Журнал правовых и экономических исследований.
Journal of Legal and Economic Studies, 2019, 4: 21–27

DOI 10.26163/GIEF.2019.40.42.003
УДК 346.54

A.N. Litvinenko, Y.A. Lozina

DIGITAL ECONOMY: CHALLENGE OR THREAT TO ECONOMIC SECURITY? NORMATIVE APPROACH

Aleksandr Litvinenko – Professor, the Department of Economic Security and Social Economic Processes Management, Saint-Petersburg University of MIA of Russia, Full Professor, Doctor of Economics, St. Petersburg; **e-mail: lanfk@mail.ru**.
Yuliya Lozina – Senior Lecturer, the Department of Civil Law and Civil Procedure, Saint-Petersburg University of MIA of Russia, PhD in Law, Associate Professor, St. Petersburg; **e-mail: 1612ulia.l@mail.ru**.

The relevance of reviewing digital economy in the context of ongoing challenges and threats to economic security is based on the increased comprehensive digitalization in all spheres of public life. It also stems from the importance of introducing advanced information technologies to ensure economic growth of the country that results in immediate synchronous emergence of new challenges and threats to economic security as well as in generation of the ones already existing. At the same time there is a separate independent task dealing with performing normative analysis of the distinction between existing challenges and threats wherein digital economy has leading positions and also is deemed to be itself a challenge and threat to economic security.

Keywords: *digital economy; economic security strategy; challenges and threats to economic security; digitalization; cyberattack; cybersecurity; cybercrime; biosecurity; nanotechnology; block-chain technology; innovative development; cryptocurrency.*

А.Н. Литвиненко, Ю.А. Лозина

ЦИФРОВАЯ ЭКОНОМИКА: ВЫЗОВ ИЛИ УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ? НОРМАТИВНЫЙ ПОДХОД

Александр Николаевич Литвиненко – профессор кафедры экономической безопасности и управления социально-экономическими процессами, Санкт-Петербургский университет МВД России, доктор экономических наук, профессор, г. Санкт-Петербург; **e-mail: lanfk@mail.ru**.
Юлия Александровна Лозина – доцент кафедры гражданского права и гражданского процесса, Санкт-Петербургский университет МВД России, кандидат юридических наук, доцент, г. Санкт-Петербург; **e-mail: 1612ulia.l@mail.ru**.

Актуальность рассмотрения цифровой экономики в системе вызовов и угроз экономической безопасности определяется усилением цифровизации во всех сферах общественной жизни, важностью внедрения передовых информационных технологий для экономического роста страны, что влечет одновременное появление новых и генерирование имеющихся вызовов и угроз экономической безопасности. При этом самостоятельной задачей является проведение нормативного анализа разграничения имеющихся вызовов и угроз, в которых сегодня цифровая экономика занимает лидирующие позиции, и позиционирование ее самой как вызова или как угрозы экономической безопасности страны.

Ключевые слова: *цифровая экономика; Стратегия экономической безопасности; вызовы и угрозы экономической безопасности; цифровизация; кибератака; кибербезопасность; киберпреступность; биобезопасность; нанотехнологии; блокчейн-технологии; инновационное развитие; криптовалюта.*

На данный момент нет четкого понимания, что же представляет собой цифровая экономика, поскольку постепенно она становится неотделимой и незаменимой частью функционирования всей экономики в целом. На конференции ООН было озвучено, что различные технологии и экономические аспекты цифровой экономики в настоящее время могут быть разделены на три широких компонента: это цифровая экономика, в состав которой входят фундаментальные инновации (полупроводники, процессоры), основные технологии (компьютеры, телекоммуникационные устройства) и вспомогательные инфраструктуры (Интернет и телекоммуникационные сети) [15].

Выступая на конференции, генеральный секретарь ООН Антонио Гутьеррес отметил важность дальнейшего исследования цифровой экономики для всего мирового сообщества, поскольку достижения цифровизации предоставили возможность получить небольшому количеству частных лиц, компаний и стран огромное богатство, что увеличило разрыв между странами-лидерами в области технологий и развивающимися, которые имеют ограниченный доступ к Интернету или не имеют его вовсе [15, с. 5].

Вызовом для безопасности стран считает быстрое развитие цифровизации в своем докладе Мухиса Китуйи, генеральный секретарь Конференция Организации Объединенных Наций по торговле и развитию [15, с. 6].

Приоритетным проектом национальной безопасности назвал Президент РФ цифровую экономику на совещании Совета по стратегическому развитию и приоритетным проектам еще в июле 2017 г. [13].

