Гимранов Р.Д.[1]

[1] Публичное акционерное общество «Сургутнефтегаз», Сургут, Россия

Группировка угроз и рисков экономической безопасности цифрового предприятия нефтегазовой отрасли: ситуационный подход

ЦИТИРОВАТЬ СТАТЬЮ:

Гимранов Р.Д. Группировка угроз и рисков экономической безопасности цифрового предприятия нефтегазовой отрасли: ситуационный подход // Креативная экономика. — 2020. — Том 14. — № 7. — С. 1291-1310. doi: 10.18334/ce.14.7.110684

АННОТАЦИЯ:

Цифровая трансформация предприятий, с одной стороны, обеспечивает конкурентные преимущества на рынке, с другой стороны, является вызовом, ставящим под угрозу само существование предприятия. Нефтегазовый сектор российской экономики, сформировавшийся в советский период, отличается институциональным консерватизмом и входит в эпоху цифровых технологий достаточно инертно. Тем не менее некоторых лидеров отрасли уже можно назвать цифровыми предприятиями. Статья раскрывает особенности цифрового предприятия сквозь призму уязвимости процессов. Отмечено, что цифровая трансформация порождает новые угрозы и риски экономической безопасности. Выделены основные специфические угрозы и риски цифрового предприятия, а также специфические отраслевые угрозы и риски цифрового предприятия нефтегазовой отрасли. На основе определения риска как ситуативной характеристики деятельности предприятия предложено применять ситуационный подход к группировке угроз и рисков экономической безопасности цифрового предприятия. Представлена классификация угроз и рисков экономической безопасности цифрового предприятия нефтегазовой отрасли при нестабильной ситуации, которая может быть использована в качестве инструмента управления экономической безопасностью цифрового предприятия нефтегазовой отрасли.

КЛЮЧЕВЫЕ СЛОВА: цифровая трансформация, угрозы и риски, экономическая безопасность, цифровое предприятие, нефтегазовая отрасль, ситуационный подход

ОБ АВТОРЕ

Гимранов Ринат Дамирович, начальник управления информационных технологий (gimranov_rd@mail.ru)

издательство КРЕАТИВНАЯ ЭКОНОМИКА

creativeconomy.ru

Gimranov R.D.[1]

[1] «Surgutneftegas» PJSC, Russia

ISSN 1994-6929

Grouping threats and risks to economic security of a digital enterprise in the oil and gas industry: situational approach

CITE AS:

Gimranov R.D. (2020) Gruppirovka ugroz i riskov ekonomicheskoy bezopasnosti tsifrovogo predpriyatiya neftegazovoy otrasli: situatsionnyy podkhod [Grouping threats and risks to economic security of a digital enterprise in the oil and gas industry: situational approach]. *Kreativnaya ekonomika. 14*. (7). — 1291-1310. doi: 10.18334/ce.14.7.110684

ABSTRACT:

Digital transformation of enterprises, on the one hand, provides competitive advantages in the market, on the other hand, it is a challenge that threatens the very existence of the enterprise. The oil and gas sector of the Russian economy, which was formed during the Soviet period, is characterized by institutional conservatism, and enters the era of digital technologies rather inertly. However, some industry leaders can already be called digital enterprises. The authors of the article reveal the features of a digital enterprise through the prism of process vulnerabilities. It is noted that digital transformation creates new threats and risks to economic security. The main specific threats and risks of a digital enterprise are highlighted. Specific industry-specific threats and risks of a digital enterprise in the oil and gas industry are identified. Based on the definition of risk as a situational characteristic of an enterprise, it is proposed to apply a situational approach to grouping threats and risks to the economic security of a digital enterprise. The classification of threats and risks to economic security of a digital enterprise in the oil and gas industry with an unstable situation is given. This classification be used as a tool of economic security management of the digital oil and gas companies.

KEYWORDS: digital transformation, threats and risks, economic security, digital enterprise, oil and gas industry, situational approach

JEL Classification: O33, G32, L86, L71

Received: 10.07.2020 / **Published:** 31.07.2020
© Author(s) / Publication: CREATIVE ECONOMY Publishers
For correspondence: Gimranov R.D. (gimranov_rd@mail.ru)

ФИНАНСИРОВАНИЕ:

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-47-860008 р_а.

Введение

Вопросы обеспечения экономической безопасности и экономического роста предприятий нефтегазовой отрасли приобретают особую актуальность в силу усиления волатильности на рынке углеводородов в пока безальтернативном сценарии наполнения государственного бюджета России. На экономическую безопасность предприятий нефтегазовой отрасли оказывает влияние общеэкономическая ситуация в стране и в мире. Глобальным вызовом для предприятий нефтегазовой отрасли является тенденция цифровой трансформации лидеров отрасли. Цифровая трансформация предприятий подразумевает техническое, технологическое и организационное развитие, при этом генерирует новые, ранее неизвестные угрозы и риски их экономической безопасности. Группировка угроз и рисков экономической безопасности цифрового предприятия нефтегазовой отрасли позволяет построить систему обеспечения его экономической безопасности с учетом особенностей новых форм экономических отношений, возникающих в процессе его деятельности. Применение ситуационного подхода к группировке угроз и рисков экономической безопасности цифрового предприятия нефтегазовой отрасли обусловлено возможностью связать концепцию управления предприятием с конкретными ситуациями на разных этапах его жизненного цикла для обеспечения его стабильной работы и развития.

