

<https://doi.org/10.54220/v.rsue.1991-0533.2026.93.1.011>
УДК 338

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ

Миронова О. А.^{1*}, Хвоевская Л. И.²

¹ Ростовский государственный
экономический университет (РИНХ),
Ростов-на-Дону, Россия

² Донской государственный
технический университет,
Ростов-на-Дону, Россия

* lady.sensey2010@yandex.ru

Аннотация. *Введение.* Современное развитие общества и экономики характеризуется противоречивыми явлениями и процессами, обуславливающими неопределенность и изменчивость. К их числу относятся трансформация миропорядка и формирование новой модели глобализации, постиндустриальный переход, повсеместное внедрение цифровых технологий во все сферы человеческой деятельности. В условиях появления новых рисков и угроз задачи обеспечения национальной и экономической безопасности России приобретают все более актуальный характер. *Материалы и методы.* Теоретико-методологической основой проведенного исследования послужили работы российских и зарубежных авторов, акцентирующих внимание на вопросах обеспечения экономической безопасности в условиях нестабильности и неопределенности внешней среды, а также изучающих различные аспекты цифровизации и постиндустриализации экономики. *Результаты исследования.* В статье рассмотрены важнейшие проблемы обеспечения экономической безопасности России в условиях развития и широкого внедрения в производственную практику и жизнь общества цифровых технологий при сохранении и расширении спектра экономических санкций Запада. Выявлены ключевые угрозы экономической безопасности страны, идущие из цифрового сектора. На основе проведенного анализа сделан вывод о необходимости разработки национальной стратегии обеспечения цифровой безопасности и разработан комплекс мероприятий по ее обеспечению на региональном уровне. *Обсуждение и заключение.* Учитывая двойственный характер влияния процессов информатизации и цифровизации современной стадии на общество и экономику, делается вывод о необходимости адекватного управления рисками и своевременной минимизации или нейтрализации вызовов и угроз со стороны цифрового пространства, что повысит доверие хозяйствующих субъектов и населения к цифровым инструментам и технологиям, позволит эффективно реализовывать преимущества цифровой экономики, обеспечить рост производительности труда и повышение уровня жизни за счет внедрения передовых технологий.

Ключевые слова: экономическая безопасность, инновации, цифровизация, цифровые технологии, цифровое неравенство.

Для цитирования: Миронова О. А., Хвоевская Л. И. Проблемы обеспечения экономической безопасности России в условиях цифровизации экономики. *Вестник Ростовского государственного экономического университета (РИНХ)*. 2026;1(33):130-142. DOI: 10.54220/v.rsue.1991-0533.2026.93.1.011

Research article

JEL F63 O32

**PROBLEMS OF ENSURING RUSSIA'S ECONOMIC SECURITY
IN THE CONTEXT OF DIGITALIZATION OF ECONOMICS****Mironova O.^{1*}, Khvoevskaya L.²**¹ *Rostov State University of Economics,
Rostov-on-Don, Russia*² *Don State Technical University,
Rostov-on-Don, Russia*** lady.sensey2010@yandex.ru*

Annotation. *Introduction.* The current development of society and the economy is characterized by contradictory phenomena and processes that cause uncertainty and variability. These include the transformation of the world order and the formation of a new model of globalization, the post-industrial transition, and the widespread introduction of digital technologies in all areas of human activity. In the face of new risks and threats, the task of ensuring Russia's national and economic security becomes increasingly urgent. *Materials and methods.* The theoretical and methodological basis of this study was provided by the works of Russian and foreign authors who focus on ensuring economic security in conditions of instability and uncertainty in the external environment, as well as on studying various aspects of digitalization and post-industrialization of the economy. *Research results.* The article discusses the most important issues of ensuring Russia's economic security in the context of the development and widespread implementation of digital technologies in production and society, while maintaining and expanding the range of economic sanctions imposed by the West. The article identifies key threats to the country's economic security that originate from the digital sector. Based on the analysis conducted, the article concludes that it is necessary to develop a national strategy for ensuring digital security and proposes a set of measures to ensure digital security at the regional level. *Discussion and conclusion.* Given the dual nature of the impact of informatization and digitalization processes at the current stage on society and the economy, a conclusion is drawn about the need for adequate risk management and the timely minimization or neutralization of challenges and threats from the digital space, which will increase the confidence of economic entities and the population in digital tools and technologies, allow for the effective realization of the advantages of the digital economy, ensure growth in labor productivity and an improvement in the standard of living through the introduction of advanced technologies.

Keywords: economic security, innovation, digitalization, digital technologies, digital inequality.

