

УДК 331.45

***ОБЕСПЕЧЕНИЕ РЕЖИМА ОХРАНЫ ОБЪЕКТА И БЕЗОПАСНОСТИ
ПЕРСОНАЛА НА ПРИМЕРЕ КРУПНЕЙШЕГО ГАЗОДОБЫВАЮЩЕГО
ПРЕДПРИЯТИЯ РФ***

Загарских А.А.

студент,

Вятский государственный университет,

Киров, Россия

Маджара А.А.

студентка,

Вятский государственный университет,

Киров, Россия

Котанджян А.В.

старший преподаватель,

Вятский государственный университет,

Киров, Россия

Аннотация: В данной статье рассматривается наше видение по обеспечению режима охраны объекта и безопасности персонала на примере крупнейшего газодобывающего предприятия РФ, данная компания является одной из крупнейших независимых газодобывающих компаний России. В условиях глобальной конкуренции и сложной политической обстановки вопросы безопасности становятся особенно актуальными как для бизнеса, так и для государства. В статье мы уделяем особое внимание рискам, связанным с угрозами безопасности, и нашим рекомендациям, для компании, как она будет реагировать на них, обеспечивая эффективность рабочего процесса и защиту

работников. Также рассматривается предложенная нами базовая модель нарушителя для данного предприятия. В заключение, подчёркивается, что применение современных технологий и методов управления безопасностью является залогом устойчивой работы предприятия в условиях меняющихся вызовов и угроз в данной отрасли.

Ключевые слова: обеспечение безопасности, охрана объекта, риски безопасности, угрозы, безопасность

***ENSURING SITE SECURITY AND STAFF SAFETY USING THE
EXAMPLE OF THE LARGEST GAS PRODUCING ENTERPRISE IN THE
RUSSIAN FEDERATION***

Zagarskikh A.A.

student,

Vyatka State University,

Kirov, Russia

Madzhara A.A.

student,

Vyatka State University,

Kirov, Russia

Kotanjyan A.V.

Senior Lecturer,

Vyatka State University,

Kirov, Russia

Abstract: This article discusses our vision of ensuring the security of the facility and the safety of personnel using the example of the largest gas producing enterprise of the

Russian Federation, this company is one of the largest independent gas producing companies in Russia. In the context of global competition and a difficult political situation, security issues are becoming especially relevant for both business and the state. In the article, we pay special attention to the risks associated with security threats and our recommendations for the company on how it will respond to them, ensuring the efficiency of the work process and the protection of employees. We also consider the basic model of an intruder proposed by us for this enterprise. In conclusion, it is emphasized that the use of modern technologies and security management methods is the key to the sustainable operation of the enterprise in the context of changing challenges and threats in this industry.

Key words: security, facility security, security risks, threats, safety.

Обеспечение режима охраны объекта и безопасности персонала — это система мероприятий и процедур, направленных на защиту материальных и нематериальных активов организации, а также обеспечение безопасных условий труда для сотрудников. Она включает в себя оценку рисков, внедрение мероприятий по охране, контроль доступа, физическую охрану, обучение персонала, мониторинг потенциальных угроз и реакцию на чрезвычайные ситуации для минимизации угроз и предотвращения инцидентов [1].

ПАО «НОВАТЭК» — крупнейший российский независимый производитель природного газа и сжиженного природного газа (СПГ) с одним из самых низких в мире углеродным следом. С момента своего основания в 1994 году компания придерживается принципов ответственного ведения бизнеса, фокусируясь на поставках доступной и надежной энергии, обеспечивая растущий спрос среди своих потребителей и способствуя глобальному энергетическому переходу.

Стратегические цели «НОВАТЭКа» [4]:

- Наращивание ресурсной базы
- Сохранение низкого уровня затрат

- Устойчивое развитие
- Увеличение добычи углеводородов
- Оптимизация каналов маркетинга
- Масштабирование СПГ-проектов

Проанализировав подробно данную компанию, можно сказать, что ПАО «НОВАТЭК» относится к объектам подгруппы АІ. Объекты подгрупп АІ — это объекты особо важные, повышенной опасности и жизнеобеспечения, противоправных действия (кража, грабеж, разбой, терроризм и другие) на которых, в соответствии с уголовным законодательством Российской Федерации могут привести к крупному, особо крупному экономическому или социальному ущербу государству, обществу, предприятию, экологии или иному владельцу имущества [5].

