Хамидуллин Р.Д. ¹

1 Российский экономический университет имени Г.В. Плеханова, Москва, Россия

Оценка риск-менеджмента организации удаленного доступа

ЦИТИРОВАТЬ СТАТЬЮ:

Хамидуллин Р.Д. Оценка риск-менеджмента организации удаленного доступа // Креативная экономика. – 2022. – Том 16. – № 5. – С. 1939–1952. doi: 10.18334/ce.16.5.114636

аннотация:

В статье рассматриваются вопросы оценки риск-менеджмента организации удаленного управления производственными системами в условиях нефтегазодобывающих организаций. Целью исследования было методическое обоснование оценки рисков при реализации удаленного управления процессами разработки и добычи нефти и газа на базе цифровых технологий управления в форме создания центров удаленного централизованного управления производственными процессами. Анализ процессов трансформации нефтегазодобывающих организаций при переходе на удаленный доступ предполагает учет как можно большего количества видов и факторов риска с целью минимизации общего риска проекта. Оценка рисков в общем плане представляет собой реализацию трех основных этапов (анализ, оценка и обработка рисков). Также в статье отмечено, что наиболее значимым и существенным при организации удаленного управления является киберриск, который связан с использованием, владением, эксплуатацией, участием, воздействием и внедрением информационных технологий управления в организации. Результаты исследования могут быть интересны руководителям организаций, осуществляющих переход от традиционной модели управления к централизованной на основе удаленного доступа, а также студентам и аспирантам, интересующимся данной темой.

КЛЮЧЕВЫЕ СЛОВА: риск-менеджмент, управление производственными системами, удаленный доступ, цифровые технологии управления, трансформация моделей управления, традиционная и централизованная модель управления

ОБ АВТОРЕ

издательство КРЕАТИВНАЯ ЭКОНОМИКА **Хамидуллин Ринальд Дамирович**, лицо, прикрепленное для подготовки диссертации на соискание ученой степени кандидата наук, кафедра менеджмента и бизнес-технологий (rinald.khamidullin@lukoil.com)

Khamidullin R.D. 1

¹ Plekhanov Russian University of Economics, Russia

Risk management in remote access

CITE AS:

Khamidullin R.D. (2022) Otsenka risk-menedzhmenta organizatsii udalennogo dostupa [Risk management in remote access]. *Kreativnaya ekonomika. 16.* (5). – 1939–1952. doi: 10.18334/ce.16.5.114636

ABSTRACT:

The issues of risk management assessment of production system remote management in oil and gas producing organizations are considered. The purpose of the study was a methodological justification of risk assessment in the implementation of remote control of oil and gas development and production processes based on digital control technologies in the form of the creation of remote centralized control centers for production processes. Analysis of the transformation processes of oil and gas producing organizations during the transition to remote access involves taking into account as many types and risk factors as possible in order to minimize the overall risk of the project. Risk assessment in general terms is the implementation of three main stages: analysis, assessment and processing of risks. The most significant factor in the organization of remote management is cyber risk, which is associated with the use, possession, operation, participation, impact and implementation of information management technologies in the organization. The results of the study may be of interest to managers of organizations making the transition from a traditional management model to a centralized one based on remote access, as well as students and postgraduates interested in this topic.

KEYWORDS: risk management, production system management, remote access, digital management technologies, management model transformation, traditional and centralized management model

JEL Classification: M11, M21, D81, O31

Received: 18.04.2022 / **Published:** 31.05.2022

© Author(s) / Publication: CREATIVE ECONOMY Publishers

For correspondence: Khamidullin R.D. (rinald.khamidullin@lukoil.com)

Введение

В условиях перехода на новый технологический уклад происходит трансформация традиционных форм управления, в ходе которой активное распространение получили цифровые технологии [1] (Klochko, Fomenko, Nekrasova, 2016). К таким технологиям относится в том числе и применение удаленного доступа к производственным системам путем формирования Центров удаленного управления производственными системами.