Цель исследования — выделить угрозы и риски экономической безопасности цифрового предприятия нефтегазовой отрасли и представить их классификацию с позиции ситуационного подхода.

В целях обоснования результатов исследования в работе использованы научные обзоры и труды отечественных и зарубежных авторов в области цифровой экономики и цифровой трансформации предприятий, угроз и рисков экономической безопасности предприятия.

Методологическую базу исследования составили общенаучные методы анализа и синтеза, индукция, дедукция, сравнение, методы научной абстракции, группировка, обобщение, формализация, систематизация, теория и методология ситуационного подхода.

Цифровая экономика и цифровая трансформация предприятий

Появление и распространение цифровых технологий определяют направления развития экономики и приводит к кардинальным изменениям для хозяйствующих субъектов. Анализ публикаций, посвященных понятийному

creativeconomy.ru

ISSN 1994-6929

аппарату цифровой экономики, позволяет говорить о формировании как минимум двух подходов к ее определению:

1) узкий подход, предполагающий, что цифровая экономика представляет собой экономику, основанную на цифровых технологиях производства товаров, выполнения работ и оказания услуг;
2) расширенный подход, согласно которому цифровая экономика — это «экономическое устройство, в котором товары и услуги производятся с преобладающим использованием цифровых технологий, а данные в цифровой форме являются ключевым фактором производства продукции и оказания услуг» [1, с. 28] (*Abroskin, Zaytsev, Idrisov, 2019, p. 28*).

Второе определение закреплено в государственной программе «Цифровая экономика» и в экспертном сообществе также подвергается критике за узость. По нашему мнению, широкий подход может быть в том, что цифровая экономика предполагает как выпуск продуктов, товаров и услуг в цифровой или гибридной форме, так и использование цифровых средств производства и управления предприятием. Например, каждая партия нефти выпускается с цифровым сертификатом качества, и для ее добычи используются цифровые модели, и производство управляется цифровыми бизнес-процессами, включая вспомогательные и дополнительные процессы.

Основой цифровой экономики являются информационно-коммуникационные технологии. Внедрение информационно-коммуникационных технологий на предприятиях способствовало их цифровой трансформации. Первоначально под цифровой трансформацией понимался переход от аналоговых данных к цифровым, т.е. так называемая цифровизация. Этот процесс привел к кардинальным изменениям на уровне хозяйствующих субъектов, позволив повысить производительность труда в определенный период времени с помощью перехода на новые прорывные цифровые технологии. Особого внимания заслуживают так называемые технологии третьей платформы (облако, мобильность, большие данные). Существует мнение, согласно которому именно технологии третьей платформы привели к цифровой трансформации предприятий, а предыдущие технологии лишь прокладывали путь к будущей трансформации [2]. Предыдущие технологии не изменяли принципиально организацию социально-экономических отношений на предприятии, не создавали платформы интеграции и взаимодействия всех участников отношений. Они лишь поддерживали существующие бизнес-модели при помощи фиксации процессов в электронном виде, обеспечения неизменности данных, высокой надежности их сохранности.

Находясь в конкурентной среде, действующим предприятиям приходится быстро адаптироваться, оптимизировать и менять бизнес-стратегии и бизнес-

процессы, подстраиваясь под быстро меняющиеся условия. Цифровая трансформация в данном случае является: 1) необходимостью, обеспечивающей конкурентные преимущества на рынке; 2) вызовом, ставящим под угрозу само существование предприятия. Первое достигается за счет изменения бизнес-модели, снижения транзакционных издержек с помощью перехода на полностью управляемый и прозрачный процесс производства. Второе сопряжено с необходимостью преодоления ряда проблем:

- административные: несоответствие действующего отраслевого регулирования потребностям нового технологического уклада и отсутствие единых стандартов, ограничения на закупку иностранного оборудования и программного обеспечения при отсутствии отечественных аналогов [3];
- финансовые: необходимость отвлечения и инвестирования значительного объема финансовых ресурсов для внедрения цифровых технологий;
- недостаток достоверной информации, который оказывает влияние на низкий уровень доверия к цифровым технологиям и выгодам от их внедрения, низкий уровень готовности хозяйствующих субъектов к адаптации цифровых технологий [3];
- нехватка высококвалифицированных специалистов;
- отсутствие мотивации руководящего звена предприятия, необходимость повышения его цифровой грамотности, особенно в капиталоемких отраслях промышленности.

Глобальный характер перечисленных выше проблем объясняет тот факт, что промышленные предприятия до цифровой эпохи с большой долей консерватизма принимают решения о переходе на «цифру». Этот тезис подтверждается узким кругом компаний, получивших положительный опыт комплексного перехода в цифровой формат. Выбор набора технологий, способных решить сложившиеся проблемы, зависит от отраслевой принадлежности хозяйствующего субъекта.

