Трансверсальный подход при управлении цифровыми рисками

Получено: 15.10.2020 Статья доработана после рецензирования: 10.11.2020 Принято: 16.11.2020

УДК 004.9:005.342 JEL 014 DOI 10.26425/2658-3445-2020-3-4-49-56

Воронцова Юлия Владимировна

Канд. экон. наук, доцент, ФГБОУ ВО «Государственный университет управления», г. Москва, Российская Федерация
ORCID: 0000-0001-7995-6395, *e-mail: jvms2008@yandex.ru*

Баранов Владимир Николаевич

Руководитель группы закупок, ООО «Сузуки Мотор Рус», г. Москва, Российская Федерация
ORCID: 0000-0002-2094-6421, *e-mail: jvms@yandex.ru*

АННОТАЦИЯ

Кратко представлен обзор цифровых рисков, так как управление ими является неотъемлемой частью управления бизнесом. Цифровая трансформация открывает невероятные возможности как для роста организации, так и для создания ее стоимости. Тем не менее, ни одна из этих возможностей не может быть реализована без учета связанных с этим рисков. Все большее количество организаций становятся уязвимыми для определенного рода цифровых угроз. Управление рисками имеет решающее значение для устойчивости организации, а понимание областей риска – для выявления и устранения всех рисков, которым организация может подвергаться в цифровой среде. Для эффективного управления цифровыми рисками выделены те их области, которые представляются наиболее существенными.

Выделены три подхода к смягчению цифровых рисков: тактический, оперативный и стратегический. При исследовании основных областей появления цифровых рисков в организации был сделан вывод о необходимости разработки универсального подхода к созданию эффективного механизма управления рисками в цифровой среде. В рамках такого подхода были сформулированы основные этапы управления цифровыми рисками.

В качестве эффективного инструментария при управлении цифровыми рисками организации предложено использовать трансверсальный подход, то есть организацию таких связей, взаимодействия и сотрудничества между отдельными сотрудниками и подразделениями организации, которые позволяют эффективно осуществлять процессы, связанные с выявлением рисков, их анализом, а также принятием решений, направленных на минимизацию возможных отрицательных последствий уже наступивших рисковых событий. При этом эффективное управление цифровыми преобразованиями для обеспечения межфункциональной синергии предполагает устранение рисков, возникающих из-за взаимозависимых процессов. Также предложено разрабатывать стратегию управления цифровыми рисками на базе трансверсального подхода в интеграции с уже реализуемой в организации стратегией цифровизации. Это позволит организации чувствовать себя более уверенно в будущем при внедрении и использовании инновационных технологий для решения стоящих перед ней проблем.

КЛЮЧЕВЫЕ СЛОВА

Межфункциональная синергия, мониторинг, непрерывность, стратегия организации, трансверсальный подход, угрозы, управление, цифровая трансформация, цифровой актив, цифровые риски

ДЛЯ ЦИТИРОВАНИЯ

Воронцова Ю.В., Баранов В.Н. Трансверсальный подход при управлении цифровыми рисками//E-Management. 2020. Т. 3. № 4. С. 49–56.

© Воронцова Ю.В., Баранов В.Н., 2020.
Статья доступна по лицензии Creative Commons «Attribution» («Атрибуция») 4.0. всемирная.

Transversal approach to digital risk management

Received: 15.10.2020 Revised: 10.11.2020 Accepted: 16.11.2020

JEL 014 DOI 10.26425/2658-3445-2020-3-4-49-56

Yulia V. Vorontsova

PhD in Economics, associate professor, State University of Management, Moscow, Russia
ORCID: 0000-0001-7995-6395, *e-mail: jvms2008@yandex.ru*

Vladimir N. Baranov

Head of Suzuki Motor Rus Procurement Group, Moscow, Russia
ORCID: 0000-0002-2094-6421, *e-mail: jvms@yandex.ru*

ABSTRACT

The article presents a brief overview of digital risks, since their management is an integral part of business management. Digital transformation opens up incredible opportunities for both organizational growth and value creation. However, none of these opportunities can be realized without taking into account the associated risks. An increasing number of organizations are becoming vulnerable to certain types of digital threats. Risk management is critical to the sustainability of an organizations, and understanding risk areas is critical to identifying and eliminating all the risks that an organization may be exposed to in a digital environment. For effective management of digital risks, the authors highlight those their areas that seem to be the most significant.

