

УДК 330 + 06
ББК 65.01 + 06
DOI: 10.26140/anie-2020-0901-0096

РИСКИ И УГРОЗЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В ЦИФРОВОЙ ЭКОНОМИКЕ

© 2020
SPIN-код: 8959-9151
AuthorID: 358141

Графова Татьяна Олеговна, доктор экономических наук, доцент, заведующий кафедрой
«Экономической теории и международных экономических отношений» Российской
таможенной академии (Ростовский филиал), профессор кафедры
«Экономика, учет и анализ»

Шаповалов Александр Федорович, магистрант
Ростовский государственный университет путей сообщения
(344038, Россия, Ростов-на-Дону, пл. Ростовского Стрелкового Полка Народного
Ополчения, д. 2, e-mail: alschap@rambler.ru)

Аннотация. В статье выявлены, классифицированы и рассмотрены основные риски и угрозы экономической безопасности в цифровой экономике, их влияние и последствия, а так же основные направления для их минимизации. Показано, что в условиях перехода на цифровую экономику, понятие экономической безопасности значительно расширяется. Обеспечение экономической безопасности со всеми ее составляющими является ключевым фактором эффективности новой экономики России. Начавшийся процесс цифровизации экономики, затрагивает практически все сферы жизнедеятельности не только отдельно взятого общества и государства, но и всего мира в целом. Существует риск появления новых, ранее неидентифицируемых угроз не только экономической безопасности, но и безопасности личности, общества, государства. Экономическая безопасность в условиях цифровой экономики направлена на обеспечение противодействия вызовам и угрозам, связанным с новыми технологиями и особенностями цифровой экономики. Решение проблемы обеспечения экономической безопасности цифровой экономики, в целом, в первую очередь связано с решением вопросов обеспечения информационной безопасности, направленных на защиту информации и информационных технологий, защиты персональных данных и неприкосновенности частной жизни российских граждан в цифровом пространстве, правовое обеспечение социально-экономической деятельности в формате единого цифрового пространства. Развитие кадрового потенциала как главного ресурса цифровой экономики. Ключевым в экономической безопасности цифровой экономики России является недопущение навязывания и исключение заимствования «чужих» технологий, сервисов, программного обеспечения. Одной из основных и важнейших задач в обеспечении экономической безопасности Российской Федерации в условиях перехода на цифровую экономику является исключение зависимости отечественной промышленности от зарубежных информационных технологий за счет создания, развития и широкого внедрения отечественных разработок, а также производства продукции и оказания услуг на их основе.

Ключевые слова: национальная безопасность, цифровая экономика, экономическая безопасность, риски, угрозы, уязвимости, информационная безопасность, киберпреступность.

RISKS AND THREATS OF ECONOMIC SAFETY IN DIGITAL ECONOMY

© 2020

Grafova Tatyana Olegovna, Doctor of Economics, Associate Professor, Head of the Department
of Economic Theory and International Economic Relations, Rostov Branch of the State
Customs Institution of Higher Education "Russian Customs Academy", Professor,
Department of Economics, Accounting and Analysis
Shapovalov Alexander Fedorovich, master student
Rostov State Transport University
(344038, Russia, Rostov-on-Don, Rostovskogo Strelkovogo Polka Square
of the National Militia, 2, e-mail: alschap@rambler.ru)

Abstract. In article the main risks and threats of economic safety in digital economy, their influence and effects, and also main directions for their minimization are revealed, classified and considered. It is shown what in the conditions of transition to digital economy, a concept of economic safety considerably extends. Providing economic safety with all its components is a key factor of efficiency of new economy of Russia. The begun process of digitalization of economy, affects practically all spheres of life activity not only a single society and the state, but also the whole world in general. There is a risk of emergence of the new, earlier not identified threats not only economic safety, but also safety of the personality, society, the state. Economic safety in the conditions of digital economy is aimed at providing counteraction to the calls and threats connected with new technologies and features of digital economy. The solution of the problem of providing economic safety of digital economy, in general, first of all is connected with a solution of the questions of information security support directed to information protection and information technologies, protection of personal data and personal privacy of the Russian citizens in digital space, legal support of social and economic activity in a format of uniform digital space. Development of personnel potential as main resource of digital economy. In economic safety to digital economy of Russia prevention of imposing and an exception of loan of "others" technologies, services, the software is key. One of the main and major objectives in providing economic safety of the Russian Federation in the conditions of transition to digital economy is the exception of dependence of the domestic industry on foreign information technologies due to creation, development and widespread introduction of domestic developments and also production and rendering services on their basis.