Важными технологиями с точки зрения цифровой трансформации для нефтегазовой отрасли являются промышленный «Интернет вещей», большие данные, распределенный реестр и блокчейн, облачные технологии, аддитивное производство, искусственный интеллект (технологии интеллектуальных скважин, месторождений, «безлюдные» технологии (Robotic process automation), позволяющие заменить часть человеческого труда роботами). Цифровая трансформация предприятий нефтегазовой отрасли нацелена на снижение эксплуатационных затрат и увеличение объема извлекаемых запа-

creativeconomy.ru

ISSN 1994-6929

сов углеводородов на действующих месторождениях. Так, внедрение цифровых технологий позволяет повысить коэффициент извлечения нефти до 50% в сравнении со средним общемировым 30% [4, с. 47] (*Eryomin, Dmitrievskiy, Tikhomirov, 2015*).

Результатом цифровой трансформации является появление цифрового предприятия. *Цифровое предприятие — это предприятие с новой организацией деятельности, с созданной цифровой платформой интеграции и взаимодействия всех участников на протяжении всего жизненного цикла предприятия.*

Под цифровой платформой понимается «совокупность цифровых данных, моделей и инструментов, информационно и технологически интегрированных в единую автоматизированную функциональную систему, предназначенную для эффективного управления целевой предметной областью с организацией взаимодействия заинтересованных субъектов» [5]. Суть цифрового предприятия заключается в одновременном присутствии цифрового двойника выпускаемого продукта и цифрового двойника предприятия [5].

Ключевым ресурсом цифрового предприятия является цифровой капитал. Цифровой капитал в рамках настоящей работы можно определить как цифровой двойник капитала физического предприятия, прошедшего цифровую трансформацию. В его структуре выделим информационный капитал, человеческий и организационный капиталы. В зависимости от подхода (функциональный, системный, процессный, ситуационный и т.п.), структура цифрового капитала может быть представлена разным набором составляющих.

Информационный капитал определим как совокупность баз данных, информационных систем, коммуникаций, технологий. Основу информационного капитала составляют бизнес-приложения, инфраструктура и сервисы [6, с. 221].

Под человеческим капиталом цифрового предприятия понимаем опыт, знания, навыки, компетенции, творческие способности его трудовых ресурсов.

Под организационным капиталом цифрового предприятия понимаем совокупность организационных способностей и возможностей предприятия, полученных в результате рационального использования потенциала трудовых ресурсов и ИТ-активов.

Цифровое предприятие характеризует ряд особенностей:

1) фокус в автоматизации сдвигается с учета и контроля на взаимодействие и интеграцию;
2) меняется подход к автоматизации процессов: приоритет сквозной автоматизации и интеграции процессов на основе гибких BPM-платформ, решений BI, омниканальных фронт-офисных систем [7] (*Yapparov, 2017*);

3) дополняется информационная инфраструктура предприятия: используется не только локальная, но и облачная, формируется гибридный ИТ-ландшафт;
4) видоизменяется контент: все данные оцифрованы, в т.ч. неструктурированные.

Цифровые предприятия создают целостную систему, в которой размыты границы между цепочкой поставки, производства, исполнителями, контрагентами и конечными потребителями. Они используют цифровые технологии для институциональных улучшений бизнес-моделей и отдельных бизнес-процессов. Здесь они сталкиваются с проблемой несоответствия существующих систем, способов защиты данных применяемым цифровым технологиям. Технологии защиты данных имеют большое количество ограничений и не успевают за развитием цифровых технологий, применяемых в производственном процессе цифрового предприятия. Проблематика существующих систем защиты данных состоит в фокусе исключительно на инцидентах в рамках конкретной защищаемой системы, направленности атак на эксплуатацию уязвимостей бизнес-логики, а не на преодоление систем защиты, а также вероятности моментального повторения ошибки в множестве экземпляров [8]. Бизнес-процессы остаются уязвимыми, системы защиты не способны защитить процессы. Под влиянием этих обстоятельств возникают различные угрозы и риски экономической безопасности цифрового предприятия.

Угрозы и риски в системе экономической безопасности цифрового предприятия

Обычно угроза определяется как прямая или косвенная вероятность нанесения ущерба. В общем смысле безотносительно к сфере возникновения угрозу можно определить как «совокупность факторов и условий, способствующих реализации опасности для конкретного объекта в определенный момент или интервал времени» [9, с. 9] (*Krivorotov, Kalina, Eriashvili, 2015, p. 9*).

Угрозы экономической безопасности предприятия можно определить как совокупность условий и факторов, создающих прямую или косвенную возможность нанесения ущерба ресурсам и капиталу предприятия. Специфические угрозы базируются на вышеописанных особенностях цифрового предприятия (табл. 1).