Чтобы детально изучить данный охраняемый объект, мы составили примерную его схему, используя программу Microsoft Visio (рис. 1).

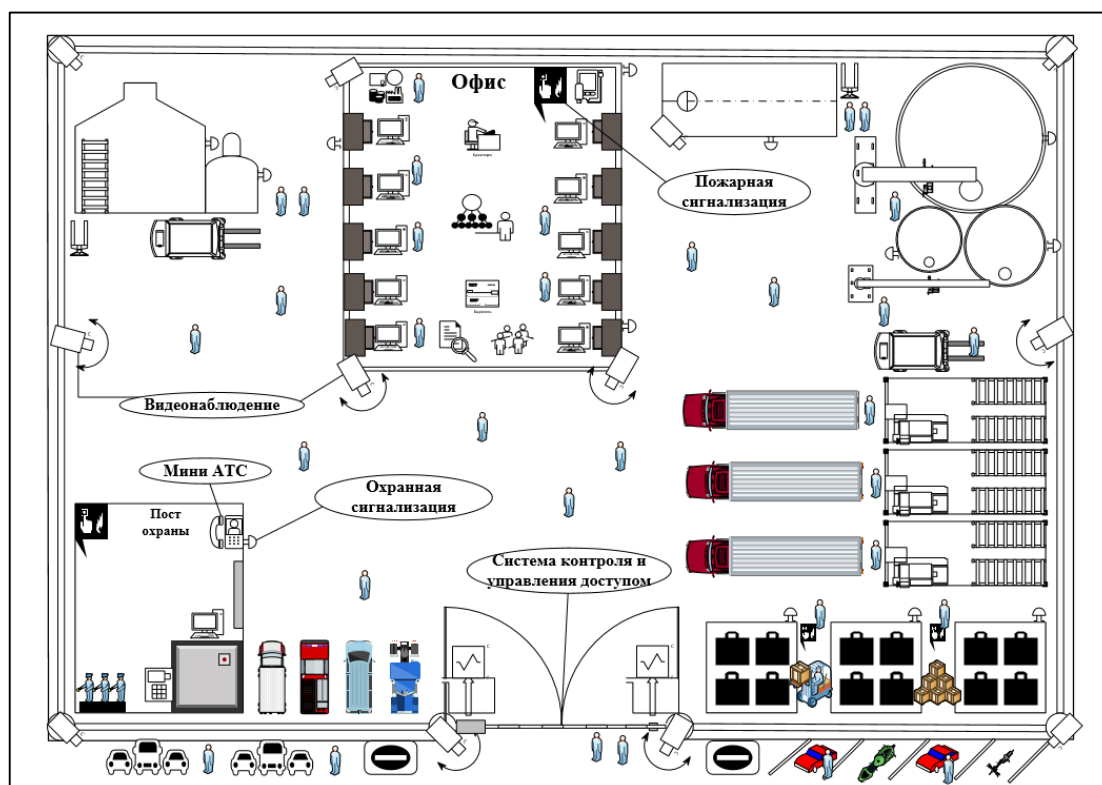


Рис. 1 — Схема охранного объекта ПАО «НОВАТЕК»

Итак, когда мы уже поняли, что это за компания, мы перешли к рассмотрению и выявлению конкретных рисков (угроз), которые присущи ПАО «НОВАТЭК», разберём их подробнее [4]:

Операционные риски:

1. Технологические риски

Аварии, пожары, взрывы на производстве и морских судах:

- Ущерб имуществу и потери от приостановки деятельности (в т. ч. катастрофические и хвостовые риски)
- Ущерб жизни и здоровью, в т. ч. третьих лиц

2. Климатические риски

• Риски, связанные с ведением производственной деятельности в районах многолетней мерзлоты и Крайнего Севера

- Физические и переходные риски, связанные с изменением климата

3. Экологические риски

• Воздействие на окружающую среду в результате аварий, разливов нефти и нефтепродуктов

• Влияние на состояние водных ресурсов и компонентов биоразнообразия, в т. ч.:

- нехватка водных ресурсов
- нарушение прав местных сообществ на свободный доступ к водным и биологическим ресурсам

4. Социальные риски

- Нарушение этических норм
- Нарушение прав человека
- Нехватка квалифицированных кадров, ограничение свободы объединений

• Нарушение прав и интересов местных сообществ

5. Риски форс-мажорных ситуаций

- Природные бедствия

- Массовые эпидемии
- Террористические акты
- Киберриски

Корпоративные риски:*6. Законодательно-регуляторные риски в области экологии и климата*