Итак, важность исследования цифровой экономики не вызывает сомнений, поскольку одновременно она является и приоритетным направлением экономического развития, и вызовом, и угрозой экономической безопасности государства.

Можно сказать, что цифровая экономика – это определенная среда, где значительно расширен круг привычных субъектов экономических отношений, отсутствуют территориальные ограничения, сделки осуществляются в пределах бизнес-платформ с использованием новых технологий. При этом государства уже не могут влиять на экономическую деятельность субъектов в привычном для их понимания виде. Налаживать новые модели взаимодействия приходится на условиях, предлагаемых лидерами в сфере цифровизации.

Осознавая отсутствие возможностей регулировать всестороннее техническое развитие в настоящее время, государства и мировые корпорации сосредоточились на факторах, которые уже причиняют ущерб их экономикам, и выразили готовность обмениваться данными о кибератаках [14, с. 24], что, несомненно, актуально, поскольку на обнаружение факта кибератаки сегодня требуется примерно три месяца [14, с. 26].

Анализируя имеющееся законодательство, так или иначе касающееся цифровизации, начнем с главного документа, рассчитанного до 2030 года – Стратегии экономической безопасности (далее – Стратегия) [2]. Она в своих нормах для определения глубины проблемы влияния цифровизации на экономическую безопасность России использует понятия «вызовы» и «угрозы», как факторы, дальнейшее развитие которых может привести к неблагоприятным последствиям. При этом вызов – это совокупность факторов, приводящих в определенных условиях к угрозе экономической безопасности. Угроза – совокупность условий и факторов, создающих возможность причинения ущерба экономическим интересам России.

Понятие угрозы определяется в Стратегии национальной безопасности РФ как прямая или косвенная возможность нанесения ущерба конституционным правам, свободам, достойному качеству и уровню жизни граждан, суверенитету и территориальной целостности, устойчивому развитию Российской Федерации, обороне и безопасности государства [3]. Понятно, что в настоящее время развитие цифровой экономики влияет на все перечисленные

объекты.

Рассматривая принятые в последние годы нормативные акты, так или иначе связанные с цифровой экономикой, можно попытаться выделить, что же сегодня является угрозой, а что – вызовом для экономической безопасности страны с учетом анализа содержания этих факторов и условий в имеющихся источниках.

В Стратегии экономической безопасности выделим основные вызовы и угрозы развития цифровизации с точки зрения экономики:

а) недостаточная активность в сфере инноваций;

б) низкий рейтинг России в области разработки новых перспективных технологий и их внедрения (в том числе технологий цифровой экономики);

в) отсутствие образовательных организаций, готовящих специалистов высокой квалификации, и научных разработок в данной области.

Рассмотрим подробнее каждое из указанных выше положений:

А) Недостаточную активность в сфере инноваций в Прогнозе научно-технологического развития РФ на период до 2030 г.[4] предлагается усилить в приоритетных сферах: информационно-коммуникационные технологии, био- и нанотехнологии, природопользование, космос, энергосбережение и т.д. В данном нормативном акте инновационное отставание понимается как вызов. В контексте Прогноза – это крупная проблема, затрагивающая наиболее важные сферы и требующая принятия комплексных мер, направленных на ее решение как минимум на уровне государства.

Стратегия инновационного развития РФ до 2020 г. должна показать уже определенные результаты, определить правильность основных направлений деятельности, которые были актуальны в момент ее принятия. Уровень расходов в экономике на научные исследования, сферу образования и поддержку инноваций должен к 2020 г. достичь уровня стран Организации экономического сотрудничества и развития.

Итак, в данном документе четко выделены внешние вызовы, стоящие перед страной в инновационном развитии:

- ускорение технологического развития мировой экономики; в частности, это энергетика и новые технологии добычи полезных ископаемых;

- уменьшение высококвалифицированных специалистов, работающих в сфере технологий и инноваций;

- климатические изменения, проблемы в здравоохранении, старение населения.

Как видим, два первых вызова зеркально отражают указанные в Стратегии экономической безопасности в качестве вызова и угрозы, только с внутренней стороны, как проблема России: отставание в разработке новых технологий и отсутствие квалифицированных специалистов.

В Энергетической стратегии России на период до 2030 г. выделяются внешние и внутренние вызовы безопасности государства. При этом главным внутренним вызовом определена необходимость выполнения энергетическим сектором основной задачи – перехода на инновационный путь развития.

Что касается внешнего вызова, то все неоднозначно. Он должен преодолеть угрозы, связанные с неустойчивостью мировых энергетических рынков, цен на энергоресурсы, т.е. необходимо достичь устойчивых результатов в мировом масштабе [8].