Keywords: national security, digital economy, economic safety, risks, threats, vulnerabilities, information security, cyber crime.

ВВЕДЕНИЕ

Как было подчеркнуто в Декларации лидеров G20 (июль 2017 г.), цифровая трансформация является движущей силой глобального, инновационного и устойчивого

роста, способствующего сокращению неравенства и выводу на устойчивое развитие к 2030 г [1].

Программа масштабной трансформации экономики России и перехода на цифровую экономику, является за-

дачей стратегической важности в контексте обеспечения национальной безопасности [2] и социально-экономического благополучия страны, а так же условием сохранения суверенитета государства в условиях глобализации и ускоренного освоения и внедрения цифровых технологий другими участниками мирового рынка [3].

Согласно «Стратегии экономической безопасности Российской Федерации на период до 2030 года», «экономическая безопасность» - это состояние защищенности национальной экономики от внешних и внутренних угроз, при котором обеспечиваются экономический суверенитет страны, единство ее экономического пространства, условия для реализации стратегических национальных приоритетов Российской Федерации [4].

МЕТОДОЛОГИЯ

В условиях перехода на цифровую экономику, учитывая ее официально принятое в России определение, приведенное в указе Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы», понятие экономической безопасности значительно расширяется. Структура экономической безопасности в условиях цифровой экономики включает в себя производственно-техническую, валютно-кредитную, инфляционную, сырьевую, внешнеэкономическую, промышленную, инновационную, финансовую, инвестиционную, информационную и кадровую безопасность [5].

Экономическая безопасность в условиях цифровой экономики направлена на обеспечение противодействия вызовам и угрозам, связанным с новыми технологиями и особенностями цифровой экономики [6].

Анализ многих источников научно-технической информации, а также статистических данных показывает, что начавшийся процесс цифровизации экономики, затрагивает практически все сферы жизнедеятельности не только отдельно взятого общества и государства, но и всего мира в целом. Существует риск появления новых, ранее неидентифицируемых угроз не только экономической безопасности, но и безопасности личности, общества, государства, а так же, стремительного роста социального неравенства и дисбаланса отношений в мире в целом [7].

РЕЗУЛЬТАТЫ

Условно, возможные риски и угрозы экономической безопасности в цифровой экономике автором распределены по следующим группам (рисунок 1):

1. Риски и угрозы политического характера:

Глава рабочей группы программы «Цифровая экономика» по направлению «Информационная безопасность» Наталья Касперская отметила, что гонка за новыми технологиями цифровой экономики, новые рынки, массовые зарубежные сервисы, инвестиции, бизнес-модели, стартапы, новые деньги, новые индустрии, «перелицовка традиционных» индустрий порождает зависимость социально-экономического развития от экспортозависимой политики иностранных государств, что может нести угрозу внешнего управления экономикой страны [8].

Существует возможность информационно-технического воздействия со стороны ряда зарубежных стран на информационную инфраструктуру экономики в политических, экономических и в военных целях [7].

Информация и данные в цифровом виде являются основополагающими принципами в новой экономике. Манипулирование информацией и тиражирование ложных новостей и фактов становится новым средством для достижения различных политических целей. Спецслужбами отдельных государств ведется «информационная война», в которой СМИ и возможности информационных и цифровых технологий используются для информационно-психологического воздействия, направленного на подрыв суверенитета другого государства [7].

В последнее время существует тенденция к росту в зарубежных СМИ объема материалов, содержащих пред-

взятую оценку государственной политики Российской Федерации [9].

Существует угроза возможности трансформации политической системы вследствие влияния виртуальных социальных сообществ.

В области стратегической стабильности и равноправного стратегического партнерства возможно использование отдельными государствами технологического превосходства для доминирования в информационном пространстве. Существующее в настоящее время распределение между странами ресурсов, необходимых для обеспечения безопасного и устойчивого функционирования сети «Интернет», не позволяет реализовать совместное справедливое, основанное на принципах добросовестного управления ими [7].