Удаленное управление производственными системами на базе комплексной цифровизации представляет собой инновационный процесс, позволяющий осуществлять как организационную трансформацию самих организаций и их структурных подразделений, так и трансформацию операционной модели управления такими организациями в целом [2] (Khamidullin, 2021). Удаленное управление на базе цифровых технологий предполагает централизацию основных функций с частичным делегированием их на другие уровни управления. Часть процессов подлежит полной автоматизации [3] (Kravchenko, 2017).

Все эти процессы реализуются под воздействием множества факторов внешней и внутренней среды, которые не всегда носят позитивный характер. В связи с неопределенностью и негативными воздействиями на организацию, происходящими в результате таких изменений, менеджменту необходимо разрабатывать и реализовывать целый комплекс управленческих решений, которые можно отнести к риск-менеджменту. Риск присущ всем аспектам деятельности организации, независимо от отрасли или сектора, в результате чего риск-менеджмент стал неотъемлемой частью управления современными организациями, в особенности на тех этапах их развития, которые связаны со сложными структурными преобразованиями или переходом на новые технологии управления. При этом риск-менеджмент представляет собой стандартную практику анализа, оценки и обработки рисков для минимизации их негативных последствий от неблагоприятных финансовых, операционных, экологических, политических, организационных или других подобных событий.

Среди большого количества ученых активно обсуждаются вопросы риск-менеджмента при переходе на цифровые технологии управления, среди которых особого внимания заслуживают труды: Безденежных В.М. [4] (Bezdenezhnyh, Rodionov, 2017), Умновой М.Г. [5] (Umnova, 2019), Капустиной Н.В. [6] (Aloyan, Filimonova, Petrukhin, Kapustina, 2017), Качалова Р.М. [7] (Kachalov, 2012), Кузнецова Ю.В. [8] (Polzunova, Kapustina, Kuznetsov, 2015),

Корнеева Д.В. [9] (Korneev, 2015), Кравченко О.Ю. [10] (Kravchenko, 2011), Лемеш О.П. [11] (Lemesh, 2011), Скобелевой И.П. [12] (Skobeleva, Legostaeva, Kalashnik, 2016), Фоменко Н.М. [13] (Krepkov, Efimov, Fomenko, 2010), Халикова М.А. [14] (Khalikov, Maksimov, 2015), Хачатуряна А.А. [15] (Khachaturyan, Sinko, 2013) и др.

В рамках данного исследования под риском будет пониматься следствие влияния неопределенности на достижение поставленных целей [16], а под риск-менеджментом – процесс принятия и реализации управленческих решений, которые направлены на снижение вероятности возможных потерь и неблагоприятного результата деятельности [17] (*Umnova*, 2019).

Целью исследования являлось методическое обоснование оценки рисков при реализации удаленного управления процессами разработки и добычи нефти и газа на базе цифровых технологий управления в форме создания центров удаленного централизованного управления производственными процессами (ЦУЦПП).

Методически работа основана на фундаментальных и прикладных трудах ученых, теории организации и управления рисками.

Новизна исследования заключается в решении научной проблемы – оценка риск-менеджмента организации удаленного доступа к производственным системам нефтегазодобывающих организаций.

Управление рисками подразумевает в себе процесс, посредством которого организации выявляют возможные риски, оценивают эти риски с точки зрения их терпимости, вероятности возникновения рисковых ситуаций и на основе полученной информации принимают управленческие решения с целью недопущения рисковых ситуаций и снижения потерь на основе их допустимости [18] (Fomenko, 2015). Базовые положения оценки рисков закреплены в Методических рекомендациях по оценке эффективности инвестиционных проектов и их отбору для финансирования, в ГОСТ 2.103–68 и ГОСТ Р 15.201–2000, в которых выделены статистические, экспертные методы и методы моделирования рисков.