Как видим, перечисленные вызовы имеют общие формулировки, в силу недостаточной изученности каждого фактора и условия в настоящее время не представляется возможным просчитать имеющиеся риски и потери.

Транспортная стратегия Российской Федерации на период до 2030 г. определяет системный вызов, который состоит из трех факторов: усиление конкуренции в мировых масштабах; усиление роли человеческого капитала и качества профессиональных кадров в инновационной сфере; исчерпание сырьевых источников транспортного обслуживания [7]. Приведенные факторы сформулированы в качестве проблемы, которую необходимо решать в перспективе, и при этом также де-

тально рассматривать все входящие в нее составляющие. Ущерб при таком широком диапазоне достаточно трудно подсчитать. Меж тем системные вызовы Транспортной стратегии идентичны Стратегии инновационной.

В Прогнозе долгосрочного социально-экономического развития РФ на период до 2020 г. ключевыми внешними вызовами для России в части инновационного развития являются:

- ускорение технологического развития мировой экономики;

- глобальное усиление конкурентной борьбы за высококвалифицированных рабочих и инвестиции, и как следствие – отток из страны конкурентоспособных кадров, технологий, идей и капитала;

- изменение климата, старение населения, проблемы систем здравоохранения.

Отметим, что данные вызовы не переведены в угрозы и в прогнозе долгосрочного развития на период до 2030 года [10].

Б) Преодоление низкого рейтинга России в области разработки новых перспективных технологий и их внедрения (в том числе технологий цифровой экономики) реализуется в ряде нормативных актов, в том числе в Федеральной научно-технической программе развития генетических технологий на 2019–2027 гг. [5], в которой задачей является формирование условий для развития научно-технической деятельности, генетических технологий, кадрового потенциала российской науки и снижение ее зависимости от иностранных баз данных. Отмечается низкая конкурентоспособность России в этой сфере и значительное отставание от лидеров по числу полученных патентов. В первом разделе программы, касающейся биобезопасности и технологической независимости указывается, что обостряется угроза распространения инфекционных заболеваний с пандемическим потенциалом, причиняющих социальный и экономический ущерб. Программа предлагает четыре направления развития: биобезопасность и технологическая независимость, развитие генетики в сельском хозяйстве, медицине и в промышленной микробиологии. В программе нет четко сформулированных вызовов и угроз, однако технологическая независимость является одним из факторов, который уже сегодня приводит к экономическому ущербу государства.

Отметим, что среди ожидаемых результатов Программы – развитие кадрового потенциала российской науки в данных областях.

В) Специалистам в области цифровой экономики посвящен федеральный проект «Кадры для цифровой экономики» [9], ответственным исполнителем которого является Минэкономразвития России. В обосновании проекта указаны три основных направления: обеспечение квалифицированными кадрами, поддержка талантливых школьников и студентов, содействие гражданам в освоении цифровой экономики. В проекте указываются сложившиеся вызовы в системе образования. Среди них – отставание в технологиях подготовки специалистов, низкая заработная плата, отсутствие интереса у старшеклассников к техническим профессиям, российские образовательные программы среднего и высшего образования не содержат в себе «цифровой компонент» и т.д.

Таким образом, среди трех приоритетных вызовов и угроз, непосредственно связанных Стратегией с цифровизацией, согласно проанализированным источникам только один является угрозой – низкий рейтинг в сфере разработки технологий. Два же других формулируются в качестве вызова экономической безопасности.

Понятно, что перечисленные нормативные источники в полном объеме не отражают всех процессов, которые происходят в реальной жизни. Между тем уже сегодня новые технологии, особенно искусственный интеллект, неизбежно ведут к серьезным сдвигам на рынке труда, в том числе исчезновению рабочих мест в одних секторах экономики и созданию возможностей в других – в массовом масштабе. Ускоренное развитие цифровой экономики в ближайшее время потребует применения ранее не использованных навыков в трудовой сфере, другого уровня отношений, возникающих в связи с вне-

дрением новых технологий. Соответственно, изменится суть таких понятий, как работа, отдых и их соотношение, поскольку добавится иной характер труда и отдыха.

Ведущие страны мира, в данном случае понимая цифровую экономику как фактор, являющийся вызовом для их безопасности, и осознавая важность решения уже поставленной задачи, начали совместно с крупными компаниями осуществлять переподготовку и повышение квалификации своих работников, делая инвестиционные вложения в образование. При этом денежные средства вкладываются не только в обучение, но и в обучение тому, как учиться, и обеспечение пожизненного доступа к возможностям обучения для всех [16].