Завершение расшифровки генома человека открыло возможность генетической медицины, которая не только дает возможность устранения врожденных генетических дефектов, но и позволяет перейти к новому этапу - к созданию «абсолютного человека» - евгенике. Это одна из крайне опасных и тревожных тенденций развития человечества. Поскольку генетическая терапия достаточно дорогостоящая, то она является уделом богатых. Есть опасения, что мировая элита узурпирует право использования генетических технологий модификации в собственных интересах, создав новую расу «правителей», что закрепит социальное неравенство на генетическом уровне [7].

2. Риски и угрозы финансово-экономического характера

Кардинально меняется финансово-экономический уклад.

В цифровой экономике принципиально по-иному оцениваются результаты экономического развития, в связи изменяются такие понятия как «валовой продукт», «производительность труда». К примеру, сегодня уже появились отрицательные проценты по депозитным вкладам [7].

Существующие и применяемые методики статистического учета и прогнозирования финансово-экономической деятельности отстают от цифровой экономики и остаются прежними, что ведет к возникновению опасного дисбаланса в оценке реального состояния дел в экономике [7].

Широкое распространение зарубежных сервисов определяет зависимость отечественных информационно-телекоммуникационных систем, в том числе российского сегмента сети Интернет, от зарубежных компаний. В этих условиях внедрение новых технологий будет означать инвестиции в экономики других государств без соответствующего развития отечественных отраслей. Эти инвестиции будут вестись за счет российского бюджета. Поэтому каждая попытка внедрения новых технологий должна предваряться проведением оценки ее экономической целесообразности и эффективности, возможных рисков и угроз, в том числе санкций [8].

Еще одной угрозой являются использование «криптовалюты» поскольку на сегодняшний день отсутствует их нормативно-правовое регулирование, что делает возможным распространение мошеннических схем. Кроме того, постоянная нестабильность курса, может носить умышленный характер и стать причиной финансовых потерь. Принципиальным отличием криптовалют от традиционных «денег» является отсутствие единого центра эмиссии. Государства утрачивают возможность эмитировать валюту и тем самым изменять ее обменный курс в зависимости от собственных предпочтений. Это негативно сказывается на возможности государств накапливать средства в различных фондах, поскольку стоимость хранения средств в них возрастает быстро и они становятся обузой для экономики. Снижение значимости таких понятий как «финансовый центр» и утрата контроля со стороны мировой элиты над глобальными финансовыми потоками, становится следствием еще од-

ной особенности криптовалют – их сетевой структуры [8].

3. Риски правового характера – это, прежде всего, юридическая неопределенность законодательства, регулирующего деятельность в виртуальном пространстве и правил использования новых цифровых технологий экономики, а так же отставание нормативно-правового регулирования экономических отношений в виртуальном пространстве от скорости цифровизации. Следствием этого может стать рост мошенничества и коррупции в виртуальном пространстве. Кроме того существует неопределенность правового статуса трудовых отношений в виртуальной среде цифровой экономики [10, 11].

4. Технологические риски и риски информационной безопасности – по определению Н. Касперской – это приемы и методы злоумышленников, пытающихся воспользоваться уязвимостями и незаконными возможностями новых технологий [8].

Новейшие технологии, такие как искусственный интеллект, Big Data (Большие данные), Блокчейн, Криптовалюты, Интернет вещей (включая промышленный интернет вещей) виртуальная реальность являются заимствованными технологиями [8].

ным каналом доступа к информационной системе [12].

Зависимость отечественной промышленности от зарубежных информационных технологий и средств является источником значительных угроз и уязвимостей информационной безопасности.

Основой новой экономики являются цифровые информационные технологии и данные, что в значительной степени расширяет понятие и сущность информационной безопасности.

На большинстве предприятий и компаний используется заимствованные технологии и программное обеспечение, разработанное на Западе. В случае если развитие таких сквозных технологий не будет сопровождаться созданием соответствующей отечественной производственной базы, которая обеспечивала бы их внедрение, возможно резкое увеличение импортозависимости вследствие необходимости импорта зарубежных компонентов и устройств [8].