The paper emphasizes three approaches to mitigating digital risks: tactical, operational and strategic. When studying the main areas of the emergence of digital risks in an organization, the authors concluded that it is necessary to develop a universal approach to creating an effective risk management mechanism in the digital environment. Within this approach, the article formulated the main stages of digital risk management.

As an effective toolkit in managing digital risks of an organization, the paper proposes to use a transversal approach, that is, the organization of such connections, interaction and cooperation between individual employees and divisions of the organization, which allow you to effectively implement processes associated with risk identification, their analysis, and decision-making aimed at minimization of possible negative consequences of already occurred risk events. At the same time, effective management of digital transformations to ensure cross-functional synergy presupposes the elimination of risks arising from interdependent processes. The study also proposes to develop a digital risk management strategy based on a transversal approach in integration with the digitalization strategy already being implemented in the organization. This approach will allow the organization to feel more confident in the future when implementing and using innovative technologies to solve the problems it faces.

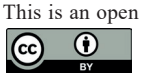
KEYWORDS

Continuity, cross-functional synergy, digital asset, digital risks, digital transformation, management, monitoring, organization strategy, threats, transversal approach

FOR CITATION

Vorontsova Yu.V., Baranov V.N. (2020) Transversal approach to digital risk management. *E-Management*, vol. 3, no. 4, pp. 49–56. DOI 10.26425/2658-3445-2020-3-4-49-56

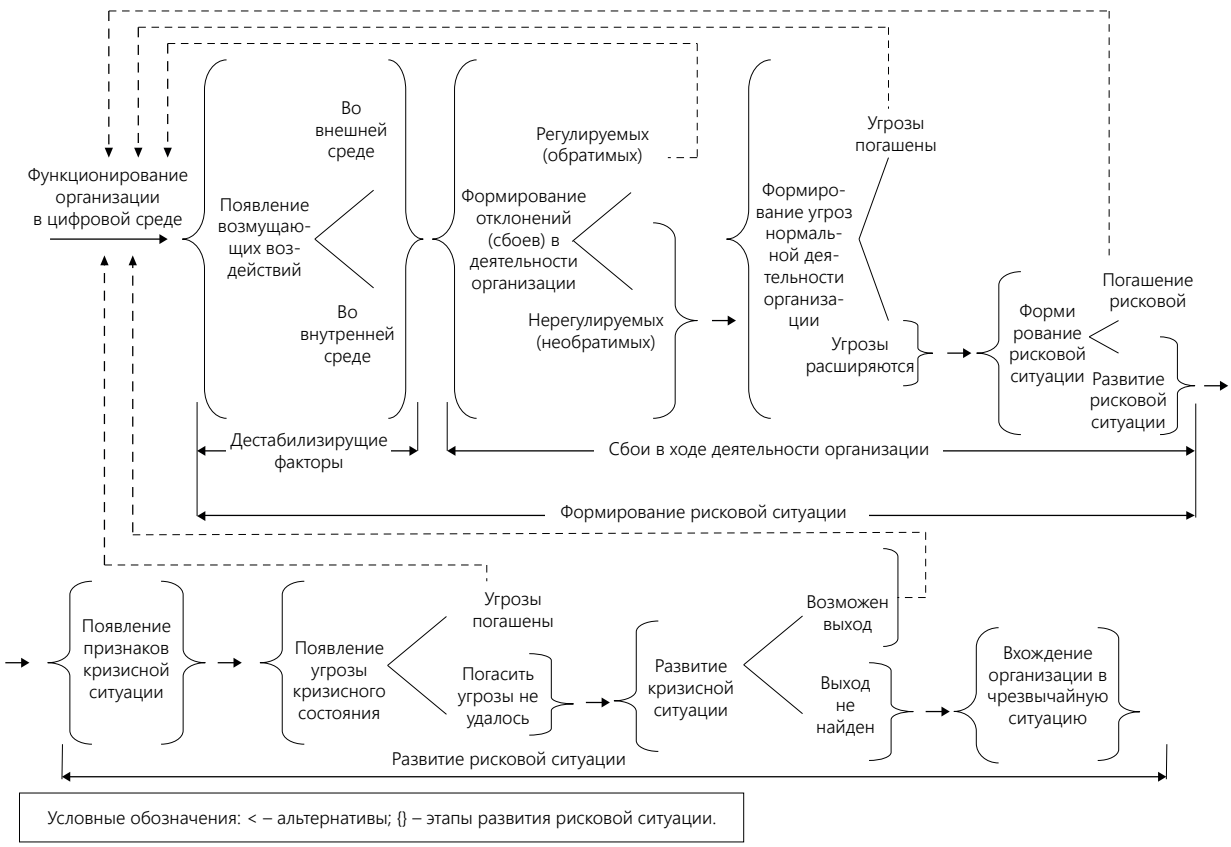
© Vorontsova Yu.V., Baranov V.N., 2020.
This is an open access article under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).