Операционная деятельность нефтегазодобывающей организации на основе удаленного доступа к производственным системам, как и любого проекта, имеет определенную долю риска, который, в свою очередь, может повлечь провал самого проекта. Поэтому при анализе процессов трансформации в условиях перехода на цифровые технологии и удаленный доступ следует учесть как можно большее количество видов и факторов риска с целью минимизации общего риска проекта. Для принятия правильного управленческого решения необходимо оценить, насколько ожидаемый доход компенсирует

предполагаемый риск. Однако сложность данного процесса состоит в сложной формализации процесса. Тем не менее анализ риска имеет особую важность для предотвращения возможных потерь и убытков.

Оценка риск-менеджмента деятельности нефтегазодобывающих организаций в условиях перехода на цифровые технологии управления предполагает применение определенной методики оценки рисков, которая аккумулирует в себе идентификацию, качественный и количественный их анализ.

Оценка рисков в общем плане представляет собой реализацию трех основных этапов (рис. 1).



Рисунок 1. Основные этапы управления рисками *Источник*: составлено автором на основе [19] (*Kaplan, Garrick*, 1981).

Этап 1, анализ рисков, традиционно использует методологию, которая отвечает на три вопроса:

- Что может пойти не так?
- Какова вероятность того, что все пойдет не так?
- Каковы будут последствия, если что-то пойдет не так?

На этапе 2 организация оценивает свою подверженность риску в соответствии со своей толерантностью к риску, чтобы определить значимость риска события или событий. Несмотря на то, что оценка риска включает определение приоритетов рисков на основе вероятности и последствий, важно отметить, что риск является не просто результатом вероятности и последствий, а скорее функцией вероятности и последствий. Например, событие с низкой вероятностью и высокой последовательностью, приводящее к смертельным исходам, будет иметь для организации совершенно иную значимость риска, чем событие с высокой вероятностью и низкими последствиями, несмотря на то, что потенциально может иметь тот же результат при умножении оценок последствий на вероятность.

Этап 3 процесса управления рисками включает определение реакции на реализовавшийся риск. После выявления и оценки рисков у организации

обычно есть четыре варианта реагирования на риск: принятие риска, предотвращение или устранение риска, передача риска или смягчение риска. Снижение рисков предполагает снижение вероятности и/или серьезности последствий путем внедрения изменений или средств контроля в организации или процессе. Организация учитывает множество факторов при определении методов управления рисками, таких как устойчивость к риску, нормативные требования и затраты.

Анализ рисков реализации проектов можно разделить на качественный, описывающий все предполагаемые риски проекта, а также стоимость их последствий и мер по снижению, и количественный, содержит непосредственные расчеты изменений эффективности проекта в связи с рисками [18] (Fomenko, 2015). Однако в настоящее время отсутствует какая-либо общая методология и интеграция качественных и количественных подходов к оценке рисков, не представляется в форме какого-то стандартного решения. При определении риска необходимо определиться с целью и сформулировать основные требования. Данный этап характеризуется неполнотой и неточностью информации и подвержен изменениям в архитектуре объединения предприятий-партнеров.

Ввиду специфики объекта исследования – внутренних процессов и закономерностей развития производственной системы нефтегазодобывающей организации и их функционирования в условиях перехода на цифровые технологии управления – наиболее значимым и существенным является киберриск. Киберриск – это категория бизнес-рисков, связанная, в частности, с использованием, владением, эксплуатацией, участием, воздействием и внедрением информационных технологий управления в организации. Данный вид рисков включает события, вероятность возникновения которых и их размер являются неопределенными, которые могут негативно повлиять на деятельность компании и ее способность достигать стратегических целей. Этот риск не рассматривается как отдельный вид риска или как подтип операционного риска (рис. 2). Киберриск можно определить, если какие-либо действия, задачи или функции реализуются в киберпространстве, независимо от их отнесения к классическим категориям риска.