Немаловажным является тот факт, что технологическая трансформация приводит к появлению потребности общества в специалистах нового профиля и отмиранию некоторых существующих в настоящее время профессий. Это требует заблаговременной разработки

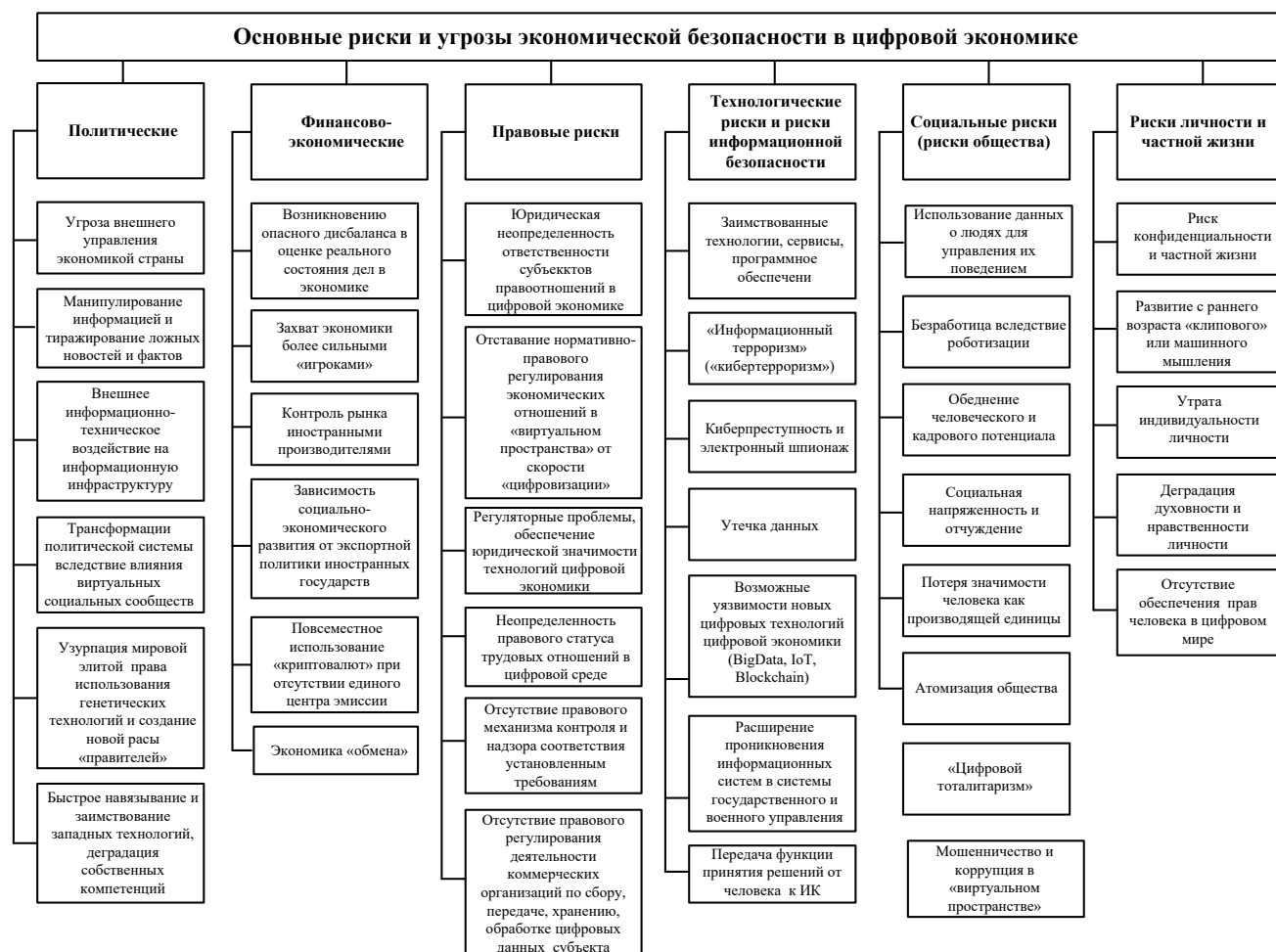


Рисунок 1 – Группы основных рисков и угроз экономической безопасности в цифровой экономике

Риски внедрения новых технологий связаны в первую очередь с появлением большого количества новых информационно-коммуникационных технологий (ИКТ). Уязвимость ИКТ может носить как характер случайной ошибки, обусловленной недоработкой на этапе реализации, так и намеренной так называемой «закладки» - умышленно внедренной уязвимости, способной вызвать сбой в работе технологии, продукта или обеспечить злоумышленникам внешний доступ и управление. Заимствование и внедрение новых ИКТ является мощ-

программ подготовки и переподготовки кадров [7].