Включив отраслевую принадлежность цифрового предприятия к нефтегазовой отрасли, приходим к выводу, что угроза представляет собой совокупность условий и факторов, создающих прямую или косвенную возможность нанесения ущерба цифровому капиталу предприятия нефтегазовой отрасли.

creativeconomy.ru

ISSN 1994-6929

Таблица 1

Специфические угрозы экономической безопасности цифрового предприятия

Специфические угрозы экономической безопасности цифрового предприятия		
Информационный капитал	Организационный капитал	Человеческий капитал
Неэффективное использование информационно — коммуникационных технологий	«Схлопывание» уровней структуры при снижении барьеров и задержек при распространении информации	Понижение уровня компетентности персонала при применении новых цифровых технологий
Присутствие «незрелых» цифровых технологий, использование несовершенных технологий и каналов коммуникации	Диверсии, аварии, кибератаки, виртуальные ограбления	Психологическое неприятие цифровых технологий работниками различных уровней
Изменения в законодательстве в области информации, цифровых технологий, лицензий и патентов, в отношениях интеллектуальной собственности	Вытеснение человека из системы управления, появление искусственного интеллекта, роботизация	Неспособность персонала ориентироваться в быстро изменяющихся условиях, консерватизм мышления
Выход из строя машин и оборудования, нарушения техники безопасности		
Рост технологической зависимости от зарубежных поставщиков цифровых технологий		

Источник: составлено автором.

К основным специфическим отраслевым угрозам экономической безопасности цифрового предприятия нефтегазовой отрасли относятся следующие:

- изменение нормативно-правовой базы нефтегазовой отрасли в части установления требований к информационным системам и программному обеспечению нефтегазового комплекса;
- сложности перехода к умным скважинам и цифровым месторождениям в связи с концентрацией углеводородного сырья в трудноизвлекаемых запасах;
- дефицит высококвалифицированных специалистов, ответственных за обслуживание оборудования поточных анализаторов, датчиков, позволяющих контролировать характеристики углеводородного сырья и нефтегазовой продукции в реальном времени;

- «незрелость» виртуальных анализаторов качества углеводородного сырья и нефтегазовой продукции, систем интеллектуального управления промыслом и другие.

В теории безопасности выделяют еще одну категорию, напрямую связанную с угрозой, — это риск. Риск — это ситуативная характеристика деятельности предприятия, которая состоит в неопределенности ее исхода и вероятности наступления отрицательных последствий в результате неуспеха.

Для цифрового предприятия риск представляет собой вероятность наступления отрицательных последствий в результате реализации угроз для цифрового капитала предприятия в различных ситуациях (стабильной, нестабильной, критической).

Специфические риски цифрового предприятия обусловлены специфическими угрозами (табл. 2).

Отраслевая принадлежность цифрового предприятия также находит отражение в классификации рисков цифрового предприятия. Для нефтегазового предприятия к основным отраслевым рискам можно отнести:

- риск увеличения затрат на внедрение цифровых технологий в связи с изменением нормативно-правовой базы нефтегазовой отрасли в части установления требований к информационным системам и программному обеспечению нефтегазового комплекса;
- риск потери контроля и управления умными скважинами и цифровыми месторождениями из единого центра:
- риск поломки, отказа оборудования поточных анализаторов, датчиков, которые позволяют контролировать характеристики углеводородного сырья и нефтегазовой продукции в реальном времени;
- риск некачественного прогнозирования показателей углеводородного сырья без их фактического замера на основании ранее выполненных лабораторных тестов при помощи виртуальных анализаторов;
- риск принятия неверных решений вследствие неверных выводов о работе оборудования, о необходимых геолого-технических мероприятиях, о балансировке ресурсов, сделанных искусственным интеллектом, и другие.

Приведем пример угроз и рисков цифрового предприятия нефтегазовой отрасли. В настоящее время в стране растет число месторождений с трудными условиями бурения, с аномальными показателями температур и давления, сейсмической активности, специфики расположения пластов. Помимо этого, растут показатели глубины бурения скважин, в России средние значения уже превысили 3 500 метров и продолжают расти [10]. В такой ситуации

creativeconomy.ru

ISSN 1994-6929

Таблица 2

Специфические риски экономической безопасности цифрового предприятия

Специфические риски экономической безопасности цифрового предприятия		
Информационный капитал	Организационный капитал	Человеческий капитал
Риск нарушения информационной безопасности (информационно-технического воздействия на информационную инфраструктуру хозяйствующего субъекта в политических и экономических целях)	Риск искажения, потери данных	Риск снижения качества и эффективности работы персонала
Инновационный риск в виде появления новых вирусов, уязвимостей	Риск уязвимости предприятия в связи с вероятностью раскрытия конфиденциальной корпоративной информации, киберриски	Риск дефицита высококвалифицированных специалистов
	Риск заменяемости экспертов роботами, исчезновения ряда профессий	Риск возрастания социальной напряженности в коллективе предприятия
	Риск недостаточных внутренних сетевых коммуникаций в связи с несовершенным интерфейсом различных программ	Риск «клипового» мышления персонала, который заключается в фрагментарном восприятии производственного процесса как набора различных фрагментов, невникании в суть постоянно появляющейся новой информации
	Риск нерациональной оптимизации численности персонала	Трудная предсказуемость действий работников, рассогласование поведения и взаимодействия персонала
	Риск принятия единоличных ошибочных решений, ведущих к потере позиций на рынке и возможному банкротству	

Источник: составлено автором.

основной угрозой является сложность перехода к умным скважинам в связи с потребностью применения новых технологий и автоматизированного оборудования сопутствующих компонентов, создания наклонно-направленных и горизонтальных скважин, их укрепления, а также обеспечения безопасности работников.