- Ужесточение углеродного регулирования в РФ и мире
- Изменение нормативов выбросов и сбросов загрязняющих веществ
- Ужесточение экологических норм в отношении особо охраняемых

природных зон (Арктика)

7. Политические риски

- Влияние политической и экономической ситуации в РФ и мире

Проектные риски:*8. Проектные риски*

- Влияние внутренних или внешних факторов на реализацию

перспективных проектов Компани

Также в процессе изучения данной компании мы самостоятельно разработали модель нарушителя для ПАО «НОВАТЕК», используя официальную статистику и другую информацию исследуемого объекта. Данную модель мы расписали и занесли в таблицу 1.

Таблица 1 — Модель нарушителя для ПАО «НОВАТЭК»

Показатели	Информация про ПАО «НОВАТЭК»
Статистика нарушений на защищаемом объекте	• Инцидент на территории ООО «НОВАТЭК-ТАРКОСАЛЕНЕФТЕГАЗ» – взрыв, произошедший в феврале 2023 года при проведении сварочных работ на трубном пучке в цехе регенерации метанола. Двое работников. Компании погибли, один пострадал. • В 2023 году произошло семь несчастных случаев на производстве: один со смертельным исходом, шесть — с легкими

	травмами. Всего от несчастных случаев, связанных с производством, пострадало девять человек. В последние три года также наблюдается положительная динамика снижения количества несчастных случаев. • В 2023 году в регионах присутствия Компании не зафиксировано случаев природных бедствий или существенного изменения условий окружающей среды под влиянием изменения климата
Криминогенная обстановка в регионе	• В 2023 году криминогенная ситуация в ямало-ненецком автономном округе характеризуется увеличением общего количества зарегистрированных преступлений на 14,9% (с 6 657 до 7 646). Рост преступности объясняется увеличением масштабов распространения преступлений, совершенных с использованием высоких технологий (+42,7%; с 2 703 до 3 858). В результате совершения преступлений причинён ущерб на сумму порядка 718 млн рублей. Обстановка по линии противодействия данным преступлениям остаётся стабильно напряжённой в условиях продолжающегося стремительного развития цифровых средств связи. За последние 3 года доля таких преступлений в общей структуре преступности увеличилась с 39% до 50%.
Возможности круга заинтересованных к охраняемому объекту лиц (организаций)	• Государство (федеральные и региональные органы власти): обладает значительными возможностями в виде контроля, регулирования, лицензирования, налогообложения, а также в обеспечении безопасности объектов критической инфраструктуры. Они могут проводить проверки, налагать санкции, изымать лицензии.

	• Подрядчики и поставщики: имеют доступ на территорию объектов для выполнения работ или поставок. Их действия могут влиять на безопасность. • Сотрудники: имеют доступ к информации и оборудованию на предприятиях. Их действия могут как способствовать, так и вредить безопасности объекта. Мотивация может быть, как добросовестной, так и связанной с различными видами злоупотреблений (например, кража, саботаж). • Акционеры и инвесторы: имеют экономический интерес в деятельности компании и следят за ее финансовыми показателями и безопасностью активов. Могут оказывать влияние через собрания акционеров, управление рисками и инвестиционные решения.
Воздействие внешних и внутренних факторов	Внешние факторы: • Геополитическая ситуация: это, пожалуй, самый значимый внешний фактор. Геополитическая нестабильность, санкции, международные отношения и политические риски в России и мире напрямую влияют на инвестиционный климат, доступ к финансированию, экспортные возможности и ценообразование на СПГ. Изменения в отношениях с ключевыми партнерами и странами-импортерами СПГ могут существенно повлиять на прибыльность компании. • Мировая экономика: глобальный экономический рост или спад, изменение спроса на энергоресурсы, колебания валютных курсов, инфляция — все это влияет на цены на СПГ, объемы продаж и прибыльность «НОВАТЭКа». • Цены на энергоносители: цены на нефть и газ, а также на альтернативные источники энергии являются ключевыми

факторами, определяющими рентабельность компании. Изменение цен на нефть может косвенно влиять на цены на газ.

- Технологические изменения: развитие технологий в сфере добычи, переработки и транспортировки СПГ, а также появление новых, более дешевых или экологически чистых источников энергии могут повлиять на конкурентоспособность «НОВАТЭКа».