В настоящее время все большее количество организаций понимает тот факт, что цифровые технологии становятся насущной необходимостью (а не опцией) и наиболее эффективным способом для создания конкурентного преимущества, а также могут способствовать успешному осуществлению преобразований внутри самой организации. Цифровая трансформация открывает невероятные возможности для ее роста и создания стоимости. Тем не менее, ни одна из этих возможностей не может быть реализована без учета связанных с этим рисков.

Управление цифровыми рисками – неотъемлемая часть управления бизнесом. Оно базируется на выявлении угроз и минимизации рисков корпоративной информации и базовых IT-систем, которые ее обрабатывают, поскольку с их помощью реализуется полный набор бизнес-процессов.

Все большее количество организаций становится уязвимыми для определенного рода цифровых угроз и, как следствие, связанных с ними цифровых рисков [Соломатин, 2019] (рис.). В связи с этим определение цифрового риска может рассматриваться как последствия внедрения инновационных технологий, среди которых важное место занимают создаваемый искусственный интеллект и другие smart-технологии. Их использование порождает как контекстные социальные, экономические, так и политические проблемы. Эти последствия новы и зачастую неожиданны. В настоящее время исследования зарубежных ученых сосредоточены также на управлении маловероятными рисками с высокой отдачей, оценке возможностей будущих технологий и очень отдаленных перспектив[1]. Управление же цифровыми рисками подразумевает четкое понимание последствий внедрения определенных инновационных технологий таким образом, чтобы минимизировать цифровой риск в конкретной организации.



Составлено авторами по материалам источника: [Воронцова, 2019] */ Compiled by the authors on the materials of the source [Vorontsova, 2019]*

Рис. Процесс возникновения и развития рисковой ситуации
Figure. The process of occurrence and development of a risky situation

[1] *Armstrong S., Bradshaw H., Beckstead N., Sandberg A.* (2015). System risk of modelling in insurance. Did your model tell you all models are wrong? / White paper by the Systemic Risk of Modelling Working Party. Режим доступа: https://tigerrisk.com/wp-content/uploads/2018/10/SystemicRisksofModellingFINALV3.pdf (дата обращения: 12.10.2020).

Таким образом, цифровые риски становятся важной частью системы управления бизнес-рисками организации независимо от того, пытается она бороться с киберугрозами с помощью сторонних инструментов или нет. Передовые smart-технологии имеют тенденцию быть «чистыми» и эффективными, так как появляется возможность существенно снизить потребности в ресурсах, виртуализируя некоторые инструменты. Низкоуровневый контроль материи позволяет эффективно перерабатывать ее. Кроме того, различные эффективные с точки зрения соотношения «затраты – отдача» системы позволяют распределять и использовать дисперсные источники энергии. В долгосрочной перспективе предполагается с помощью тех же smart-технологий предоставление возможностей для исследования новых и значимых сфер.

