**УДК 327.8**

***Харичкин И.К., доктор философских наук, профессор***
***профессор кафедры политологии***
***Московский государственный лингвистический университет***
***Россия, Москва***

# ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ СТАНОВЛЕНИЯ ЦИФРОВОЙ ЭКОНОМИКИ В РОССИИ

***Аннотация.*** *Статья посвящена развитию новых информационных технологий, в частности «цифровой экономике». Выявляются риски для гражданина, общества, государства от «цифровизации» общественной жизни. Рассмотрены угрозы национальной безопасности от цифровизации экономики, выработаны предложения по их минимизации.*

***Ключевые слова:*** *информационные технологии, «цифровая экономика», национальная безопасность, нормотворчество.*

***Annotation.*** *The article is devoted to the development of new information technologies, in particular to the "digital economy". The risks for a citizen, society, and the state from "digitalization" of public life are revealed. Threats to national security from the digitalization of the economy are considered, and proposals for their minimization are worked out.*

***Key words:*** *information technology, "Digital economy", national security, rulemaking.*

Становление и развитие цифровой экономики в Российской Федерации, связанные с этим процессы информатизации всех сфер жизнедеятельности российского общества, активное участие в этом процессе федеральных органов государственной власти Российской Федерации, разработка и реализация различных государственных программ, предусматривающих

выделение значительных объемов бюджетных средств на указанные процессы, включая программу «Цифровая экономика Российской Федерации», влекут за собой возникновение новых угроз безопасности Российской Федерации, требующих углубленного изучения. Спектр возникающих угроз достаточно широк и охватывает компетенцию всех государственных органов, в первую очередь тех, которые осуществляют контроль за безопасным развитием экономики. Вместе с тем в настоящее время в стране отсутствует единое понимание сущности цифровой экономики, а также единый подход к классификации и оценке угроз национальной безопасности в данной сфере

Распространение нового технологического уклада кардинальным образом меняет всю систему управления глобальными социально-экономическими процессами. С одной стороны, появляются новые возможности тотального контроля над поведением граждан в глобальном масштабе. В этом направлении активно работают американские спецслужбы. С другой стороны, становится возможным появление частных трансграничных систем управления экономическими, социальными и политическими процессами, затрагивающих национальные интересы государств и их объединений. Основу для таких систем обеспечивают глобальные социально-информационные и торгово-информационные сети и криптовалюты, интернет вещей и прочие обезличенные информационные средства совершения трансакций, выводящие международную торговлю и финансы за пределы национальных юрисдикций. Граждане могут отказаться от государственных систем защиты своих интересов, полагаясь на сетевые структуры и используя блокчейн-технологии и умные контракты.

Система государственно-правового регулирования явно отстает от вызовов новых технологических возможностей. Не только в вопросах обеспечения кибербезопасности, электронной торговли и регулирования Интернет, но и в использовании биоинженерных технологий, беспилотных транспортных средств, 3D принтеров и т.п.

К числу основных рисков и проблем, связанных с развитием цифровизации следует отнести такие как: угроза «цифровому суверенитету» страны; нарушение частной жизни; снижение уровня безопасности данных; уменьшение числа рабочих, особенно мест низкой и средней квалификации; повышение уровня сложности бизнес моделей и схем взаимодействия; резкое усиление конкуренции во всех сферах экономики.

Во всем конгломерате угроз следует определить и объективно оценить реальные и мнимые угрозы, а также потенциальные возможности перехода последних в реальные.

Непосредственно национальной безопасности цифровизация экономики угрожает по следующим направлениям:

1. Кибертерроризм и кибершпионаж, ведущиеся против России другими странами, иностранными террористическими и иными преступными организациями, а также отдельными лицами и группами лиц.

2. Те же угрозы со стороны внутренних преступных сообществ, террористических организаций, религиозных и прочих экстремистских группировок и антигосударственных сил.

3. Иные угрозы в информационной сфере, связанные с получением доступа к различным массивам информации, ее противоправным использованием.

4. Уход от налогообложения, незаконный вывоз капитала, легализация преступно полученных доходов и финансирование терроризма с использованием новых технологий электронных платежей.

5. Осуществление незаконной предпринимательской деятельности посредством использования сети Интернет, включая электронную торговлю и финансовые услуги.