For citation: Mironova O., Khvoevskaya L. Problems of Ensuring Russia's Economic Security in the Context of Digitalization of Economics. *Vestnik of Rostov State University of Economics (RINH)*. 2026;1(33):130-142. DOI: 10.54220/v.rsue.1991-0533.2026.93.1.011

Введение

Современная эпоха геополитических трансформаций, обусловленных накоплением системных противоречий сформировавшегося к началу XXI в. ми-

ропорядка, а также стремительное развитие цифровых технологий, постиндустриальный переход и превращение информации в важнейший фактор производства актуализируют проблемы обеспе-

чения экономической безопасности России на государственном и региональном уровне.

Внедрение цифровых технологий практически во все сферы человеческой жизни приводит к изменению старых и появлению новых формальных и неформальных институтов, серьезным социально-экономическим преобразованиям, вызывает к жизни совершенно новые риски и угрозы, с которыми человечество не сталкивалось ранее, и поэтому в настоящее время лишь формирует первичный опыт осознанного противостояния им.

Цифровизация экономики, проникая во все ее отрасли и секторы, фактически стирает национальные границы. Именно поэтому изначально глобализация началась в финансовом секторе, где в первую очередь стали распространяться новые информационные коммуникации. В настоящее время цифровая среда активно влияет на производство, формируя и изменяя спрос, трансформируя производственные процессы, создавая виртуально-электронную среду и новую культуру потребления. Таким образом, процессы цифровизации изменяют изнутри как внешнюю, так и внутреннюю среду производства и потребления и в традиционных, и в новых отраслях экономики, постепенно размывая границы между первыми и вторыми.

Процессы развития современных информационно-коммуникационных технологий (ИКТ) приводят к формированию систем Big Data (больших данных), превращающихся в своеобразный цифровой актив государств и отдельных экономических субъектов. Цифровое пространство лишено физических границ, что делает его открытым практически для любого пользователя в любой точке земного шара при наличии у него возможностей доступа. С одной стороны, это упрощает получение необходимой для пользователей информации, в том числе о потенциальных клиентах и поставщиках, товарах и услугах, ценах, качестве, наличии конкурентов,

возможность находить ответы на интересующие вопросы.

Цифровые технологии способствуют оптимизации бизнес-процессов, снижению затрат, росту эффективности производства, улучшению качества продукции и повышению конкурентоспособности национальных производителей и экономики в целом. С другой стороны, стремительное распространение цифровых технологий открывает широкий спектр возможностей для их недобросовестного использования как в экономической, так и в социально-политической сфере. К числу угроз экономической безопасности России, обусловленных использованием цифровых технологий, можно отнести кибератаки на государственные и финансовые институты, предприятия, объекты критической инфраструктуры, в том числе информационной, получение доступа к конфиденциальной информации, сбои в работе и вывод из строя систем управления в различных сферах и секторах, распространение фейковой информации, в том числе с целью манипуляций на финансовых рынках, иные виды угроз, способных нанести существенный ущерб экономике страны и спровоцировать серьезные социально-политические потрясения.

Все вышеизложенное обуславливает необходимость выявить основные угрозы экономической безопасности России в условиях развития процессов цифровизации экономики и определить основные способы их нейтрализации или минимизации.

Материалы и методы

В качестве теоретико-методологической базы исследования выступают опубликованные в отечественной и зарубежной печати работы ученых и экспертов, посвященные вопросам теории и практики обеспечения экономической безопасности на макро- и мезоуровне, а также труды российских и зарубежных исследователей в области проблем цифровой трансформации.

Методологический аппарат исследования представлен общенаучными методами познания, включающими диалектический метод, анализ и синтез, абстрагирование, аналогии, индуктивный и дедуктивный методы, а также системный анализ, системно-структурный и конкретно-исторический методы.

В качестве методологической основы анализа угроз экономической безопасности был использован риск-ориентированный подход, позволивший выявить наиболее актуальные угрозы экономической безопасности России, сопряженные с развитием процессов цифровизации, их причины, последствия возможной реализации, а также предложить комплекс мероприятий, направленных на предотвращение или минимизацию данных угроз на макро- и мезоуровне.

Информационно-эмпирическую базу исследования представляют нормативно-правовые акты РФ, а также материалы Росстата и данные, предоставленные Центрами общественных связей ФСБ и МВД России.