В процессе добычи углеводородов цифровые предприятия нефтегазовой отрасли зачастую используют технологию промышленного «Интернета вещей». В нефтегазовой сфере промышленный «Интернет вещей» представляет собой экосистему, направленную на поддержание зависимости между производственным процессом, внутрифирменным управлением и средствами внешнего взаимодействия. Эволюционируя от конвергенции различных технологий, промышленный «Интернет вещей» разрушил стены между операционными технологиями и информационными технологиями. Это означает, что неструктурированные, созданные машиной данные могут быть проанализированы для получения информации, которая способствует улучшению проектирования, выполнения и приводит к более быстрому принятию решений. Основными рисками, связанными с интеграцией и конвергенцией операционных и информационных технологий, являются инновационный риск в виде новых вирусов, киберриски, риски некачественного прогнозирования показателей углеводородного сырья без их фактического замера при помощи виртуальных анализаторов и риски принятия неправильных управленческих решений.

Группировка угроз и рисков экономической безопасности цифрового предприятия

Для обеспечения экономической безопасности цифрового предприятия требуется готовность внутреннего потенциала хозяйствующего субъекта к противостоянию появления, проникновения дестабилизирующих факторов. Существующие подходы к группировке угроз и рисков экономической безопасности не отражают учет ситуаций, возникающих в процессе производственной деятельности цифрового предприятия. В связи с этим представляется интересной попытка сгруппировать угрозы и риски экономической безопасности цифрового предприятия с позиции ситуационного подхода.

Исходя из этого, угрозы и риски экономической безопасности цифрового предприятия следует рассматривать в трех видах ситуаций:

1) в стабильной ситуации;
2) в нестабильной ситуации;
3) в критической (чрезвычайной) ситуации.

creativeconomy.ru

ISSN 1994-6929

Переход из стабильной ситуации в нестабильную или критическую характеризуется потерей предсказуемости реакции объекта на управленческое воздействие. В нестабильной ситуации принятие и реализация управленческих решений проходит со скоростью развития самих ситуаций. Критической ситуации присущи уникальность и дефицит информации, знаний, времени; ценой ошибки является дальнейшая судьба предприятия.

Учет особенностей различных ситуаций важен для группировки классификационных признаков угроз и рисков экономической безопасности цифрового предприятия с позиции ситуационного подхода (рис. 1).

Угрозы экономической безопасности цифрового предприятия с позиции ситуационного подхода практически одинаково классифицируются при разных ситуациях:

1) при нестабильной и критической ситуации классификация происходит по источнику возникновения (внешние, внутренние), по природе возникновения (объективные, не зависящие от человека; субъективные, обусловленные человеческой деятельностью; смешанные), по времени воздействия (кратко-, средне-, долгосрочные);
2) при стабильной ситуации классификация угроз расширяется на дополнительный классификационный признак — прогнозируемость. Именно в условиях стабильности и определенности возможно выделить прогнозируемые и непрогнозируемые угрозы.

Риски экономической безопасности цифрового предприятия в стабильной ситуации классифицируются:

1) по сферам реализации (имущественные риски; финансовые; технические; технологические; информационные; экологические; риски, связанные с работой персонала с организационной структурой предприятия, и другие);
2) по ожидаемым результатам (спекулятивный, чистый);
3) по возможности предотвращения (предотвратимые, непредотвратимые);
4) по времени возникновения (ретроспективные, текущие, перспективные).

Разделение рисков по сферам реализации и по ожидаемым результатам возможно и в нестабильной ситуации. Кроме того, в нестабильной ситуации риски экономической безопасности классифицируются по следующим критериям:

1) по масштабам локализации (локальный, глобальный);
2) по длительности воздействия (кратковременный, длительный);
3) по уровню новизны (повседневный, инновационный).