ТЕОРИЯ И МЕТОДЫ

Управление рисками имеет решающее значение для устойчивости организации [Юрченко, Галяткина, 2012], а понимание областей риска – для выявления и устранения всех рисков, которым организация может подвергаться в цифровой среде [Шеве и др., 2019]. Для эффективного управления цифровыми рисками необходимо выделить те их области, которые представляются наиболее существенными:

– стратегические, проистекающие из цифрового видения и оценки технико-экономических инициатив, которые могут подвергнуться цифровой трансформации;

– технологические, оказывающие влияние на системы, людей и процессы. Сюда можно отнести потери из-за технологических сбоев или устаревших технологий. Кроме того, основными факторами риска здесь могут быть: масштабируемость, совместимость и точность функциональных возможностей внедренной технологии [Bajo Sanjuán & Villagra García, 2017];

– информационные (риски конфиденциальности данных), подразумевающие несанкционированное использование, нарушение конфиденциальности и целостности технологических систем, утечку данных; а также риски, возникающие в связи с ненадлежащим обращением с персональными данными клиентов или сотрудников, что может влиять на конфиденциальность физического лица; сюда же можно отнести риски, связанные с обменом данными, интеграцией технологий с третьими лицами (например, поставщиками). Минимизация влияния таких рисков [Цветков, В. и др., 2019] может включать укрепление платформы, оптимизацию данных (классификацию, хранение и обработку), шифрование данных, проработку сетевой архитектуры, своевременное выявление уязвимостей и постоянный мониторинг безопасности;

– операционные, включающие риски, возникающие из-за неадекватного контроля в операционных процедурах [Зеленцова, Тихонов, 2019];

– криминалистические, подразумевающие способность/неспособность цифровой среды проводить расследование в случае мошенничества или нарушения безопасности, включая сбор доказательств данных, которые могут быть представлены в суде (например, видеофиксация). В источниках специальной литературы этот риск рассматривается как риск кибербезопасности (риск кибератак, то есть получение конфиденциальной информации и ее использование для злонамеренных действий);

– нормативные, возникающие из-за несоблюдения законодательных требований, включая технологические законы, отраслевые законы и нормативные акты. Данный вид рисков еще определяют как риск соответствия, который относится к любым новым требованиям или правилам, необходимым для новой технологии, и заключается в несоблюдении нормативных требований в отношении бизнес-операций, хранения данных и других методов ведения бизнеса.

Кроме того, выделяют также следующие виды рисков:

– кадровые риски (нехватка навыков работы с цифровыми платформами и программами и высокая текучесть кадров может поставить под угрозу цели организации);

– риски третьих лиц (связанные с привлечением сторонних поставщиков или поставщиков услуг, например, уязвимость, связанная с интеллектуальной собственностью, данными, операциями и др.);

– риски автоматизации (связанные с проблемой совместимости с другими технологиями, нехватки ресурсов и, среди прочего, с проблемой управления);

– риски отказоустойчивости (возникновение негативных событий при внедрении новой технологии и сложности при минимизации нанесенного ущерба).

При управлении цифровыми рисками следует руководствоваться выполнением следующих задач.

1. Определение ключевых активов и проведение внутреннего аудита. Организации необходимо разработать стратегию, позволяющую предвидеть риски с целью принятия упреждающих воздействий или, если упущено время, их снижения. При этом можно использовать стратегию GRC (от англ. governance, risk and compliance strategy) как подход организации к трем практикам: корпоративного управления, управления рисками и соблюдения нормативных требований (соответствия). Чтобы управлять цифровыми рисками организации нужно определить свои критически важные активы, в числе которых ее клиенты и сотрудники, а также IT-системы. Определив эти ключевые активы, можно понять, в чем их уязвимость и характер потенциальных атак. После этого нужно убедиться, что эти активы соответствуют GRC стратегии организации. Решения и услуги GRC позволяют организациям внедрять, управлять, отслеживать и измерять эффективность своих цифровых стратегий. Эти стратегии должны включать четко определенные измеримые параметры, которые позволят организациям осознать степень своей эффективности в соответствующих областях. Несмотря на очевидную эффективность использования данного инструментария, он не в полной мере отвечает требованиям, предъявляемым к эффективному механизму управления цифровыми рисками, так как не отражает взаимодействие между цифровыми объектами.
2. Определение поля потенциальных угроз для организации с целью изучения их поведения. На сегодняшний день существуют различные структуры, помогающие организациям настраивать защиту от реальных цифровых угроз. Это помогает лучше подготовиться к их появлению с учетом того, что цифровые угрозы «предпочитают атаковать» на основе кратчайшего пути или минимально необходимых усилий.
3. Мониторинг нежелательных воздействий путем выявления уязвимых активов.
4. Принятие мер по защите от цифровых рисков. На этом этапе необходимо убедиться, что в организации разработана и готова к реализации стратегия смягчения последствий. Существует три подхода к их смягчению: тактический, оперативный и стратегический. Тактические смягчения подразумевают уменьшение поверхности атаки. Здесь следует поставить себя на место атакующего и определить уязвимые системы либо для их удаления, либо для блокировки в случае атаки. Оперативное смягчение подразумевает отслеживание цифровых рисков в режиме реального времени с одновременным использованием операционных мер по их снижению. Для этого следует осуществлять стратегический мониторинг, что позволит укрепить доверие к стратегии управления цифровыми рисками. Стратегическое смягчение подразумевает корректировку модели рисков и угроз с учетом критически важных цифровых активов. При этом возможна интеграция управления цифровыми рисками в общие процессы управления инцидентами.