Результаты исследования

В современных условиях в число важнейших задач обеспечения экономической безопасности входит не только нейтрализация реализовавшихся угроз или минимизация их последствий, но и превентивные меры, направленные на предотвращение развития негативных тенденций, которые существуют в зачаточном состоянии или могут сформироваться в будущем, прогнозирование вызовов и угроз, к реализации которых нужно быть готовыми уже сегодня. Процессы цифровизации, принявшие в настоящее время всеобщий характер, являются не только фактором экономического развития, но и серьезным вызовом, проявляющимся на всех уровнях экономической системы – от глобального до микроуровня.

Для России в настоящее время задачи обеспечения экономической безопасности усложняются с учетом санкционного давления и в целом враждебного отношения ряда западных стран. Выделим актуальные проблемы, связанные с процессами цифровизации экономики (рис. 1).



Рисунок 1 – Актуальные проблемы экономической безопасности России в условиях цифровизации экономики

Figure 1 – Current issues of Russia's economic security in the context of digitalization of the economy

Одной из наиболее очевидных угроз является рост безработицы вследствие вытеснения человеческого труда из различных сфер профессиональной деятельности технологиями искусственного интеллекта. С одной стороны, это приведет к сокращению рабочих мест, с другой – к появлению новых профессий, связанных с ИКТ, для овладения компетенциями в которых работникам необходимо будет проходить профессиональную переподготовку.

Данная угроза может быть связана также с проблемой цифрового неравенства на поколенческом уровне: обучение компьютерным технологиям будет практически элементарным для зумеров (и в перспективе альфа), родившихся в начале XXI в. и обладающих «врожденной» цифровой грамотностью, достаточно легким для миллениалов, более сложным для иксов, которые хорошо осваивают данные технологии, однако по степени уверенности владения ими все же проигрывают своим более младшим коллегам, очень тяжелым для беби-бумеров, многие из которых сохраняют работоспособность, физические возможности и желание трудиться даже после выхода на пенсию.

Проблема цифрового неравенства представляет угрозу также на иных уровнях, будучи связана, в частности, с разными возможностями граждан с различным уровнем доходов, жителей городской и сельской местности, где зачастую доступ к интернет-коммуникациям ограничен, что обусловлено достаточно высокой стоимостью как цифровой инфраструктуры, так и цифровых продуктов. Также данная проблема актуальна для предприятий, регионов вследствие неравномерности стартовых возможностей и условий для хозяйствующих субъектов на микро- и мезоуровне.

Существенная стратификация по уровню технологического и цифрового развития прослеживается и на уровне национальных экономик, где выделяются как страны, в которых процессы постиндустриализации начались еще в конце XX

столетия, так и государства, национальные производители которых зависят от зарубежных поставок высокотехнологичной, в том числе цифровой, продукции. В настоящее время на мировом рынке цифровых технологий доминируют крупные ТНК: 80 % глобального ВВП производят 10 % мировых корпораций, на долю России приходится всего лишь 2-3 % мирового рынка. В результате страны, не являющиеся лидерами в цифровом сегменте, сталкиваются с ослаблением технологической и, как следствие, экономической безопасности на национальном, региональном и отраслевом уровне [1].

Региональный аспект данной проблемы для России связан как со значительной протяженностью территории, географическим положением различных регионов, разнообразием природно-климатических условий, так и с неравномерностью социально-экономического развития различных субъектов РФ. Так, суровый климат Сибири и Дальнего Востока не позволяет широко использовать традиционные для других территорий страны наземные базовые станции и кабельные сети, которые заменяются использованием менее надежного, но дорогого спутникового интернета. В то же время цифровые технологии ускоренными темпами развиваются в Москве и Московской области, Татарстане, Краснодарском крае, иных высокодоходных российских регионах, еще больше увеличивая их экономическое лидерство. Такая ситуация чревата «цифровой стратификацией» регионов, углублением разрыва в уровне социально-экономического и научно-технического разрыва между ними.

Существует также весьма ощутимая угроза монополизации бизнеса крупными цифровыми экосистемами, охватывающими в настоящее время практически все сферы экономической жизни: от заказа продуктов питания и покупки товаров на маркетплейсах до финансовых операций, обладающих значительными конкурентными преимуществами по сравнению с малыми и средними предприятиями,

которые не в силах конкурировать с компаниями-гигантами.