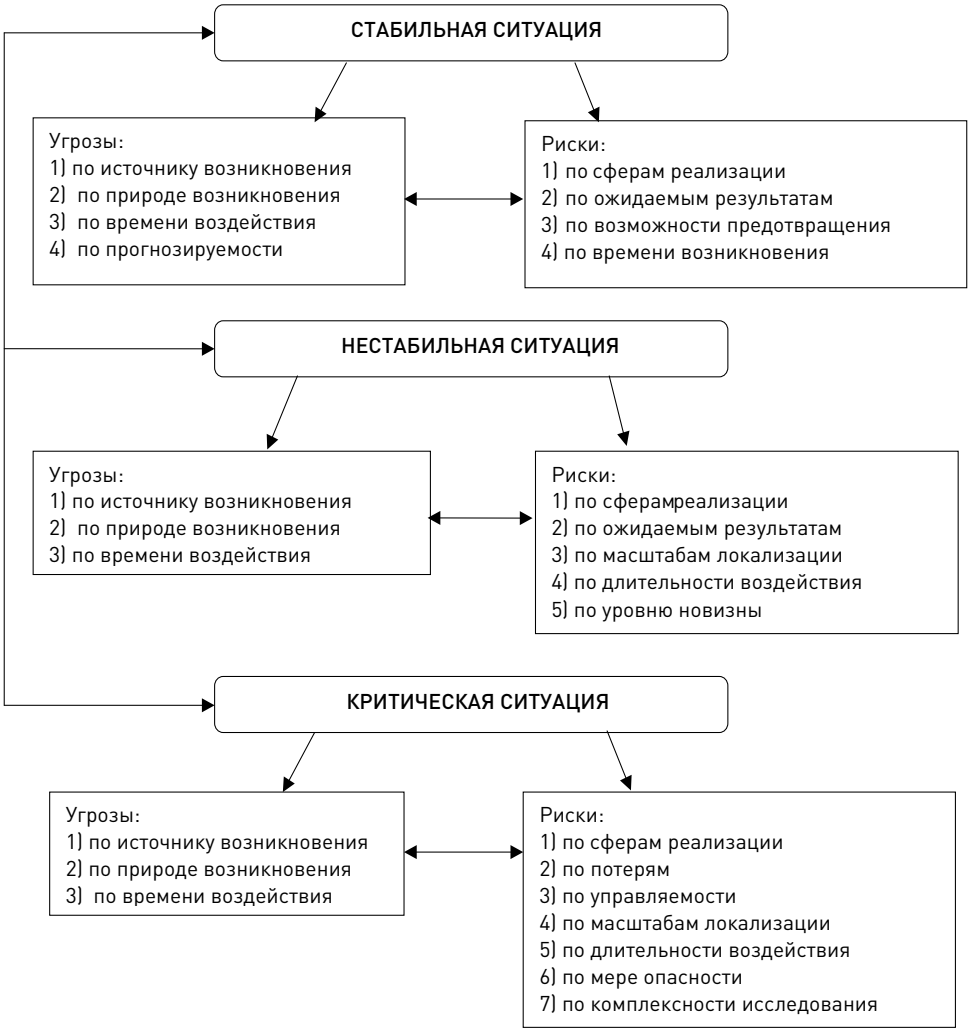


Рисунок 1. Группировка классификационных признаков угроз и рисков экономической безопасности цифрового предприятия с позиции ситуационного подхода

Источник: составлено автором.

В качестве уникальных классификационных признаков деления рисков экономической безопасности цифрового предприятия в критической ситуации выделяем:

1) потери (экономические потери, потери упущенной выгоды, потери контроля производства, объектов нефтегазовой инфраструктуры, управления запасами и активами);

creativeconomy.ru

ISSN 1994-6929

2) управляемость (управляемый, неуправляемый риски);
3) мера опасности (приемлемый риск, ущерб при реализации которого минимален; критический риск, при котором ущерб сказывается на деятельности предприятия, однако не парализует его деятельность; фатальный риск, при котором останавливается деятельность предприятия или ликвидируется хозяйствующий субъект);
4) комплексность исследования (простой риск, который не расчленяется на подвиды; сложный риск, который состоит из комплекса подвидов).

Отраслевые особенности угроз и рисков экономической безопасности цифрового предприятия нефтегазовой отрасли возможно раскрыть по предложенным классификационным признакам с позиции ситуационного подхода.

Угрозы и риски экономической безопасности цифрового предприятия нефтегазовой отрасли при нестабильной ситуации представлены в таблицах 3 и 4.

Таблица 3

Классификация угроз экономической безопасности цифрового предприятия нефтегазовой отрасли при нестабильной ситуации

Наименование классификационного признака, виды угроз	Описание угроз
По источнику возникновения:	
1) внешние угрозы	Изменения в законодательстве в области информации, цифровых технологий, лицензий и патентов, кибератаки, обнаружение меньшего запаса нефтегазовых ресурсов, чем планировалось
2) внутренние угрозы	Ошибки и злоупотребления работниками служебным положением, раскрытие корпоративных данных, конфиденциальной информации, снижение качества и эффективности работы персонала
По природе возникновения:	
1) объективные угрозы	Концентрация месторождений углеводородов в трудных климатических условиях, истощение минерально-сырьевой базы, тупиковые ветви развития предприятия вследствие применения «незрелых» цифровых технологий
2) субъективные угрозы	Сознательное искажение или порча информации, кража и передача конкурентам стратегически важных данных, увеличение количества ошибок и сбоев в связи с повышением требований к квалификации персонала для цифровых технологий
3) смешанные угрозы	Появление значительного объема «информационного мусора» в связи со способностью цифровых систем порождать огромные потоки различной информации

Наименование классификационного признака, виды угроз	Описание угроз
По времени воздействия:	
1) краткосрочные угрозы	Утечки, аварийные розливы углеводородов
2) среднесрочные угрозы	Возгорания, поломки машин и оборудования
3) долгосрочные угрозы	Финансовые потери от неграмотного использования цифровых технологий оперативного размещения свободных средств предприятия

Источник: составлено автором.