Активная информационная борьба и против конкурентов в условиях цифровой экономики, дополняет «электронный шпионаж» и становится обычным явлением в мире рыночных отношений, в том числе и на международной экономической арене [7].

Развитие средств искусственного интеллекта, передача им задач управления комплексами вооружения и военной техники, формируют целый пласт принципиально иных задач, требующих решения юридического и морально-этического обоснования применения оружия против человека в условиях, когда решение о применении принимает машина [7].

4. Социальные риски (риски общества)

Роботизация производств и услуг несет угрозу безработицы и социальной дисгармонии, вследствие не востребованности многих существующих профессий и компетенций. Все это в совокупности ведет к возникновению серьезных проблем с занятостью населения, а дополнительно - к проблеме пенсионного и медицинского обеспечения. Государство перестает справляться с основными своими обязательствами перед гражданами, а социальная нестабильность возрастает [7].

Развитие контента, отработка технологий виртуальной и дополненной реальности создает условия дальнейшей атомизации общества - все больше времени человек будет проводить не в реальном, а в виртуальном мире. Заимствованные технологии влекут за собой деградацию собственных компетенций и обеднение человеческого и кадрового потенциала [8].

5. Риски личности и частной жизни

Глобальная цифровизация расширяет возможности преступлений против личности. Так, например, уже имеют место скандалы вокруг компьютерных видеороликов, в которых реальные видеоизображения актеров делают то, что заблагорассудится программистам. Такие «новые» возможности могут быть использованы для мошенничества, шантажа, в том числе и в политической борьбе [7].

Часто нет методов и средств расследования новых преступлений информационно-технического характера. Да и соответствующее законодательство не соответствует сегодняшним потребностям. Практически полностью утрачивается понятие «конфиденциальность» и «частная жизнь». Повсеместное развитие систем видеонаблюдения, баз персональной информации, систем анализа «больших данных» и др. делают человека фактически «прозрачным» для любого, кто располагает доступом к его персональной информации [7].

Распространение электронного контроля за жизнью, настроениями, планами граждан, политических организаций и т.д.

Усиление электронной слежки - нередкое социальное следствие прогресса информационных технологий. Правящие слои переходят от примитивного подслушивания телефонных разговоров, контроля переписки, использования «детекторов лжи» к тотальному цифровому (компьютерному) контролю, «кибернадзору» за населением [7].

Глобальная цифровизация несет риски развития личности. Компьютеризация с раннего возраста приводит к развитию у детей машинного (так называемого «клипового») мышления (моментальное, математически-линейное, визуальное, фрагментарное, скоростное и поверхностное) в ущерб системному (многоплановое, целостное, гуманитарное, философское, причинно-следственное, комплексно целевое). В дальнейшем сформированное «клиповое» мышление не позволит нелинейно, творчески и логично мыслить [8].

Даже личностные, человеческие ценности теряют традиционный смысл.

У компьютера нет нравственности. Учитывая, что нравственность - исключительно чувственное понятие, она исчезает вместе со свойственными человеку эмоциями.

Способность соучастия - эмпатии, этой главной цели и критерия развития личности - исчезает напрочь [7].

ВЫВОДЫ

Подводя итоги всего выше указанного, справедливо отметить, следующее:

- цифровая трансформация является движущей силой глобального, инновационного и устойчивого роста, способствующего сокращению неравенства и выходу на устойчивое развитие, что является приоритетной задачей стратегии национальной безопасности нашей страны. В этих условиях, обеспечение экономической безопасности со всеми ее составляющими является ключе-

вым фактором эффективности новой экономики России.

Переход на цифровую экономику, учитывая ее определение, приведенное в указе Президента РФ В.В. Путина «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» радикально изменяет понимание и сущность экономической безопасности.