Неменьшую опасность представляют и угрозы, связанные с недобросовестным использованием персональных данных, доступ к которым в цифровой среде значительно упрощается, в том числе с помощью применения мошеннических схем, число которых растет. Современные цифровые технологии позволяют взламывать базы данных и атаковать объекты дистанционно практически из любой точки земного шара. С данным комплексом проблем связаны также этические аспекты использования цифровых технологий, которые позволяют автоматизированным системам не только собирать и анализировать информацию, но и использовать ее в различных целях, что приводит к вопросу о правовой ответственности за действия и решения, которые входят в компетенцию технологии [2]. Кроме того, существенную угрозу может представлять применение цифровых технологий террористическими организациями в целях получения доступа к объектам государственной тайны, вооружениям, критической инфраструктуре, государственным финансам и т. д. Актуальными остаются также проблемы распространения фейковой информации, кибертерроризма, риски появления кибероружия.

Ответом на совершенствование систем безопасности государственных органов и крупных компаний становятся новые способы и схемы совершения киберпреступлений. Федеральная служба безопасности России сообщила о регистрации более 640 тыс. случаев дистанционного мошенничества за 2024 г. Общий ущерб от киберпреступлений составил свыше 170 млрд руб. Об этом 7 мая 2025 г. заявил Центр общественных связей ФСБ России. В 2024 г. в России зафиксированы 765,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Это составляет примерно 40 % от об-

щего числа противоправных деяний. Такие данные в конце января 2025 г. обнародовало МВД РФ. В отчете ведомства говорится, что в 2024 г. общее количество киберпреступлений в России увеличилось на 13,1 % по сравнению с предыдущим годом. При этом в ИТ-сфере совершены 369,3 тыс. тяжких и особо тяжких противоправных деяний, что на 7,8 % больше в годовом исчислении. В значительной степени этот фактор повлиял на рост в 2024 г. общего числа тяжких и особо тяжких преступлений на 4,8 % [3].

Помимо кибератак, недобросовестного и преступного использования цифровых технологий существуют также угрозы и опасности, связанные со сбоями в их работе, ошибками программного обеспечения, отключениями электроэнергии, магнитными бурями и иными космическими явлениями, приводящими к сбоям в работе оборудования. Учитывая, что в настоящее время цифровые технологии пронизывают практически все отрасли, крупный сбой может привести к технологическому коллапсу и парализовать работу различных организаций и структур.

Еще одной проблемой, обусловленной существованием комплекса рассмотренных угроз экономической безопасности России, связанных с процессами цифровизации, является низкая степень доверия населения цифровым технологиям и цифровым инструментам, стремление избежать или максимально снизить степень пользования ими как потенциально опасными и ненадежными.

Подобная ситуация является фактором, сдерживающим распространение цифровых технологий и, как это ни парадоксально, одновременно снижает уровень безопасности цифровых инструментов в силу цифровой неграмотности части населения.

Таким образом, перечисленные выше угрозы, идущие со стороны цифрового сектора российской экономики, позволяют сделать вывод о его уязвимости и

необходимости выделить цифровую безопасность (кибербезопасность) в отдельный элемент системы экономической и информационной безопасности России. Это предполагает разработку и реализацию стратегии цифровой безопасности на федеральном и региональном уровне, типовые цели которой могут включать:

- разработку четкой нормативно-правовой базы в области регулирования цифровых процессов, а также методологии перехода на цифровые технологии;

- развитие национальных средств цифровой коммуникации, средств и систем передачи информации, ИКТ, электроники и вычислительной техники;

- минимизацию зависимости российских компаний от зарубежных программных продуктов и цифровых технологий, внедрение отечественных разработок в процессы производства и управления;

- создание благоприятных условий для развития отечественного сектора цифровых технологий, инструментов и программных продуктов, электронной компонентной базы, что позволит обеспечить потребности цифрового сегмента национального рынка и повысить конкурентоспособность на внешних рынках;

- предотвращение потенциальных угроз кибербезопасности, своевременное обнаружение угроз цифрового характера и оперативное реагирование на них;

- разработку надежных цифровых продуктов для всех категорий пользователей;

- разработку национальных стандартов киберфизических систем, систем контроля и доступа к различным базам данных, в том числе в социальных сетях и мессенджерах;

- создание федеральных и региональных служб оперативного реагирования на инциденты в цифровом пространстве;

- поддержку государственных и частных организаций и операторов, обеспечивающих безопасность киберпространства;

- реализацию программ цифровой грамотности для широкого круга пользователей. С учетом динамичного характера развития цифровых технологий и связанных с ними опасностей и угроз программы цифровой грамотности должны постоянно обновляться, а пользователи – иметь возможность повышать степень своей осведомленности о них по мере их возникновения и распространения.

В целях нивелирования цифрового неравенства на мезоуровне представляется актуальным развитие процессов цифровизации в регионах, где следует создавать благоприятные условия для инвестирования местных производителей в развитие цифровых технологий и привлечения в данные сферы деятельности высококвалифицированных специалистов.