Первоначально киберриск был связан с угрозами, возникающими в результате использования интернет-пространства. Позже, наряду с распространением идеи киберпространства, киберриск был отнесен к видам рисков, которые возникают в результате угроз, возникающих в киберпространстве. Также термин «киберриск» сопоставляют с некоторыми недостатками циф-

ровых активов, которые могут быть подвержены угрозам, исходящим из киберпространства.



Рисунок 2. Киберриск в иерархии рисков

Источник: составлено автором.

Отвечая на вопрос «что может пойти не так?» при анализе киберрисков, обычно определяется цифровое устройство, система и/или функция, уязвимости, связанные с этими устройствами или системами, и возможные угрозы для них, чтобы создать сценарии или наборы сценариев, которые приводят к неблагоприятным последствиям.

Поскольку полный набор угроз и уязвимостей часто неизвестен и постоянно меняется, набор сценариев или возможных нежелательных событий трудно определить полностью, что тем самым затрудняет процесс принятия управленческих решений. Факторы, влияющие на оценку преднамеренных угроз нападения на информационные системы нефтегазодобывающих организаций, включают знания противников, мотивацию, намерения, характеристики и возможности, тактику, методы и процедуры.

Определение вероятности возникновения киберриска или кибер-угроз также затруднительно, поскольку не только невозможно определить вероятность, если полный набор сценариев неизвестен, но также трудно точно смоделировать вероятность преднамеренных атак интеллектуальных и адаптивных противников. Действительно, иногда пренебрегают вероятностью и определяют условный риск на основе происходящего сценария. Альтернативные подходы могут учитывать вероятность возникновения атаки, вероятность успешного завершения атаки и/или вероятность возникновения неблагоприятного воздействия.

Факторы, влияющие на вероятности, часто являются функцией угроз, уязвимостей и любых возможных мер по смягчению последствий. Например, противник может попытаться атаковать систему управления из Интернета – эта атака может иметь высокую вероятность возникновения, основанную на его доступности, но низкую вероятность успеха ввиду применения средств управления безопасностью, используемых для реализации безопасной архитектуры, таких как разделение сети, антивирусы. Вероятность совершения атаки также зависит от стимулов противника, которые для каждого из них различны и зависят от мотивов, намерений и навыков противника.

Как показано на *рисунке 3*, последствия киберинцидента обычно определяются в терминах триады С – I – А (конфиденциальность – целостность – доступность). Потеря конфиденциальности, обычно считающаяся наименее важным последствием в промышленных системах управления, может привести к потере конфиденциальной информации, которая может быть использована для планирования будущих, более разрушительных атак. Кроме того, потеря данных о компании или объекте может нанести финансовый ущерб или иной ущерб организации.



Рисунок 3. Цели кибербезопасности производственных систем управления нефтегазодобывающих организаций

Источник: составлено автором.

Потеря целостности и доступности может привести к последствиям, связанным с безопасностью (например, саботаж, гибель людей, травмы), финансовым (например, потеря генерации, повреждение оборудования) или связанным с репутацией последствиям. Потеря целостности включает изменение данных, логики или команд; это может повлиять на достоверность системы, что приведет к неблагоприятной работе системы. Потеря доступности (например, атака на отказ в обслуживании) может повлиять на поток данных и связи в системе, что также может привести к неблагоприятной работе системы.

Поскольку исторические данные ограничены, а определение вероятности и воздействия часто субъективно и основано на мнении экспертов, киберриск является более сложным, чем простое решение уравнения. Анализ киберрисков еще более усложняется тем фактом, что угрозы и уязвимости постоянно меняются по мере того, как противники становятся умнее, меняются векторы угроз и развиваются технологии. Поэтому не только трудно определить текущее состояние риска, но и практически невозможно предсказать будущее состояние. Как отметили Твенебоа-Кодуа и Бьюкенен, оценки рисков безопасности являются «скорее искусством, чем наукой» [19] (Kaplan, Garrick, 1981). Опплигер также отмечает, что «мы должны признать, что зашли в тупик и что наша хорошая математическая формула для количественной оценки рисков вряд ли работает на практике и поэтому бесполезна» [20] (Тат, Jones, 2019).