Решение проблемы обеспечения экономической безопасности цифровой экономики, в целом, в первую очередь связано с решением вопросов обеспечения информационной безопасности, направленных на защиту информации и информационных технологий, защиты персональных данных и неприкосновенности частной жизни российских граждан в цифровом пространстве, правовое обеспечение социально-экономической деятельности в формате единого цифрового пространства. Развитие кадрового потенциала как главного ресурса цифровой экономики. Ключевым в экономической безопасности цифровой экономики России является недопущение навязывания и исключения заимствования «чужих» технологий, сервисов, программного обеспечения.

Одной из основных и важнейших задач в обеспечении информационной безопасности Российской Федерации в условиях перехода на цифровую экономику является исключение зависимости отечественной промышленности от зарубежных информационных технологий за счет создания, развития и широкого внедрения отечественных разработок, а также производства продукции и оказания услуг на их основе.

Президент РФ В.В. Путин, в своем послании Федеральному собранию 1 декабря 2016 года, предложил «запустить масштабную системную программу развития экономики нового технологического поколения, так называемой цифровой экономики», в реализации которой следует «копироваться именно на Российские компании, научные, исследовательские и инжиниринговые центры страны» [3]. Последнее является одним из ключевых направлений обеспечения не только экономической, но и национальной безопасности и будущего России в целом.

СПИСОК ЛИТЕРАТУРЫ:

1. Манахова И.В. Цифровое будущее и глобальная экономическая безопасность // Экономическая безопасность и качество. 2018. № 1 (30). URL: http://www.seun.ru/content/nauka/5/1/doc/Economical%20security_1_30_2018.pdf
2. Указ Президента Российской Федерации от 31.12.2015 г. № 683 «О стратегии национальной безопасности Российской Федерации». Режим доступа - URL: <http://www.kremlin.ru/acts/bank/40391>
3. Развитие Цифровой экономики в России. Программа до 2035 года. / <http://spkurdyumov.ru>. Режим доступа: URL: <http://spkurdyumov.ru/uploads/2017/05/strategy.pdf>
4. Указ Президента Российской Федерации от 13.05.2017 г. № 208 «О стратегии экономической безопасности Российской Федерации на период до 2030 года». Режим доступа - URL: <http://www.kremlin.ru/acts/bank/41921>
5. Скорев М.М., Графова Т.О., Бакина С.С. Стратегическая устойчивость в условиях цифровой экономики - Кадровый и финансовый аспекты // Наука и образование: хозяйство и экономика; предпринимательство: право и управление. 2018 № 2 <93>. С. 24-29.
6. Графова Т.О., Горбик Д.А. Система обеспечения экономической безопасности предприятия и обеспечения национальной безопасности Материалы Всероссийской национальной научно-практической конференции. 2017. С. 21-24.
7. Гриняев С.Н. Угрозы цифровой эпохи: краткий анализ возможных последствий Режим доступа - URL: <http://csef.ru/ru/nauka-i-obshchestvo/445/ugrozy-cifrovoj-epohi-kratkij-analiz-vozmozhnyh-posledstvij-7875>
8. Цифровая экономика и риски цифровой колонизации. Н. Касперская, развернутые тезисы выступления на Парламентских слушаниях в Госдуме Режим доступа - URL: <http://narodosnova.ru/2018/04/tsifrovaya-ekonomika-i-riski-tsifrovoj-kolonizatsii.html>
9. Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» Режим доступа - URL: <http://static.kremlin.ru/media/acts/files/0001201612060002.pdf>
10. Стрижов С.А. Барьеры и риски цифровой экономики / Инновации. Инвестиции (118) УЭК. 12/2018 / Институт бизнеса и делового администрирования Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации. Режим доступа - URL: http://uecs.ru/index.php?option=com_flexicontent&view=items&id=5330
11. Bainan В.А. Правовое регулирование цифровой экономики.

Режим доступа – URL: <https://urfac.ru/?p=725>

12. Черняков М.К., Чернякова М. М. Инновационные риски цифровой экономики // Национальные приоритеты России. 2018. №4 (31).
URL: <https://cyberleninka.ru/article/n/innovatsionnye-riski-tsifrovoy-ekonomiki>

Статья поступила в редакцию 22.10.2019

Статья принята к публикации 27.02.2020