К числу мер, обеспечивающих повышение уровня экономической безопасности в условиях цифровизации в регионах России, можно отнести меры, представленные на рисунке 2.

Реализация всех перечисленных мероприятий в целом направлена на достижение российскими пользователями на макро-, мезо- и микроуровне уровня цифровой зрелости, актуального современному уровню развития цифровых технологий и обусловленных им вызовов и угроз.

Таким образом, экономическая безопасность России на всех ее уровнях в условиях цифровизации экономики во многом будет определяться тем, насколько быстро и эффективно удастся обеспечить высокую степень цифровой зрелости юридических и физических лиц, органов власти, всех хозяйствующих субъектов.



Рисунок 2 – Комплекс мероприятий, способствующих повышению уровня экономической безопасности регионов России в условиях цифровизации
 Figure 2 – A set of measures to improve the economic security of Russian regions in the context of digitalization

Обсуждение и заключение

Исследования экономической безопасности, определение ее содержания, понятия и структуры имеют длительную историю и восходят к началу 30-х гг. XX в., когда в 1934 г. во время Великой депрессии в США впервые был создан Федеральный комитет по экономической безопасности, деятельность которого должна была способствовать снижению безработицы и обеспечивать защиту экономических интересов предпринимательского сектора [4]. Однако наиболее активные исследования вопросов экономической безопасности начались в эпоху глобализации в связи со значительным увеличением числа глобальных рисков, прямо или косвенно влияющих на состояние национальных экономических систем в условиях их открытости. Так, в начале 90-х гг. прошлого столетия Б. Бузан определил экономическую безопасность как состояние экономики, в котором обеспечено экономическое благополучие субъектов, вовлеченных в общественные отношения. При этом, согласно его представлениям, стабильность внутреннего рынка зависит от внешних факторов, отрицательное воздействие которых нивелируется резервами хозяйствующих

субъектов, что позволяет сохранить их стабильное состояние [5].

В российской научной литературе экономическую безопасность принято рассматривать как состояние национальной экономики и органов власти, обеспечивающее гарантированную защиту национальных интересов страны и возможности поступательного социально-экономического развития в условиях внешних и внутренних вызовов [6]. К числу таких внешних вызовов в том числе может быть отнесена и цифровизация экономики. Данное понятие является дискуссионным и до сих пор не имеет конкретной дефиниции ни в зарубежной, ни в отечественной экономической литературе, что обусловлено многогранностью и неоднозначностью последствий данного процесса.

Цифровизацию часто характеризуют как одну из составляющих процесса постиндустриализации, формирования информационного общества, где информация и знания превращаются в важнейшие факторы производства. Данный аспект может предполагать еще более широкую трактовку понятия цифровизации как процесса формирования глобальной цифровой среды, которая может рассматриваться с помощью различных подходов:

– технологического, понимающего под цифровой средой созданное человеком обособленное пространство (киберпространство) объектов, широко применяющихся в компьютерных сетях, а также весь континуум компьютерных и сетевых технологий, базовым компонентом которого является интернет;

– медийного, с позиций которого цифровая среда рассматривается как электронная медийная платформа и совокупность информационно-коммуникационных технологий общения, стирающих границы между создателями и потребителями контента, производством и потреблением информации. При этом основополагающую роль играют электронные СМИ.

Интеграция данных подходов позволяет говорить о двух процессах, развивающихся параллельно друг другу, но оказывающих друг на друга взаимное воздействие: цифровизации как процессе повсеместного распространения цифровых технологий, и медиатизации, под которой в данном случае понимается проникновение электронных медиа во все основные сферы жизнедеятельности людей, от политики и экономики до межличностного общения.

Взаимосвязь между цифровизацией и медиатизацией осуществляется посредством перехода различных аспектов социально-культурной жизни в цифровой формат. Также следует различать понятия цифровой экономики как специфического типа хозяйственной системы, характеризующегося широким применением и активным внедрением в процессы производства и управления цифровых технологий сбора, хранения, обработки и передачи информации, и цифровизации как процесса перехода к данному типу экономики, формирования новой системы социально-экономических отношений, опосредованных использованием цифровых коммуникаций [7].

Таким образом, цифровизация предполагает переход от традиционных форм ведения хозяйственной деятельности с использованием доцифровых технологий к цифровой экономике как более прогрессивному способу ведения хозяйственной деятельности, основанному на использовании современных информационных технологий и их продуктов.

Специфические особенности цифровой экономики представлены на рисунке 3.