Аналогичная проблема с вероятностной неопределенностью существует и при оценке физической безопасности. Чтобы преодолеть это препятствие, методология управления безопасностью предприятия с учетом рисков (RIMES) использует степень сложности атаки, а не вероятность атаки для анализа рисков физической безопасности объектов.

Заключение

Учитывая сложность оценки киберрисков, необходимо использовать инструменты анализа рисков, которые обеспечивают целостный, дифференцированный подход к выявлению киберрисков, выходящий за рамки традиционного внимания к безопасности и включающий другие проблемы, такие как финансовые или операционные последствия. Возможность предоставить относительную оценку риска, которую нефтегазодобывающие организации могут использовать для определения приоритетов решений по обработке рисков, для включения как нормативных, так и бизнес-воздействий в один

анализ, поможет внедрить разумные и эффективные методы снижения киберрисков.

источники:

- 1. Klochko E., Fomenko N., Nekrasova V. Modelling of network mechanisms of management in the conditions of organizational development // Mediterranean Journal of Social Sciences. − 2016. − № 1. − p. 101–107.
- 2. Хамидуллин Р.Д. <u>Особенности формирования централизованной модели управления производственными системами (на примере компании «ЛУ-КОЙЛ»)</u> // Креативная экономика. 2021. № 10. с. 3851–3866. doi: 10.18334/ce.15.10.113687.
- 3. Кравченко К.Ю. Информация один из главных продуктов, который производит и потребляет компания // Сибирская нефть. 2017. № 139. с. 40–43.
- 4. Безденежных В.М., Родионов А.С. <u>Проактивный риск-ориентированный подход в сценарном планировании деятельности хозяйствующих субъектов</u> // Экономика. Налоги. Право. 2017. № 6. с. 76–83.
- 5. Умнова М.Г. <u>Модель работы организаций-поставщиков с государственным</u> заказом и перспективы требований, рисков и мер по их регулированию // Российское предпринимательство. 2019. № 1. с. 141–158.
- 6. Алоян Р.М., Филимонова Н.М., Петрухин А.Б., Капустина Н.В. <u>Управление логистическими факторами риска в процессе организации производства</u> // Известия высших учебных заведений. Технология текстильной промышленности. 2017. № 4(370). с. 94–97.
- 7. Качалов Р.М. Управление экономическим риском. / Теоретические основы и приложения: монография. Москва, Санкт-Петербург, 2012.
- 8. Ползунова Н.Н., Капустина Н.В., Кузнецов Ю.В. <u>Концепция развития предприятия текстильной промышленности на основе риск-менеджмента</u> // Известия высших учебных заведений. Технология текстильной промышленности. 2015. № 4(358). с. 43–47.
- 9. Корнеев Д.В. <u>Новый подход к диагностике системы риск-менеджмента в интегрированных предпринимательских структурах</u> // Российское предпринимательство. 2015. № 10. с. 1469–1482. doi: 10.18334/rp.16.10.261.
- 10. Кравченко О.Ю. <u>Стандарты риск-менеджмента для промышленных предприятий</u> // Российское предпринимательство. 2011. № 11. с. 74–79.
- 11. Лемеш О.П. <u>К вопросу о значении системного подхода в рамках развития риск-менеджмента на предприятиях торгово-экспортной деятельности нефтегазовой отрасли</u> // Российское предпринимательство. 2011. № 6. с. 102–106.

