as a typical object of the fuel sector of the infrastructure of foreign countries based on open sources / D. A. Medvedev, R. A. Polonchuk // Jekonomika i upravlenie: problemy, reshenija. 2025. T. 3, № 2(155). S. 62–69. DOI 10.36871/ek.up.p.r.2025.02.03.007. EDN BALPNZ.

12. Meredit Dejl D27 OSINT. Rukovodstvo po sboru i analizu otkrytoj informacii v internete = Guidelines for collecting and analyzing open information on the Internet Astana : Sprint Buk, 2025. 224 s.

13. Murashko M. M. Rossijskaja strategija importozameshhenija v TJeK = Russian strategy of import substitution in the fuel and energy complex // Geojekonomika jenergetiki. 2023. T. 22, № 2. S. 18–39. DOI 10.48137/26870703_2023_22_2_18. EDN CGWZMO.

14. Novak A. V. Zadacha TJeK Rossii – nadezhnoe snabzhenie potrebitelej strany i mira = The task of the fuel and energy complex of Russia is to reliably supply consumers of the country and the world // Jenergeticheskaja politika. 2021. № 2(156). S. 6–17. DOI 10.46920/2409-5516_2021_2156_6. EDN MSLPVF.

15. Organizacija Ob#edinennyh Nacij = United Nations: oficial'nyj sajt. URL: https://www.unodc.org/unodc/frontpage/2025/March/using-open-source-intelligence-to-investigate-human-trafficking-and-migrant-smuggling.html (data obrashhenija: 24.04.2025).

16. Osadchenko E. A. Mesto jenergeticheskoj bezopasnosti v sisteme bezopasnosti Rossijskoj Federacii = Place of energy security in the security system of the Russian Federation // Vestnik Omskogo universiteta. Serija: Jekonomika. 2024. T. 22, № 3. S. 83–91. DOI 10.24147/1812-3988.2024.22(3).83-91. EDN GFFCRN.

17. Paleev D. L. Puti ukreplenija jenergeticheskoj bezopasnosti Rossii v uslovijah obostrenija geopoliticheskoj situacii = Ways to strengthen Russia's energy security amid a worsening geopolitical situation / D. L. Paleev, M. V. Chernjaev // Jekonomicheskie sistemy. 2022. T. 15, № 4. S. 154–164. DOI 10.29030/2309-2076-2022-15-4-154-164. EDN ORLTKI.

18. Perov A. V. Processy transformacii rossijskoj jenergetiki: geopoliticheskoe izmerenie = Russian energy transformation processes: geopolitical dimension // Geojekonomika jenergetiki. 2024. T. 25, № 1. S. 111–124. DOI 10.48137/26870703_2024_25_1_111. EDN MJFCRA.

19. Podhody k obespecheniju bezopasnosti na neftegazovyh predprijatijah = Approaches to Safety at Oil and Gas Enterprises / A. S. Kravcov, V. A. Sedel'nikova, K. A. Chizhov [i dr.] // Moskovskij jekonomicheskij zhurnal. 2021. № 9. DOI 10.24411/2413-046X-2021-10573. EDN UKNVMY.

20. Protivodejstvie ugrozam i riskam ustojchivogo razvitija neftegazovoj otrasli kak strategicheskoe napravlenie obespechenija jekonomicheskoj bezopasnosti RF = Countering threats and risks of sustainable development of the oil and gas industry as a strategic direction for ensuring the economic security of the Russian Federation / Ju. A. Chugaeva, A. A. Ljutynskaja, A. R. Ashaljan, E. E. Tkalja // Estestvenno-gumanitarnye issledovanija. 2023. № 1(45). S. 303–309. EDN QNWORI.

21. Samarin I. V. Obespechenie informacionnoj bezopasnosti ASU TP s ispol'zovaniem metoda prediktivnoj zashhity = Ensuring information security of APCS using the predictive protection method // Programmnye produkty i sistemy. 2022. № 3. S. 111–118. DOI: 10.15827/2311-6749.22.3.111.

22. Rossijskij i mirovoj TJeK: ugrozy i perspektivy povyshenija jekonomicheskoj bezopasnosti = Russian and world fuel and energy complex: threats and prospects for improving economic security / Ju. A. Chugaeva, A. L. Unanov, M. S. Bozhenov, M. Z. Thagushev // Estestvenno-gumanitarnye issledovanija. 2024. № 2(52). S. 283–286. EDN GKEPZR.

23. Trofimov S. E. Gosudarstvennoe regulirovanie neftegazovogo kompleksa v uslovijah cifrovizacii mirovoj jekonomicheskoj sistemy = State regulation of the oil and gas complex in the context of digitalization of the global economic system // Upravlencheskie nauki. 2023. T. 13, № 1. S. 71–82. DOI 10.26794/2304-022X-2023-13-1-71-82. EDN ESQTLH.

24. Sharmaev V. I. Obespechenie informacionnoj bezopasnosti s pomoshh'ju razvedki po otkrytym istochnikam (OSINT) = Information Security through Open Source Intelligence (OSINT) / V. I. Sharmaev, Ja. A. Andreeva, K. A. Vasilevskij // Voprosy zashhity informacii. 2022. № 2(137). S. 45–50. DOI 10.52190/2073-2600_2022_2_45. EDN KRYLPB.

25. Jangaeva M. O. OSINT. Poluchenie kriminalisticheski znachimoj informacii iz seti Internet = Obtaining criminally relevant information from the Internet / M. O. Jangaeva, N. O. Pavlenko // Altajskij juridicheskij vestnik. 2022. № 2(38). S. 131–135. EDN HDISPM.

26. Jarosh A. S. Cifrovaja jekonomika i bezopasnost' KII TJeK = Digital Economy and Security CII Fuel and Energy Complex / A. S. Jarosh, A. V. Zhitnikov // Vestnik nauchnogo centra po bezopasnosti rabot v ugol'noj promyshlennosti. 2020. № 3. S. 68–72. EDN CRHHVQ.

27. Blackdot Solutions: oficial'nyj sajt. URL: https://blackdotsolutions.com/wp-content/uploads/2022/10/The-Guide-to-OSINT-for-Financial-Crime-Investigators.pdf (data obrashhenija: 24.04.2025).

28. Rajamäki, Jyri & Tiitta, Krista. Implementation of OSINT for Improving an International Finance Sector Organization's Cybersecurity. International Conference on Cyber Warfare and Security. 19. 612-616. 202410.34190/iccws.19.1.1977.

29. Szymoniak, Sabina; Foks, Kacper; and Pyrkosz-Dziubczyk, Aleksandra "Application of OSINT Methods in Ensuring Cybersecurity", IPSI Transactions on Internet Research, vol. 20(2), pp. 38-49, 2025. https://doi.org/10.58245/ipsi.tir.2502.05.

30. The IC OSINT Strategy 2024-2026. URL: https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf (data obrashhenija: 24.04.2025).

Статья поступила в редакцию 20.03.2025; одобрена после рецензирования 25.04.2025; принята к публикации 15.05.2025.
The article was submitted on 20.03.2025; approved after reviewing 25.04.2025; accepted for publication on 15.05.2025