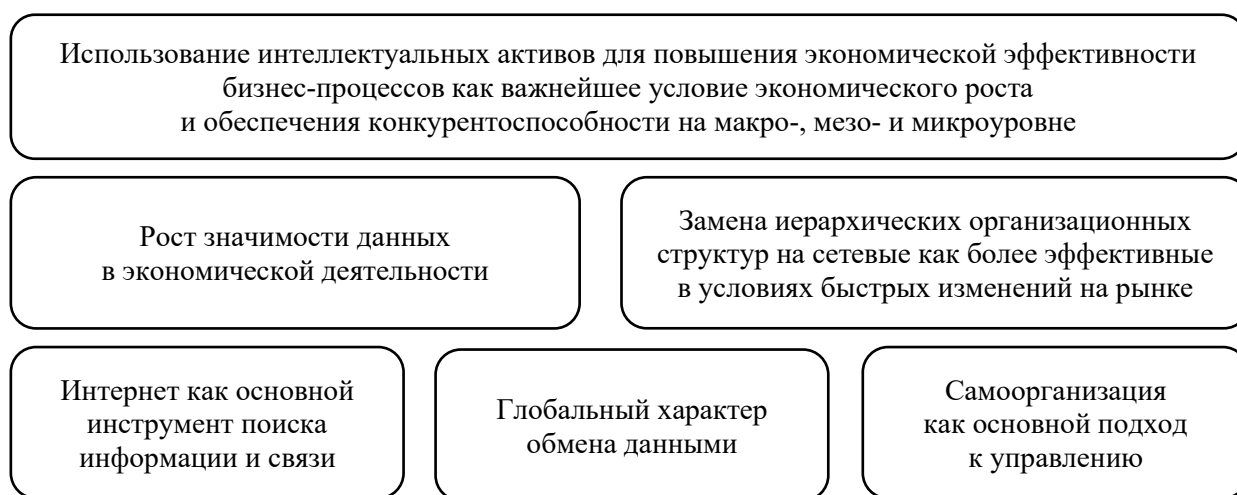


Рисунок 3 – **Важнейшие специфические особенности цифровой экономики**

Figure 3 – **The most important specific features of the digital economy**

Обеспечение экономической безопасности в цифровой экономике должно опираться на адекватную современным

вызовам нормативно-правовую базу, которая в России в настоящее время представлена пакетом законодательных актов,

направленных на регулирование и защиту информации на уровне государства, организации, отдельной личности. К их числу относятся, в частности, Конституция РФ, Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента РФ от 05.12.2016 № 646, федеральные законы РФ «О государственной тайне», «Об информации, информационных технологиях и о защите информации», «О персональных данных», «Об электронной подписи» и др. [8].

Поскольку технологии киберпреступлений развиваются параллельно технологиям защиты от них и даже с опережением последних, можно ожидать, что в ближайшей перспективе правовое регулирование и стандарты в области цифровой безопасности будут значительно отставать и от процессов цифровизации в целом, и от роста числа технологий и инструментов, позволяющих использовать данные процессы в преступных целях. Это будет приводить к постоянному росту финансовых затрат со стороны государства и бизнеса на защиту цифровой безопасности на макро- и микроуровне, что может оказаться неподъемным для малых и средних предприятий. Актуальной задачей является обеспечение эффективного взаимодействия и сотрудничества между государством и бизнесом, разработка мер, направленных на безопасное осуществление экономической деятельности в цифровой среде.

Наряду с нормативно-правовой базой, России необходимы создание и четкое согласованное взаимодействие в цифровой среде федеральных и региональных органов управления, разработка национальных программ, направленных на защиту данных и объектов инфраструктуры, учет региональной специфики при решении задач обеспечения безопасности в цифровой среде, развитие региональной информационно-коммуникационной инфраструктуры, мониторинг рынков информационных продуктов и услуг. Представляется важным найти оптимальные пропорции между применением мер

жесткого регулирования в отношении обеспечения цифровой безопасности и возможностей предприятий малого и среднего бизнеса адаптироваться к введению указанных мер, иными словами, найти эффективное соотношение между ограничениями и свободой в цифровой экономике. В настоящее время в России уже реализуется ряд мероприятий, направленных на решение этих задач.

На текущий момент на государственном уровне реализуется ряд проектов, направленных на развитие как методов защиты персональных данных, так и на разработку превентивных мер по предотвращению киберпреступлений. Так, с 2021 г. по настоящее время Специализированным подразделением по надзору за исполнением законов в сфере информационных технологий и защиты информации было предотвращено либо устранено более 155 тысяч нарушений в сфере цифровых технологий и закрыт доступ более чем к 40 тыс. фишинговых сайтов [8].