- 12. Скобелева И.П., Легостаева Н.В., Калашник Н.Е. <u>Интегрированный риск-менеджмент: инновационные модели реализации</u> // Креативная экономика. 2016. № 2. с. 185–196. doi: 10.18334/ce.10.2.35000.
- 13. Крепков И.М., Ефимов Е.Н., Фоменко Н.М. <u>Анализ и учет рисков продвижения интернет-проектов предприятия</u> // Вестник МЭИ. 2010. № 2. с. 101–107.
- 14. Халиков М.А., Максимов Д.А. <u>Концепция и теоретические основы управления производственной сферой предприятия в условиях неопределенности и риска</u> // Международный журнал прикладных и фундаментальных исследований. 2015. № 10–4. с. 711–719.
- 15. Хачатурян А.А., Синько В.А. <u>Роль информационных технологий в управлении рисками на промышленных предприятиях</u> // Вестник Московского университета им. С.Ю. Витте. Серия 1: Экономика и управление. 2013. № 4 (6). с. 76–82.
- Национальный стандарт Российской Федерации ГОСТ Р 5 1 8 9 7–2011/ Руководство ИСО 73:2009. Менеджмент Риска. [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200088035 (дата обращения: 10.10.2021).
- 17. Умнова М.Г. <u>Оценка рисков компаний-поставщиков при участии в госзакуп-ках</u> // Экономика, предпринимательство и право. 2019. № 4. с. 567–578.
- 18. Фоменко Н.М. Управление организацией в условиях развития инновационно-сетевых коммуникаций в электронной бизнес-среде. / автореферат дис.,.. доктора экономических наук / Рос. акад. нар. хоз-ва и гос. службы при Президенте РФ. Ростов-на-Дону, 2015.
- 19. Kaplan S., Garrick B.J. On the quantitative definition of risk. Risk Anal. 1, 11–27. [Электронный ресурс]. URL: https://doi.org/10.1111/j.1539-6924.1981.tb01350.x. (дата обращения: 09.10.2021).
- 20. Tam K., Jones K. MaCRA: a model-based framework for maritime cyber-risk assessment // WMU J. Maritime Affairs. 2019. № 18. p. 129–163.

REFERENCES:

- Aloyan R.M., Filimonova N.M., Petrukhin A.B., Kapustina N.V. (2017). *Upravlenie logisticheskimi faktorami riska v protsesse organizatsii proizvodstva* [Management of logistic risk factors in the process of organization of production]. *Izvestiya vysshikh uchebnyh zavedeniy. Tekhnologiya tekstilnoy promyshlennosti.* (4(370)). 94–97. (in Russian).
- Bezdenezhnyh V.M., Rodionov A.S. (2017). *Proaktivnyy risk-orientirovannyy podkhod v stsenarnom planirovanii deyatelnosti khozyaystvuyushchikh subektov* [Proactive risk-oriented approach in scenario planning of company activities]. *Economy. Taxes. Law.* (6). 76–83. (in Russian).