- Экологические требования: ужесточение экологического законодательства, требования по сокращению выбросов парниковых газов, общественное давление на компании, занимающиеся добычей углеводородов, влияют на операционные затраты и инвестиционные планы «НОВАТЭКа».

- Регуляторная среда: изменения в законодательстве, налоговом режиме, лицензировании и других аспектах регулирования энергетического сектора в России могут существенно повлиять на деятельность компании.

Внутренние факторы:

- Эффективность управления: качество менеджмента, стратегическое планирование, эффективность операционной деятельности, управление персоналом — все это влияет на рентабельность и конкурентоспособность компании.

- Технологические возможности: уровень технологического развития, инновации, использование современного оборудования определяют эффективность и безопасность производственных процессов.

	• Финансовое состояние: доступ к финансированию, уровень задолженности, дивидендная политика, инвестиционная активность влияют на финансовую устойчивость компании. • Управление рисками: эффективность системы управления рисками, связанными с безопасностью, экологией, геополитикой и другими факторами, определяет способность компании предотвращать потери и поддерживать репутацию. • Кадровый потенциал: квалификация персонала, уровень мотивации, кадровый резерв — все это влияет на эффективность работы компании.
--	--

С учетом модели нарушителя и наиболее важных рисков для компании, можно составить рекомендации и предложить необходимый материал в концепцию безопасности ПАО «НОВАТЕК» [4]. Рассмотрим этот вопрос подробнее.

Рекомендации по технологическим рискам

- 1) Обучение требованиям охраны труда и промышленной безопасности и контроль знаний персонала
- 2) Контроль технологических режимов работы оборудования, устранение рисков в цикле PDCA (PDCA расшифровывается как Plan, Do, Check, Act — «планируй, делай, проверяй, действуй»).
- 3) Разработка и реализация планов ликвидации аварий, разливов нефти и нефтепродуктов, планов непрерывности бизнеса и др.
- 4) Страхование технологических рисков

Рекомендации по экологическим рискам

Предотвращение аварийных ситуаций с нанесением вреда окружающей среде необходимо:

- 1) Контроль технологических режимов работы оборудования

2) Реализация мероприятий по достижению экологических и климатических целей – 2030

3) Страхование рисков экологического ущерба и ответственности в случае аварий

Предотвращение разливов нефти и нефтепродуктов при хранении или транспортировке по трубопроводам / морскими судами необходимо:

1) Контроль технического состояния трубопроводов (коррозия, износ, проседание и др.) и морских судов

2) Разработка и реализация планов ликвидации аварий, разливов нефти

3) и нефтепродуктов, планов непрерывности бизнеса

4) Анализ областей с наиболее существенными последствиями в случае разливов

5) Страхование рисков ущерба и гражданской ответственности в случае разливов нефти/нефтепродуктов

Предотвращение негативного воздействия на водные ресурсы и биоразнообразие необходимо:

1) Соблюдение норм природоохранного законодательства (экологические требования, порядок водоотведения) и регулярный контроль надзорными органами

2) Обеспечение свободного доступа к водным и биологическим ресурсам местным сообществам

3) Разработка и реализация мероприятий по сохранению биоразнообразия и природных экосистем в регионах присутствия Компании

Рекомендации по законодательно-регуляторным рискам в области экологии и климата

1) Прогноз и контроль инициатив введения/ужесточения углеродного регулирования в РФ и мире

2) Участие в заседаниях комитетов Государственной думы и профильных ассоциациях по вопросам изменения климата

3) Разработка и реализация технических решений по декарбонизации и снижению углеродного следа продукции Компании

4) Контроль соблюдения всех норм природоохранного законодательства, в т. ч. в особо охраняемых природных зонах

Рекомендации по политическим рискам

1) Реализация программы импортозамещения и локализации производства на территории РФ

2) Поиск альтернативных решений в условиях введенных ограничений

3) Поиск альтернативных покупателей и рынков сбыта

4) Разработка и использование собственных технологических решений в области производства СПГ и переработки газа

Рекомендации по проектным рискам

1) Поиск альтернативных технологических решений, поставщиков и производителей из дружественных юрисдикций

2) Локализация производства необходимого оборудования на предприятиях РФ

3) Реализация собственных запатентованных технологий сжижения

4) Поиск альтернативных логистических решений по вывозу и перевалке СПГ

Также хочется порекомендовать несколько предложений по созданию системы охраны исследуемого объекта. Система охраны ПАО «НОВАТЭК» должна быть многоуровневой, интегрированной и учитывать специфику объектов, их расположение и потенциальные угрозы. Она должна обеспечивать физическую, техническую и информационную безопасность, а также эффективное реагирование на чрезвычайные ситуации [3]. Разберёмся подробнее.