6. В то же время информатизация систем управления остается наиболее коррупциогенной сферой, поглощающей растущую часть бюджетов органов управления без пропорциональной затратам отдачи.

При изучении угроз следует особое внимание уделить вопросу использования big data (больших данных) - огромных объемов данных о реальных людях и их действиях, которые создает «цифровая экономика», и технологий их обработки. Собственно, глава Минкомсвязи и называет «цифровую экономику» — «экономикой данных».

Рассматривая идущие процессы цифровизации экономики России и возможные угрозы, обусловленные этим процессом следует отметить, что исторически развитие цифровой экономики может идти двумя путями:

- эволюционный путь, в рамках которого Россия будет развивать и использовать цифровые технологии будучи участником международных экономических отношений для обеспечения сопоставимых по уровню развития цифровых технологий условий участия в них и обеспечения своей конкурентоспособности. Как справедливо отмечают современные исследователи, «дальнейшее проникновение цифровых технологий в жизнь – одна из характерных особенностей будущего мира. Это обусловлено прогрессом в областях микроэлектроники, информационных технологий и телекоммуникаций. Таким образом, цифровизация - процесс объективный, неизбежный и остановить его невозможно» [1, с. 5];

- второй путь плановый (или программный), в рамках которого государство принимает активное участие в становлении и развитии цифровой экономики в стране, разрабатывая и утверждая соответствующий план (программу). Цели и содержание плановых мероприятий зачастую имеет выраженную политическую окраску, ввиду чего реализация подобных программ во многом зависит от превалирующего интереса политических элит.

В России с 2017 года избран второй - программный путь развития, реализующийся в рамках программы «Цифровая экономика Российской Федерации».

В свою очередь Указом Президента РФ от 7 мая 2018 года «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» перед Правительством РФ поставлены цели и задачи, решение которых должно быть обеспечено до 2024 года при реализации национальной программы «Цифровая экономика РФ». В их числе:

- увеличение внутренних затрат на развитие цифровой экономики за счет всех источников (не менее чем в три раза по сравнению с 2017 годом);

- создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств;

- создание системы правового регулирования цифровой экономики, основанного на гибком подходе в каждой сфере;

- обеспечение информационной безопасности на основе отечественных разработок при передаче, обработке и хранении данных, гарантирующей защиту интересов личности, общества, государства;

- обеспечение подготовки высококвалифицированных кадров для цифровой экономики;

- преобразование приоритетных отраслей экономики и социальной сферы посредством внедрения цифровых технологий и др.

Отнесение вопросов развития цифровой экономики в стране к числу национальных целей и стратегических задач еще раз говорит о переходе от эволюционного развития цифровой экономики к форсированному программно-плановому, который будет осуществляться при активнейшем участии и поддержке государства.

Исследователи проблем цифровой экономики справедливо отмечают, что современные тенденции развития мировой экономики во многом обусловлены и будут определяться в дальнейшем развитием глобальной электронной сети, информационно-интеллектуальными и цифровыми

технологиями, более полной реализацией потенциала человеческого капитала и искусственного интеллекта [2, с.115]. При этом следует согласиться с утверждением о том, что формирование информационного общества без должного внимания к данному процессу может создать ряд угроз [3, с. 286]. Одновременно следует учитывать, что ускоренная цифровизация экономики может кратно актуализировать перечисленные угрозы и породить пока не осознанные до конца новые вызовы национальной безопасности.

Как отмечалось, информационные технологии стали неотъемлемой частью всех сфер деятельности личности, общества и государства, именно этот факт констатируется в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 года № 646. Следует понимать, что сфера криминальной деятельности не является исключением, она также охвачена процессом информатизации. Транснациональная организованная преступность, функционирующая в рамках основных наиболее доходных криминальных рынков, представляет собой прежде всего широкомасштабный теневой бизнес, основу существования и развития которого формирует главный движущий экономический фактор - спрос на предметы нелегального оборота и криминальные услуги.

Преступные организации все в большей мере заимствуют и с успехом адаптируют к своей деятельности современные формы и методы маркетинга, технологии менеджмента организации, прочие правомерные способы предпринимательской деятельности, в том числе активно используют новые информационные технологии. Такие изменения повышают стабильность, прибыльность и безопасность преступного бизнеса, позволяют взаимодействовать и объединяться с законопослушными экономическими субъектами, в том числе при полной не посвященности последних в вопросы преступной деятельности контрагента.