РЕЗУЛЬТАТЫ И ВЫВОДЫ

Исследование основных областей появления цифровых рисков в организации показывает необходимость разработки универсального подхода к созданию эффективного механизма управления рисками в цифровой среде. В рамках такого подхода можно выделить основные этапы управления рисками.

1. Выявление. При этом проводится анализ цифровых помощников с целью оценить цифровой след организации и его влияние; создается реестр цифровых рисков.
2. Внедрение. На этом этапе в контексте бизнеса происходит внедрение цифровой архитектуры, основанной на учете рисков, для выбранных цифровых средств поддержки.
3. Развитие. Данный этап включает в себя разработку и развитие цифровой архитектуры, основанной на учете рисков, адаптированной к цифровым потребностям организации и ее операционной среде. Необходима также поддержка управления рисками путем проведения семинаров и тренингов по повышению осведомленности о рисках. Кроме того, на этом этапе формируются условия для применения проактивного подхода вместо того, чтобы просто работать в реактивном режиме.
4. Контроль. На этапе контроля происходит внедрение непрерывного процесса мониторинга, который может развиваться как ответ на сбои и новые события в цифровой среде, а также возможно изменение правовых и нормативных требований.

В качестве эффективного инструментария при управлении цифровыми рисками организации можно использовать трансверсальный подход [Воронцова, Баранов, 2019], то есть организацию таких связей, взаимодействия и сотрудничества между отдельными сотрудниками и подразделениями организации, которые

позволяют эффективно осуществлять процессы, связанные с выявлением рисков, их анализом, а также принятием решений, направленных на минимизацию возможных отрицательных последствий уже наступивших рисковых событий (линейная цепочка формирования риска представлена на рисунке). Кроме того, управление рисками, как одна из областей менеджмента, находится на пересечении таких различных сфер знаний, как стратегический, финансовый и инвестиционный менеджмент, страхование и даже математика, а именно, математическое моделирование [Акаев, Садовничий, 2019]. Трансверсальный подход в той же степени уместен и при управлении цифровыми рисками организации. Для создания эффективного механизма управления цифровыми рисками следует использовать принцип трансверсальности [Колесников, 2010] в интеграции с уже реализуемой в организации стратегией цифровизации, учитывающей вертикальное и горизонтальное взаимодействие между цифровыми объектами.

Эффективное управление цифровыми преобразованиями для обеспечения межфункциональной синергии[2] предполагает, в том числе, и устранение рисков, возникающих из-за взаимозависимых процессов.

Однако, говоря о рисках, связанных с использованием искусственного интеллекта, необходимо отметить, что их прогнозировать сложнее, чем любые другие известные цифровые риски. Некоторые ученые, стремясь к созданию искусственного интеллекта, говорят о загрузке разума и готовы идти на его прямое сканирование и реконструкцию в качестве программного обеспечения[3]. Нанотехнологии будут двигаться вперед за счет использования более традиционных низкоуровневых химических симуляторов, так как потребность для интерпретации симуляций растет [Savulescu, 2012]. Для этого существует множество способов математического описания сложных систем, смоделированных таким образом, чтобы предсказывать наиболее эффективное использование сложных моделей. Однако, никакого конкретного «рабочего» подхода не существует. Параллельно необходимо прорабатывать множество альтернативных сценариев, что потребует динамичного, восходящего процесса, а не использования одного какого-либо конкретного инструмента, даже, на первый взгляд, наиболее прогрессивного из ныне существующих.