1 Цели системы охраны:

- Предотвращение несанкционированного доступа на объекты.
- Обеспечение безопасности персонала и посетителей.

- Защита имущества от краж, вандализма и других преступных посягательств.

- Предотвращение террористических актов и диверсий.
- Обеспечение непрерывности производственных процессов.
- Минимизация экологических рисков.
- Защита конфиденциальной информации.

2 Принципы построения системы охраны:

- Комплексный подход: включает физическую, техническую и информационную безопасность, а также оперативное реагирование.

- Эшелонированность: создание нескольких рубежей защиты (периметр, внутренние зоны), каждый из которых выполняет свою функцию.

- Интеграция: объединение всех элементов системы в единый центр управления, позволяющий оперативно получать информацию о происходящих событиях и координировать действия охраны.

- Проактивность: ориентация на предотвращение угроз, а не только на реагирование на них.

- Адаптивность: способность системы адаптироваться к изменяющимся условиям и новым угрозам.

- Экономическая эффективность: оптимальное сочетание затрат на обеспечение безопасности и получаемого результата.

3 Структура системы охраны

3.1 Физическая охрана:

- Ограждение периметра: прочное ограждение периметра (заборы, ворота), оснащенное системой видеонаблюдения, датчиками обнаружения вторжения, освещением.

- Контрольно-пропускные пункты (КПП): организация КПП с системой контроля доступа (СКУД), включающей турникеты, биометрическую идентификацию, металлодетекторы, досмотровое оборудование.

- Посты охраны: размещение постов охраны в стратегически важных точках для обеспечения круглосуточного наблюдения и реагирования на инциденты.
- Патрулирование: Регулярное патрулирование территории охраняемых объектов.
- Кинологическая служба: использование служебных собак для обнаружения взрывчатых веществ, наркотиков и других запрещенных предметов.
- Группы быстрого реагирования (ГБР): создание ГБР для оперативного реагирования на чрезвычайные ситуации и пресечения противоправных действий.
- Взаимодействие с правоохранительными органами: заключение соглашений о взаимодействии с полицией, Росгвардией и другими силовыми структурами.

3.2 Техническая охрана:

- Система видеонаблюдения: установка системы видеонаблюдения с камерами различного типа (внутренние, наружные, поворотные, тепловизионные), обеспечивающей круглосуточный мониторинг территории и помещений.
- Система охранной сигнализации: установка системы охранной сигнализации с датчиками обнаружения движения, разбития стекла, открытия дверей и окон, вибрации и т.д.
- Система контроля доступа (СКУД): внедрение СКУД для управления доступом сотрудников и посетителей на территорию и в помещения, включая биометрическую идентификацию.
- Противопожарная система: Установка системы пожарной сигнализации и автоматического пожаротушения.

- Система оповещения о чрезвычайных ситуациях: создание системы оповещения о чрезвычайных ситуациях (звуковое, световое оповещение, рассылка сообщений).

- Защита от кибератак: внедрение систем обнаружения и предотвращения кибератак, защита информационных систем от несанкционированного доступа.

3.3 Информационная безопасность:

- Защита информационных систем (ЗИС): установка антивирусного программного обеспечения, брандмауэров, систем обнаружения вторжений, регулярное обновление программного обеспечения.

- Контроль доступа к информации: разграничение доступа к информации на основе принципа «нулевого доверия», шифрование данных.

- Резервное копирование данных: Регулярное резервное копирование важных данных.

- Обучение персонала: Проведение обучения персонала основам информационной безопасности.

- Центр управления охраной (ЦУО):

- Мониторинг: круглосуточный мониторинг поступающей информации от всех элементов системы охраны (видеонаблюдение, сигнализация, контроль доступа).

- Анализ: Анализ информации, выявление угроз и потенциальных нарушителей.

- Принятие решений: принятие решений о реагировании на инциденты и координация действий охраны.

- Связь: Обеспечение связи между сотрудниками охраны, службами реагирования и правоохранительными органами.

- Архивирование: архивирование данных с камер видеонаблюдения и других источников информации.