Таблица 4

Классификация рисков экономической безопасности цифрового предприятия нефтегазовой отрасли при нестабильной ситуации

Наименование классификационного признака, виды рисков	Описание рисков
По сферам реализации:	
1) имущественные риски	Увеличение расходов на ремонт, оплату простоев, компенсации работникам
2) финансовые риски	Снижение уровня ликвидности, риски нарушения обязательств по уплате налогов и обязательных платежей в бюджеты различных уровней бюджетной системы РФ
3) технологические риски	Нарушение цикла производства или отказ отдельных производственных процессов
4) технические риски	Отключение электричества, недостаточные внутренние сетевые коммуникации, обмен информацией из-за неудобных интерфейсов программ
По ожидаемым результатам:	
1) спекулятивные риски	Изменение стоимости цифрового капитала, утечка данных, киберриски, репутационные риски
2) чистые риски	Риск неоткрытого месторождения, открытия нерентабельного месторождения, риск неточного определения характеристик объекта разработки (объема запасов, уровня нефтегазоизвлечения, объема извлекаемых запасов, динамики добычи углеводородов)

creativeconomy.ru

ISSN 1994-6929

Наименование классификационного признака, виды рисков	Описание рисков
По масштабам локализации:	
1) локальные риски	Увеличение затрат на цифровые технологии, снижение прибыли предприятия
2) глобальные риски	Проблемы в управлении производственными процессами и обеспечении учета вплоть до полной парализации деятельности предприятия в случае реализованной кибератаки
По длительности воздействия:	
1) кратковременные риски	Повышение вероятности отказа оборудования, сбоя систем, принятия ошибочных управленческих решений
2) длительные риски	Утрата прав на объекты имущества, снижение ожидаемого уровня возврата инвестиций в проектах по цифровой трансформации
По уровню новизны:	
1) повседневные риски	Увеличение трансакционных издержек, связанных с оппортунистическим поведением персонала разного уровня, применяющего цифровые технологии
инновационные риски	Снижение качества управленческих решений вплоть до потери устойчивости управления, замены работников роботами

Источник: составлено автором.

Отметим, что внешние и внутренние угрозы экономической безопасности цифрового предприятия нефтегазовой отрасли при нестабильной ситуации взаимосвязаны между собой. Так:

- изменения в законодательстве в области информации, цифровых технологий, лицензий и патентов связаны с ошибками и злоупотреблением работниками служебным положением;
- кибератаки чреваты раскрытием корпоративных данных, конфиденциальной информации;
- обнаружение большего запаса нефтегазовых ресурсов, чем планировалось, может оказать влияние на снижение качества и эффективности работы персонала.

Заключение

Резюмируя, скажем, что в нынешних условиях хозяйствования возникает необходимость менять парадигму экономической безопасности цифрового предприятия нефтегазовой отрасли. Представляется целесообразным защищать весь бизнес-процесс, а не отдельные его системы или сервисы. В первую очередь требуется получить измеряемые свойства процесса путем измерения отдельных его составляющих и их жизненного цикла. Во-вторых, определить соответствие составляющих процесса условному эталонному процессу. В-третьих, определить легитимность процесса путем сличения предшествующих ему событий или процессов. Эти действия будут способствовать возможности превентивного выявления угроз и рисков, не допуская реализации действий, способных нанести значительный ущерб экономической безопасности цифрового предприятия нефтегазовой отрасли.

В рамках ориентации на обеспечение экономической безопасности цифрового предприятия нефтегазовой отрасли возникает потребность в группировке и классификации угроз и рисков. Представленная группировка и классификация угроз и рисков экономической безопасности цифрового предприятия нефтегазовой отрасли с позиции ситуационного подхода, во-первых, дополняет существующие классификации и дает развернутое представление угроз и рисков экономической безопасности цифрового предприятия нефтегазовой отрасли в различных ситуациях, во-вторых, облегчает процесс управления рисками, способствует выработке действий и мер по предотвращению возникновения рисков, минимизации их негативных последствий, в-третьих, является основой для построения модели экономической безопасности цифрового предприятия нефтегазовой отрасли, а также организации ее мониторинга.

Отметим, что предложенная группировка угроз и рисков весьма универсальна и может быть адаптирована к предприятиям других отраслей экономики. ■

creativeconomy.ru

ИСТОЧНИКИ:

1. Аброскин А.С., Зайцев Ю.К., Идрисов Г.И. Экономическое развитие в цифровую эпоху. — М.: Издат. дом «Дело», 2019. — 88 с.
2. Galen Gruman What digital transformation really means. Infoworld.com. [Электронный ресурс]. URL: https://www.infoworld.com/article/3080644/what-digital-transformation-really-means.html (дата обращения: 10.06.2020).