ЗАКЛЮЧЕНИЕ

Управление цифровыми рисками требует времени. Для начала необходимо разобраться с тем, что понимать под цифровыми рисками, и какого типа они существуют. Для этого следует разрабатывать и реализовывать стратегию управления цифровыми рисками на базе трансверсального подхода в интеграции с уже реализуемой в организации стратегией цифровизации, что позволит организации чувствовать себя более уверенно в будущем при внедрении и использовании инновационных инструментов/технологий для решения стоящих перед ней проблем. Таким образом, возможно постоянно удовлетворять меняющиеся и требовательные запросы клиентов с учетом цифровизации внешней среды.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Акаев А., Садовничий В. (2019). К вопросу о выборе математических моделей для описания динамики цифровой экономики // Дифференциальные уравнения. Т. 55. № 5. С. 743–752.

Воронцова Ю. (2019). Управление рисками: учебное пособие. М.: Издательский дом ФГБОУ ВО «Государственный университет управления». 128 с.

Воронцова Ю., Баранов В. (2019). Трансверсальное применение стратегии цифровизации // E-management. Т. 2. № 4. С. 85–91.

Зеленцова Л., Тихонов А. (2019). Особенности развития наукоемких и высокотехнологичных производств в условиях цифровой трансформации // РИСК: Ресурсы, Информация, Снабжение, Конкуренция. № 1. С. 38–41.

[2] *Terrones Rodrígues A.L.* (2019). Una aproximación general al transhumanismo y su problematización [Общий подход к трансгуманизму и его проблематизация]. Режим доступа: https://www.academia.edu/39615257/Una_aproximación_general_al_transhumanismo_y_su_problematización?email_work_card=view-paper (дата обращения: 12.10.2020).

[3] *Sandberg A.* (2012). Gf 2045: Anders Sandberg. Video message. Режим доступа: https://yandex.ru/video/touch/search?filmld=12974653496765993043&text=%D0%90%D0%BD%D0%B4%D0%B5%D1%80%D1%81%20%D1%81%D0%B0%D0%BD%D0%B4%D0%B1%D0%B5%D1%80%D0%B3&noreask=1&path=wizard&ts=1573843519052&source=share (дата обращения: 12.10.2020).

Колесников А. (2010). Постмодерн и новое постметафизическое мышление: от трансмодернизма к трансверсальности // Вестник Ленинградского государственного университета им. А.С. Пушкина. № 1 (2). С. 42–50.

Соломатин Д. (2019) Влияние научно-технического прогресса на институциональную траекторию развития российской экономики // Экономика устойчивого развития. № 1 (37). С. 74–77.

Цветков В. [и др.] (2019). Экономико-математическое моделирование бизнес-процессов отраслевых рынков в условиях цифровой экономики: монография. М.: Компания КноРус. 190 с.

Шеве Г. [и др.] (2019). От индустрии 3.0 к индустрии 4.0: основные понятия, измерения и компоненты индустрии 4.0 // Инвестиции в России. № 9 (296). С. 32–40.

Юрченко Т., Галяткина О. (2012). Инструментарий устойчивого функционирования организации // Вестник университета. № 11 (1). С. 215–221.

Bajo Sanjuán A., Villagra García N. (2017). Los retos de la globalización a la RSE: la revolución digital [Вызовы глобализации для КСО: цифровая революция]. Madrid, España: Universidad Pontificia Comillas ICAI – ICADE. 192 p.

Savulescu J. (2012). ¿Decisiones peligrosas?: Una bioética desafiante [Опасные решения?: Сложная биоэтика]. Tecnos. 344 p.

REFERENCES

Akaev A. and Sadovnichii V. (2019), "To the issue about mathematical models for describing the dynamics of the digital economy" ["K voprosu o vybore matematicheskikh modelei dlya opisaniya dinamiki tsifrovoi ekonomiki"], *Differential Equations* [*Differentsial`nye uravneniya*], vol. 55, no. 5, pp. 743–752. (In Russian).