4 Кадровое обеспечение:

- Подбор персонала: отбор сотрудников охраны на конкурсной основе с учетом их физических, психологических и профессиональных качеств.
- Обучение: Проведение обучения сотрудников охраны основам безопасности, специальным навыкам, правилам использования технических средств охраны, действиям в чрезвычайных ситуациях.
- Аттестация: Регулярная аттестация сотрудников охраны для проверки их профессиональной подготовки.
- Мотивация: разработка системы мотивации для сотрудников охраны, поощряющей добросовестное выполнение служебных обязанностей.

5 Документация:

- Положение о системе охраны: определение целей, задач, структуры и принципов функционирования системы охраны.
- Инструкции: Разработка инструкций для сотрудников охраны, определяющих их обязанности и порядок действий в различных ситуациях.
- Планы действий: Разработка планов действий в чрезвычайных ситуациях.
- Журналы учета: Ведение журналов учета событий, происшествий и нарушений.

6 Финансирование:

- Разработка бюджета на создание и функционирование системы охраны.
- Оценка эффективности затрат и планирование расходов.

7 Этапы реализации:

- Разработка концепции: Определение целей, задач и принципов системы охраны.
- Аудит безопасности: Проведение аудита безопасности для оценки текущего уровня безопасности.
- Разработка технического задания: Разработка технического задания на проектирование системы охраны.
- Проектирование: Разработка проектной документации.

- Закупка оборудования: Закупка оборудования и программного обеспечения.
- Монтаж и наладка: Монтаж оборудования и наладка системы охраны.
- Обучение персонала: Обучение сотрудников охраны.
- Ввод в эксплуатацию: Ввод системы охраны в эксплуатацию.
- Мониторинг и совершенствование: постоянный мониторинг работы системы охраны и ее совершенствование.

8 Рекомендации:

- Использовать передовые технологии в области безопасности.
- Привлекать к разработке и реализации системы охраны профессиональных специалистов.
- Регулярно проводить независимую оценку эффективности системы охраны.
- Обеспечить взаимодействие с правоохранительными органами.
- Учитывать специфику каждого объекта и потенциальные угрозы.
- Данные предложения являются общими и требуют детальной проработки с учетом конкретных особенностей объектов ПАО «НОВАТЭК».

Обеспечение режима охраны объектов и безопасности персонала в ПАО «НОВАТЕК» представляет собой комплексную и системную задачу, учитывающую специфику деятельности компании в сфере добычи и переработки природного газа. В условиях повышенных требований к безопасности на энергетических объектах важным аспектом является внедрение современных технологий охраны, таких как системы видеонаблюдения, контроля доступа и кибербезопасности.

ПАО «НОВАТЕК» уделяет внимание не только физической охране объектов, но и безопасности персонала, обеспечивая их обучение и информирование о правилах безопасности. Внедрение регламентированных процедур, регулярное проведение тренировок и планирование действий на

случай чрезвычайных ситуаций способствуют снижению рисков и повышению уровня безопасности на рабочих местах.

Таким образом, эффективное обеспечение режима охраны в компании требует интеграции многоуровневых мер, направленных на защиту как материальных ресурсов, так и здоровья и жизни сотрудников. Применение современных технологий и методов управления безопасностью является залогом устойчивой работы компании в условиях меняющихся вызовов и угроз в отрасли [2].

Библиографический список:

1. Байрамшин Т.А. Принципы и элементы охраны труда на предприятиях нефтегазовой отрасли России // Экономика и бизнес. 2021. № 1 (64). С. 105- 111.
2. Беляков, Г. И. Охрана труда и техника безопасности: учебник для среднего профессионального образования / Г. И. Беляков. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 740 с.
3. Минаева И.А., Газизов В.Р. Формирование эффективной культуры безопасности в отрасли как направление совершенствования системы охраны труда на предприятиях нефтегазовой отрасли // Безопасность труда в промышленности. 2008. № 8. С. 48-52.
4. Ответственность и развитие. Отчет об устойчивом развитии 2023 // www.novatek.ru URL: <https://www.novatek.ru/ru/esg/?ysclid=m81fpyzg7p462238261> (дата обращения: 29.03.2025).
5. Федосов А. В., Вадулина Н. В., Шабанова В. В., Абдрахманова К. Н. Особенности организации промышленной безопасности и охраны труда на предприятиях нефтегазовой отрасли // Проблемы сбора, подготовки и транспорта нефти и нефтепродуктов. 2017. № 4 (110). С. 193–201.

Оригинальность 76%