- Fomenko N.M. (2015). *Upravlenie organizatsiey v usloviyakh razvitiya innovatsion-no-setevyh kommunikatsiy v elektronnoy biznes-srede* [Organization management in the context of the development of innovative network communications in the electronic business environment] (in Russian).
- Kachalov R.M. (2012). *Upravlenie ekonomicheskim riskom* [Economic risk management] (in Russian).
- Kaplan S., Garrick B.J. On the quantitative definition of risk. Risk Anal. 1, 11–27. Retrieved October 09, 2021, from https://doi.org/10.1111/j.1539-6924.1981. tb01350.x.
- Khachaturyan A.A., Sinko V.A. (2013). Rol informatsionnyh tekhnologiy v upravlenii riskami na promyshlennyh predpriyatiyakh [Role of information technologies in management of risks at industrial enterprises]. Vestnik Moskovskogo universiteta im. S.Yu. Vitte. Seriya 1: Ekonomika i upravlenie. (4 (6)). 76–82. (in Russian).
- Khalikov M.A., Maksimov D.A. (2015). Kontseptsiya i teoreticheskie osnovy upravleniya proizvodstvennoy sferoy predpriyatiya v usloviyakh neopredelennosti i riska [The conception and theoretical basis of management in the production sphere of enterprise in uncertainty of the market environment]. International Journal of Applied and Fundamental Research. (10–4). 711–719. (in Russian).
- Khamidullin R.D. (2021). Osobennosti formirovaniya tsentralizovannoy modeli upravleniya proizvodstvennymi sistemami (na primere kompanii «LU-KOYL») [Particularities of a centralized management model of production systems (on the example of Lukoil)]. Creative economy. (10). 3851–3866. (in Russian). doi: 10.18334/ce.15.10.113687.
- Klochko E., Fomenko N., Nekrasova V. (2016). *Modelling of network mechanisms of management in the conditions of organizational development Mediterranean Journal of Social Sciences.* (1). 101–107.
- Korneev D.V. (2015). Novyy podkhod k diagnostike sistemy risk-menedzhmenta v integrirovannyh predprinimatelskikh strukturakh [A new approach to diagnostication of the risk-management system in integrated business structures]. Russian Journal of Entrepreneurship. (10). 1469–1482. (in Russian). doi: 10.18334/rp.16.10.261.
- Kravchenko K.Yu. (2017). *Informatsiya odin iz glavnyh produktov, kotoryy proizvodit i potreblyaet kompaniya* [Information is one of the main products that the company produces and consumes]. *Sibirskaya neft*. (139). 40–43. (in Russian).

- Kravchenko O.Yu. (2011). *Standarty risk-menedzhmenta dlya promyshlennyh pred- priyatiy* [Industrial enterprise risk management standards]. *Russian Journal of Entrepreneurship*. (11). 74–79. (in Russian).
- Krepkov I.M., Efimov E.N., Fomenko N.M. (2010). *Analiz i uchet riskov prodvizheniya internet-proektov predpriyatiya* [Analysis and accounting risks during promotion of enterprise internet projects]. *Vestnik MEI*. (2). 101–107. (in Russian).
- Lemesh O.P. (2011). K voprosu o znachenii sistemnogo podkhoda v ramkakh razvitiya risk-menedzhmenta na predpriyatiyakh torgovo-eksportnoy deyatelnosti neftegazovoy otrasli [On the question of significance of a systematic approach in the development of risk management at enterprises of trade and export activities in the oil and gas industry]. Russian Journal of Entrepreneurship. (6). 102–106. (in Russian).
- Polzunova N.N., Kapustina N.V., Kuznetsov Yu.V. (2015). Kontseptsiya razvitiya predpriyatiya tekstilnoy promyshlennosti na osnove risk-menedzhmenta [The concept of development of the enterprise of the textile industry on the basis of risk-management]. Izvestiya vysshikh uchebnyh zavedeniy. Tekhnologiya tekstilnoy promyshlennosti. (4(358)). 43–47. (in Russian).
- Skobeleva I.P., Legostaeva N.V., Kalashnik N.E. (2016). *Integrirovannyy risk-menedzhment: innovatsionnye modeli realizatsii* [Integrated risk management: innovational realization models]. *Creative economy*. (2). 185–196. (in Russian). doi: 10.18334/ce.10.2.35000.
- Tam K., Jones K. (2019). MaCRA: a model-based framework for maritime cyber-risk assessment WMU J. Maritime Affairs. (18). 129–163.
- Umnova M.G. (2019). Model raboty organizatsiy-postavshchikov s gosudarstvennym zakazom i perspektivy trebovaniy, riskov i mer po ikh regulirovaniyu [Model of work of the organizations-suppliers with the state order from the perspective of requirements, risks and measures for their regulation]. Russian Journal of Entrepreneurship. (1). 141–158. (in Russian).
- Umnova M.G. (2019). Otsenka riskov kompaniy-postavshchikov pri uchastii v go-szakupkakh [Risk assessment of supplier companies participating in public procurement]. Journal of Economics, Entrepreneurship and Law. (4). 567–578. (in Russian).