С 14 августа 2025 г. в России действует комплексный план мероприятий по реализации Концепции государственной системы противодействия преступлениям, совершенным с помощью ИКТ. Целью реализации Концепции является системная борьба с киберпреступностью и создание безопасной цифровой среды для физических и юридических лиц посредством:

- ужесточения или введения административных и уголовных наказаний за цифровые преступления;
- усиления межведомственной координации усилий и взаимодействия между правоохранительными и контролирующими органами (МВД, ФСБ, Генеральная прокуратура, Следственный комитет РФ, Минцифры, Роскомнадзор) и операторами связи, интернет-провайдерами и иными организациями, предоставляющими цифровые услуги, при выявлении признаков преступлений с цифровым компонентом;
- проведение мероприятий по повышению цифровой и финансовой грамотности населения с целью профилактики правонарушений;

– разработка передовых технологий, реализация технических мер, направленных на борьбу с мошенничеством в цифровой среде, в частности создание единого реестра адресов официальных сайтов интернет-магазинов для борьбы с сайтами-двойниками, фишинговыми ресурсами, расширение возможностей использования технологий искусственного интеллекта для борьбы с преступлениями в цифровой среде.

Значительный интерес представляет создаваемая в настоящее время платформа ФинЦЕРТ, представляющая собой проект, объединяющий усилия государства, бизнеса, банков, ведущих операторов сотовой связи, владельцев социальных сетей и разработчиков мобильных приложений по обмену информацией о различных нарушениях в киберпространстве, мошеннических действиях и иных инцидентах, которые можно рассматривать как потенциальные или реальные угрозы экономической безопасности граждан, хозяйствующих субъектов, государства. В настоящее время платформа уже используется для отслеживания операций с незаконным использованием пластиковых карт.

В качестве иных мер, которые могут быть использованы для обеспечения экономической безопасности в условиях цифровизации экономики в России при объединении усилий органов власти, бизнеса и научного сообщества, предлагаются разработка системы налоговых льгот и финансовой поддержки компаний, активно разрабатывающих и внедряющих меры по повышению цифровой безопасности, осуществление регулярного обмена информацией о лучших практиках в области защиты баз данных, проведение информационных кампаний, знакомящих население, особенно представителей старших поколений, с технологиями современных киберпреступлений и способами защиты от них, при использовании не только цифровых ресурсов, в которых старшие поколения

представлены менее активно, но и традиционных офлайн-каналов и СМИ.

Таким образом, процессы информатизации и цифровизации, характерные для современной стадии развития НТП, оказывают двойственное воздействие на общество и экономику, одновременно способствуя повышению экономической эффективности и снижению производственных затрат, но при этом увеличивая число рисков и угроз экономической безопасности на уровне государств, регионов, предприятий и граждан. Для обеспечения экономической безопасности на всех уровнях важное значение имеют управление рисками и своевременная минимизация или нейтрализация вызовов и угроз со стороны цифрового пространства, что позволит повысить доверие хозяйствующих субъектов и населения к цифровым инструментам и технологиям, будет способствовать более эффективной реализации социально-экономических преимуществ цифровой экономики, росту производительности труда, повышению уровня жизни. При этом одной из важных задач выступает финансовое и административное стимулирование процессов цифровизации в субъектах Российской Федерации.

Список литературы

1. Радченко, А. А. Стратегическая роль цифровых экосистем в обеспечении экономической безопасности в условиях нестабильной внешней среды в целях обеспечения экономической безопасности страны // Цифровая экономика: проблемы и перспективы развития : сборник научных статей 5-й Всероссийской научно-практической конференции, Курск, 15 декабря 2023 г. – Курск, 2023. – С. 341-345.
2. Угрозы экономической безопасности организаций в условиях цифровой трансформации экономики / А. Л. Дыхова, Н. А. Волчкова, Е. Г. Волосова // Проблемы научно-практической деятель-

ности. Поиск и выбор инновационных решений : сборник статей Международной научно-практической конференции. – Уфа, 2021. – С. 131-135.

3. Число киберпреступлений в России [Электронный ресурс]. – URL: https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России (дата обращения: 20.03.2026).

4. Кузнецова, М. В. Механизм повышения экономической безопасности на основе инновационных и цифровых преобразований в экономике : дис. к. э. н. – 2022. – 154 с.

5. Buzan, B. New Patterns of Global Security in the Twenty-First Century // International Affairs. – 1991. – Vol. 67, № 3. – P. 431-451.