ISSN 1994-6929

3. Цифровая трансформация предприятий сталкивается с 4 вызовами. Ac.gov.ru. [Электронный ресурс]. URL: https://ac.gov.ru/news/page/cifrovaa-transformacia-predpriatij-stalkivaetsa-s-4-vyzovami-25080 (дата обращения: 20.06.2020).
4. Ерёмин Н.А., Дмитриевский А.Н., Тихомиров Л.И. Настоящее и будущее интеллектуальных месторождений // Нефть. Газ. Новации. — 2015. — № 12. — с. 45-50.
5. Голышко А. Разные грани цифрового предприятия. Habr.com. [Электронный ресурс]. URL: https://habr.com/ru/post/353864 (дата обращения: 22.04.2020).
6. Bughin J., Manyika J. Measuring the full impact of digital capital. Mckinsey.com. [Электронный ресурс]. URL: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/measuring-the-full-impact-of-digital-capital (дата обращения: 02.07.2020).
7. Яппаров Т. Цифровая трансформация: шансы и угрозы. Государство и ИТ-бизнес. [Электронный ресурс]. URL: https://www.crn.ru/numbers/reg-numbers/detail.php?ID=117484 (дата обращения: 21.06.2020).
8. Мананников Д. Необходимость изменения парадигмы безопасности в условиях цифровизации экономики. Econ.msu.ru. [Электронный ресурс]. URL: https://www.econ.msu.ru/sys/raw.php?o=56901&p=attachment (дата обращения: 21.06.2020).
9. Криворотов В.В., Калина А.В., Эриашвили Н.Д. Экономическая безопасность государства и регионов. — М.: ЮНИТИ-ДАНА, 2015. — 351 с.
10. Умные скважины и интеллектуальные месторождения. Нефть в цифре. Портал для недропользователей. [Электронный ресурс]. URL: https://dprom.online/oilngas/umnye-skvazhiny-i-intellektualnye-mestorozhdeniya-neft-v-tsifre (дата обращения: 27.06.2020).
11. О стратегии национальной безопасности Российской Федерации: указ Президента РФ от 31.12.2015 г. №683. Консультант Плюс. [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_191669 (дата обращения: 10.06.2020).
12. О Стратегии экономической безопасности Российской Федерации на период до 2030 года: указ Президента РФ от 13.05.2017 г. №208. Консультант Плюс. [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_216629 (дата обращения: 10.06.2020).
13. Счетная палата Российской Федерации. Аудит национальных целей. Исполнение расходов бюджета на нацпроекты за пять месяцев составило 29%. Gov.ru. [Электронный ресурс]. URL: http://audit.gov.ru/audit-national/ispolnenie-raskhodov-byudzheta-na-natsproekty-za-5-mesyatsev-sostavilo-29 (дата обращения: 25.06.2020).
14. Максимов А.А. Разработка системы показателей экономической безопасности предприятий атомной отрасли. / дис. ... к. э. н. — Санкт-Петербург, 2019. — 148 с.

15. Клири Ш. Глобальные риски. Деловой успех в неспокойные времена. — М.: Вопросы экономики, 2011. — 223 с.
16. Толковый словарь Ожегова. [Электронный ресурс]. URL: https://slovarozhegova.ru/word.php?wordid=27127 (дата обращения: 17.05.2020).
17. Процессный подход. Менеджмент качества. Kpms.ru. [Электронный ресурс]. URL: https://www.kpms.ru/General_info/Process_approach.htm (дата обращения: 03.06.2020).
18. Альтшулер А.И., Кузнецова Ю.В. Особенности системного подхода в теории организации. Hse.ru. [Электронный ресурс]. URL: https://www.hse.ru/data/2010/10/23/1222828015 (дата обращения: 03.06.2020).
19. Копылова Е.А. Возможности применения ситуационного подхода к анализу системы управления организацией // Экономика и менеджмент инновационных технологий. — 2014. — № 2(29). — с. 26.
20. Гимранов Р.Д., Лугачев М.И., Тищенко С.А. и др. Качественный анализ основных направлений исследования онтологии бизнес-процессов предприятия // Проблемы теории и практики управления. — 2019. — № 11. — с. 137-168.

REFERENCES:

Abroskin A.S., Zaytsev Yu.K., Idrisov G.I. (2019). *Ekonomicheskoe razvitie v tsifrovuyu epokhu* [Economic development in the digital age] M.: Izdat. dom «Delo». (in Russian).

Bughin J.,Manyika J. Measuring the full impact of digital capitalMckinsey.com. Retrieved July 02, 2020, from https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/measuring-the-full-impact-of-digital-capital

Eryomin N.A., Dmitrievskiy A.N., Tikhomirov L.I. (2015). *Nastoyashchee i budushchee intellektualnyh mestorozhdeniy* [Present and future of intellectual fields]. *Neft. Gaz. Novatsii.* (12). 45-50. (in Russian).

Galen Gruman What digital transformation really meansInfoworld.com. Retrieved June 10, 2020, from https://www.infoworld.com/article/3080644/what-digital-transformation-really-means.html

Gimranov R.D., Lugachev M.I., Tischenko S.A. i dr. (2019). *Kachestvennyy analiz osnovnyh napravleniy issledovaniya ontologii biznes-protsessov predpriyatiya* [The qualitative analysis of basic directions research of enterprise business processes ontology]. *Theoretical and Practical Aspects of Management.* (11). 137-168. (in Russian).

ISSN 1994-6929

Kliri Sh. (2011). *Globalnye riski. Delovoy uspekh v nespokoynye vremena* [Global risks. Business success in turbulent times] M.: Voprosy ekonomiki. (in Russian).

Kopylova E.A. (2014). *Vozmozhnosti primeneniya situatsionnogo podkhoda k analizu sistemy upravleniya organizatsiey* [The possibilities of applying of the contingency approach to the analysis of management of the organisation]. *Economics and innovations management.* (2(29)). 26. (in Russian).

Krivorotov V.V., Kalina A.V., Eriashvili N.D. (2015). *Ekonomicheskaya bezopasnost gosudarstva i regionov* [The economic security of the state and regions] M.: YuNITI-DANA. (in Russian).

Maksimov A.A. (2019). *Razrabotka sistemy pokazateley ekonomicheskoy bezopasnosti predpriyatiy atomnoy otrasli* [Development of the system of economic security indicators of the nuclear industry enterprises] Sankt-Peterburg. (in Russian).