Примерно 3 млн специалистов по кибербезопасности требуется сегодня мировому сообществу [14, с. 18]. Можно сделать вывод об усилении международной конкуренции за кадры высшей квалификации. Данный фактор, указанный в Стратегии экономической безопасности, будет усиливаться с каждым годом.

Цифровая экономика своим развитием не только представляет вызов, но и наносит определенный ущерб интересам российского бизнеса. По оценке ведущих топ-менеджеров, такой ее компонент, как кибербезопасность занимает третье место среди угроз финансовому состоянию, инновационному развитию России. Опережают данный фактор только риски влияния государства на бизнес и пророссийские санкции. При этом среди главных возможностей для экономического развития на первое место как раз ставится цифровизация, искусственный интеллект и переход на «умные системы [12].

Указанные в Стратегии экономической безопасности другие вызовы и угрозы прямо или косвенно касаются информационных технологий.

Анализируя такие факторы и условия, как использование развитыми государствами преимуществ в уровне развития информационных и других высоких технологий, ограничение к ним доступа, приведем данные из Официального доклада с Конференции ООН, посвященной цифровой экономике. Платформенно-ориентированные предприятия, такие как «Amazon», «Alibaba», «Facebook» и «eBay» имеют большое преимущество в экономике, поскольку собирают и управляют данными, связанными с действиями пользователей в сети «Интернет». Реализация их возможностей от цифровых разработок напрямую зависит от того, сколько доходов они смогут получить. Сегодня на США и Китай приходится 75% всех патентов, связанных с блокчейн-технологиями, 70 крупнейших цифровых платформ и 90% цифрового рынка. Доля Европы составляет 4%, а Африки и Латинской Америки – 1%. Крупнейшие цифровые платформы при этом показывают стремление к глобальному доминированию в пограничных технологических областях [15, с. 15–17].

Слабость в защите информационной структуры финансово-банковской системы сегодня можно подтвердить фактическими данными. В 2019 г. более 80% атак на клиентов банков совершалось с помощью социальной инженерии [14, с. 26]. При этом 4 млрд кибератак зафиксировано в России за последний год, прогнозируемый ущерб для финансового сектора экономики – 2 трлн рублей [14, с. 22].

Вызывают определенные трудности уже сегодня такие факторы, как недостаточный уровень квалификации и ключевых компетенций отечественных специалистов и снижение качества человеческого потенциала. По оценке зарубежных специалистов, работники с ограниченными цифровыми навыками в скором времени могут оказаться в невыгодном положении. Фирмы, которые не смогут выйти в сеть «Интернет», столкнутся с жестокой конкуренцией. Конкурентные риски будут зависеть от уровня развития и цифровой готовности страны и политики, реализуемой на международном и внутригосударственном уровне в этой сфере.

Четче с точки зрения разделения вызовы и угрозы определены в Программе цифровой экономики. Угрозы: невозможность отслеживания технически сложных данных и информации. Ущерб от этого –

незаконный вывоз капитала, уход от налогообложения, отмывание доходов с использованием криптовалют. Еще одна угроза – внешнее воздействие на информационные структуры, базы данных. Ущерб от киберпреступности уже сегодня заставляет ведущих стран-лидеров думать о превентивных мерах и возможностях прогнозировать угрозы.

Вызовы: отставание России в развитии информационных технологий, зависимость от экспортной политики иностранных государств, отток кадров за рубеж и недостаточный уровень квалификации специалистов в области информационной безопасности, капиталовложения в инновации по сравнению с другими государствами, отсутствие продуманного механизма внедрения отечественных разработок на российский и зарубежный рынок.

Таким образом, приведенные в названных документах вызовы и угрозы влияют на устойчивое развитие российской экономики, ее конкурентоспособность на мировом рынке и экономический суверенитет. Анализ нормативных актов выявил три основных условия и фактора, влияющих на экономическую безопасность в большей степени, что подтверждается их включением в изученные источники: низкий уровень инновационного развития, кадровый голод и отставание в области разработки и внедрения отечественных технологий.

Рассматриваемые в статье факторы цифровой экономики по отношению к экономической безопасности делятся в разных источниках на вызовы и угрозы в зависимости от того, возможно ли в настоящее время оценить и спрогнозировать ущерб. Однако статистические данные показывают, что ущерб уже подсчитывается и в отношении тех условий и факторов, которые в нормативных источниках считаются вызовом, что говорит о значительном отставании нормативного регулирования имеющихся процессов и явлений с учетом ускоренного развития цифровой экономики. Данный вывод подтверждается и тем, что вызовы в большинстве источников имеют достаточно общее определение, включающее в себя широкий диапазон не в полной мере исследованных условий и факторов, которые могут повлиять на возникновение угрозы. Последствием этого является оценка имеющегося ущерба, а не его прогнозирование.