6. Савельев, А. В. Актуальные угрозы и риски экономической безопасности РФ в условиях цифровых тенденций // Россия в глобальном мире : материалы II Всероссийской научно-практической конференции молодых ученых, Тверь, 9 декабря 2022 г. – Тверь, 2023. – С. 181-187.

7. Дыхова, А. Л., Семина, К. И. Цифровая экономика и проблемы экономической безопасности // Стратегии исследования в общественных и гуманитарных науках : сборник научных трудов по материалам Международной научно-практической конференции, Белгород, 31 января 2022 г. – Белгород, 2022. – С. 71-76.

8. Евстигнеева, А. А. Правовое регулирование выявления и пресечения киберпреступлений в Российской Федерации // Государственное и муниципальное управление в России: состояние, проблемы и перспективы : материалы 19-й Всероссийской научно-практической конференции, Пермь, 20-21 марта 2025 г. – Пермь, 2025. – С. 86-90.

References

1. Radchenko, A. Strategic Role of Digital Ecosystems in Ensuring Economic Security in an Unstable External Environment for Purposes of Ensuring the Country's

Economic Security // Digital Economy: Problems and Prospects of Development : collection of scientific articles of 5th All-Russian scientific-practical conference, Kursk, December 15, 2023. – Kursk, 2023. – P. 341-345.

2. Threats to the Economic Security of Organizations in Context of Digital Transformation of the Economy / A. Dykhova, N. Volchkova, E. Volosova // Problems of Scientific and Practical Activity. Search and Selection of Innovative Solutions : collection of articles of International scientific-practical conference. – Ufa, 2021. – P. 131-135.

3. Number of Cybercrimes in Russia [Electronic resource]. – URL: https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России (date of access: 20.03.2026).

4. Kuznetsova, M. Mechanism for Enhancing Economic Security on the Basis of Innovative and Digital Transformations in Economy : diss. of Cand. Sci. (Econ.). – 2022. – 154 p.

5. Buzan, B. New Patterns of Global Security in the Twenty-First Century // International Affairs. – 1991. – Vol. 67, № 3. – P. 431-451.

6. Saveliev, A. Current Threats and Risks to the Economic Security of Russian Federation in the Context of Digital Trends // Russia in Global World : proceedings of 2nd All-Russian scientific-practical conference of young scientists, Tver, December 9, 2022. – Tver, 2023. – P. 181-187.

7. Dykhova, A., Semina, K. Digital Economy and Problems of Economic Security // Research Strategies in Social Sciences and Humanities : collection of scientific articles based on materials of International scientific-practical conference, Belgorod, January 31, 2022. – Belgorod, 2022. – P. 71-76.

8. Evstigneeva, A. Legal Regulation of the Detection and Suppression of Cybercrime in Russian Federation // State and Municipal Administration in Russia: Status, Problems and Prospects : proceedings of 19th All-Russian scientific-practical conference, Perm, March 20-21, 2025. – Perm, 2025. – P. 86-90.

Об авторах

Миронова Ольга Александровна, кандидат экономических наук, доцент, доцент кафедры экономики региона, отраслей и предприятий, Ростовский государственный экономический университет (РИНХ), Ростов-на-Дону, Россия, lady.sensey2010@yandex.ru.

Хвоевская Лариса Ивановна, кандидат социологических наук, доцент кафедры государственного и муниципального управления, Донской государственный технический университет, Ростов-на-Дону, Россия, larson_larisa@mail.ru.

Конфликт интересов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Статья поступила в редакцию 06.11.2025; одобрена после рецензирования 01.12.2025; принята к публикации 30.01.2026.



Статья опубликована на условиях лицензии Creative Commons Attribution 4.0 International (CC-BY 4.0)

© 2026 Миронова О. А., Хвоевская Л. И.

About the Authors

Olga Mironova, Cand. Sci. (Econ.), Associate Professor, Associate Professor of the Department of Regional Economics, Industries and Enterprises, Rostov State University of Economics, Rostov-on-Don, Russia, lady.sensey2010@yandex.ru.

Larisa Khvoevskaya, Cand. Sci. (Socio.), Associate Professor of the Department of Public and Municipal Administration, Don State Technical University, Rostov-on-Don, Russia, larson_larisa@mail.ru.

Conflict of Interest: The authors contributed equally to this article. The authors declare no conflict of interest.

The article was submitted on 06.11.2025; approved after reviewing on 01.12.2025; accepted for publication on 30.01.2026.



This is an open access article distributed under the terms of Creative Commons Attribution 4.0 International License (CC-BY 4.0)

© 2026 O. Mironova, L. Khvoevskaya