Bajo Sanjuán A. and Villagra García N. (2017), *The challenges of globalization to CSR: the digital revolution* [*Los retos de la globalización a la RSE: la revolución digital*], Universidad Pontificia Comillas ICAI – ICADE, Madrid, España.

Kolesnikov A. (2010), "Postmodernism and new post-metaphysical thinking: from transmodernism to transversality" ["Postmodern i novoe postmetafizicheskoe myshlenie: ot transmodernizma k transversal'nosti"], Vestnik Leningradskogo gosudarstvennogo universiteta im. A.S. Pushkina. no. 1 (2), pp. 42–50. (In Russian).

Savulescu J. (2012), *Dangerous decisions?: Challenging bioethics* [*¿Decisiones peligrosas?: Una bioética desafiante*], Tecnos, España.

Sheve G. [et al.] (2019), "From industry 3.0 to industry 4.0: basic concepts, dimensions, and components of industry 4.0" ["Ot industrii 3.0 k industrii 4.0: osnovnye ponyatiya, izmereniya i komponenty industrii 4.0"], *Investments in Russia* [*Investitsii v Rossii*], no. 9 (296), pp. 32–40. (In Russian).

Solomatin D. (2019), "The impact of scientific and technological progress on the institutional trajectory of the Russian economy development" ["Vliyanie nauchno-tekhnicheskogo progressa na institutsional'nuyu traektoriyu razvitiya rossiiskoi ekonomiki"], *Economics of Sustainable Development* [*Ekonomika ustoichivogo razvitiya*], no. 1 (37), pp. 74–77. (In Russian).

Tsvetkov V. [et al.] (2019), *Economic and mathematical modeling of business processes in industry markets in the digital economy: monograph* [*Ekonomiko-matematicheskoe modelirovanie biznes-processov otraslevyh rynkov v usloviyakh tsifrovoi ekonomiki: monografiya*], KnoRus Company, Moscow, Russia. (In Russian).

Vorontsova Yu. (2019), *Risk management: tutorial* [*Upravlenie riskami: uchebnoe posobie*], State University of Management Publishing House, Moscow, Russia. (In Russian).

Vorontsova Yu. and Baranov V. (2019), "Transversal application of the digitalization strategy" ["Transversal'noe primenenie strategii tsifrovizatsii"], *E-Management*, vol. 2, no. 4, pp. 85–91. (In Russian).

Yurchenko T. and Galyatkina O. (2012), "Tools for providing stable functioning of organization" ["Instrumentarii ustoichivogo funktsionirovaniya organizatsii"], *Vestnik universiteta*, no. 11 (1), pp. 215–221. (In Russian).

Zelentsova L. and Tikhonov A. (2019), "Features of the development of high-tech and high-tech industries in the digital transformation" ["Osobennosti razvitiya naukoemkikh i vysokotekhnologichnykh proizvodstv v usloviyakh tsifrovoi transformatsii*"*], *RISK: Resources, Information, Supply, Competition* [*RISK: Resursy, Informatsiya, Snabzhenie, Konkurentsiya*], no. 1, pp. 38–41. (In Russian).

TRANSLATION OF FRONT REFERENCES

[1] Armstrong S., Bradshaw H., Beckstead, N. and Sandberg A. (2015), *System risk of modelling in insurance*. *Did your model tell you all models are wrong?* White paper by the Systemic Risk of Modelling Working Party. Available at: https://tigerrisk.com/wp-content/uploads/2018/10/SystemicRisksofModellingFINALV3.pdf (accessed 12.10.2020).

[2] Sandberg A. (2012), *Gf 2045: Anders Sandberg. Video message.* Available at: https://yandex.ru/video/touch/search?filmId=12974653496765993043&text=%D0%90%D0%BD%D0%B4%D0%B5%D1%80%D1%81%20%D1%81%D0%B0%D0%BD%D0%B4%D0%B1%D0%B5%D1%80%D0%B3&noreask=1&path=wizard&ts=1573843519052&source=share (accessed 12.10.2020).

[3] Terrones Rodrígues A.L. (2019), *Una aproximación general al transhumanismo y su problematización [A general approach to transhumanism and its problematisation]*. Available at: https://www.academia.edu/39615257/Una_aproximación_general_al_transhumanismo_y_su_problematización?email_work_card=view-paper (accessed 12.10.2020)