ЛИТЕРАТУРА

1. Указ Президента РФ от 09.05.2017 г. № 203 «О стратегии развития информационного общества в РФ на 2017–2030 годы» // Президент России: [сайт]. URL: http://www.kremlin.ru/acts/bank/41919 (дата обращения: 20.08.2019).

2. Указ Президента РФ от 13.05.2017 г. № 208 «О стратегии экономической безопасности на период до 2030 года» // СЗ РФ. 2017. 15 мая. № 20. Ст. 2902.

3. Указ Президента РФ «О Стратегии национальной безопасности РФ до 2020 года» // Российская газета. 2009. 19 мая. № 4912 (88).

4. Постановление Правительства РФ от 03.01.2014 г. «Об утверждении Прогноза научно-технологического развития РФ на период до 2030 года» // Правительство России: [сайт]. URL: http://static.government.ru/media/files/41d4b737638b91da2184.pdf (дата обращения: 19.09.2019).

5. Постановление Правительства РФ от 22.04.2019 г. № 479 «Об утверждении Федеральной научно-технической программы развития генетических технологий на 2019–2027 годы» // Правительство России: [сайт]. URL: http://static.government.ru/media/files/1FErVexYSoVYFduUn1tStWlLkyrkTEmu.pdf (дата обращения: 19.09.2019).

6. Программа «Цифровая экономика». Утв. постановлением Правительства РФ 27.07.2017 г. № 1632-р // Правительство России: [сайт]. URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения: 23.08.2019).

7. Транспортная стратегия Российской Федерации на период до 2030 года. Утв. распоряжением Правительства РФ от 22.11.2008 г. № 1734-р // Правительство России: [сайт]. URL:

http://static.government.ru/media/files/Z31ADuvq0eoXlknPdhwWRYl22ISdhpaS.pdf (дата обращения: 01.10.2019).

8. Энергетическая стратегия России на период до 2030 года. Утв. распоряжением Правительства РФ от 13.11.2009 г. № 1715-р // Министерство энергетики Российской Федерации: [сайт]. URL: https://minenergo.gov.ru/node/1026 (дата обращения: 01.10.2019).

9. Паспорт федерального проекта «Кадры для цифровой экономики» // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: [сайт]. URL: https://digital.gov.ru/uploaded/files/pasport-federalnogo-proekta-kadryi-dlya-tsifrovoj-ekonomiki.pdf (дата обращения: 19.09.2019).

10. Прогноз долгосрочного социально-экономического развития Российской Федерации на период до 2030 года // Правительство России: [сайт]. URL: http://static.government.ru/media/files/41d457592e04b76338b7.pdf (дата обращения: 01.10.2019).

11. Цифровая повестка Евразийского экономического союза до 2025 года. Перспективы и рекомендации: обзор. 2018.03.29 // Документы и доклады: [сайт]. URL: http://documents.vsemirnyjbank.org/curated/ru/413921522436739705/pdf/EAEU-Overview-Full-RUS-Final.pdf (дата обращения: 13.03.2019).

12. *Баталова А.* Риск в сети. Исследование Ассоциации менеджеров России (АМП) // Российская газета. 2019. 7 октября. № 225. URL: https://rg.ru/2019/10/07/menedzhery-nazvali-glavnye-ugrozy-dlia-kompanij.html (дата обращения: 07.10.2019).

13. Заседание Совета по стратегическому развитию и приоритетным проектам от 05.07.2017 г. // Президент России: [сайт]. URL: http://www.kremlin.ru/events/president/news/5498 (дата обращения: 15.06.2019).

14. Международный конгресс по кибербезопасности ICC-2019. Итоги // International Cybersecurity Congress: [сайт]. URL: https://icc.moscow/upload/doc/ICC_reports_RU.pdf (дата обращения: 01.10.2019).

15. Digital Economy Report – 2019 – Официальный доклад «Цифровая экономика–2019: Создание и захват стоимости: последствия для развивающихся стран». Конференция ООН по торговле и развитию // UNCTAD: [сайт]. URL: https://unctad.org/en/PublicationsLibrary/der2019_en.pdf (дата обращения: 01.10.2019).

16. WTAS: Business Leaders Pledge to Create More Opportunities for Workers Across the Country // WAS: лидеры бизнеса обещают создать больше возможностей для работников по всей стране // The White House: [сайт]. URL: https://www.whitehouse.gov/briefings-statements/wtas-business-leaders-pledge-create-opportunities-workers-across-country (дата обращения: 01.10.2019).