В этой связи решение обозначенных в указе Президента РФ целей и задач цифровизации должно происходить при непосредственном участии правоохранительных органов и органов безопасности страны в части их деятельности по обеспечению безопасности государства, общества, личности от преступных посягательств и новых угроз. При этом необходимы достаточных уровень понимания происходящих процессов всеми заинтересованными органами, четкое определение их функций, формирование адекватной реально складывающимся общественным отношениям, полной и доступной для понимания, простой в применении нормативной базы. Необходимо учитывать потребность не только в создании условий, способствующих наибыстрейшей цифровизации приоритетных отраслей экономики и социальной сферы, но и условий для высокой степени защищенности от угроз, обусловленных рассматриваемым процессом, в том числе для высокой готовности правоохранительных органов к решению новых задач.

Особого внимания заслуживает процесс нормотворчества. Современный этап нормативного регулирования цифровой экономики является переходным и в силу этого обладает высокой степенью неопределенности. В настоящий момент сложно оценить возможные последствия запланированных изменений законодательства и воздействие их на экономику, а также спектр возможных угроз, в том числе порождаемых самими правовыми нововведениями. Сложность анализа и оценки нормативных актов на это счет затруднена тем, что в настоящее время отсутствует полное представление обо всех возможных угрозах в данной области, включая представление об источниках угроз, объектах защиты, формах и способах реализации угроз.

В целом же возможность столь быстрой разработки правовой базы цифровой экономики вызывает сомнения, поскольку это требует глубокой и планомерной работы по развитию правовых институтов, установлению взаимосвязи новых, вводимых и уже имеющихся правовых понятий в рамках

отечественной правовой системы с опорой на международный опыт в данной области и существующее международно-правовое регулирование.

Как отмечается специалистами в области цифрой экономики верно отмечается, что важным с научной и практической точки зрения является исследование и разработка прогнозных и программных документов, ориентированных на определение и реакцию на новые глобальные вызовы (Grand challenges) [4, с. 31]. Важнейшую роль в данном процессе должны играть междисциплинарные исследования, которые не были проведены в необходимом с точки зрения предметной области количестве. Должны предприниматься усилия по сопряжению понятийного аппарата экономической и юридической наук с целью выработки адекватного новым экономическим явлениям языка правовых актов.

В целом решение указанных задач носит междисциплинарный характер, т.к. сами угрозы безопасности реализуются посредством использования информационных технологий, а последствия их реализации расположены не столько в информационной, сколько в политической, экономической, социальной областях жизнедеятельности общества. В этой связи предполагается, что:

1. Выявление угроз, исходящих от цифровизации, определение возможных путей их реализации, оценка актуальности угроз для РФ и поиск механизмов их выявления и мониторинга на практике, а также возможных путей их нейтрализации требует специальных познаний в области информационных технологий, полноты понимания происходящих информационно-технологических процессов и привлечения к исследованию специалистов в соответствующих областях.

2. Изучение факторов формирования угроз от цифровизации и последствий их реализации в экономической, политической, социальной сферах жизнедеятельности общества, их качественно-количественная оценка, поиск путей их минимизации должны осуществляться совместно с экономистами, политологами и юристами.

Данные обстоятельства требуют привлечения к выполнению научно-исследовательских работ смешанных авторских коллективов, состоящих из специалистов в указанных областях.

Предполагается, что материалы, подготовленные смешанными авторскими коллективами по изучению проблем, связанных с развитием цифровой экономики, будут использованы в качестве единой научно-прикладной базы для нормотворчества, а также деятельности правоохранительных органов по противодействию угрозам личности, обществу и государству от рассматриваемого процесса.

**Использованные источники:**

1. Введение в «Цифровую» экономику/ А.В. Кешелава В.Г. Буданов, В.Ю. Румянцев и др.; под общ. ред. А.В. Кешелава; гл. «цифр.» конс. И.А. Зимненко. – ВНИИГеосистем, 2017. – 28 с.

2. Развитие цифровой экономики в России как ключевой фактор экономического роста и повышения качества жизни населения: монография / Нижний Новгород:издательство «Профессиональная наука», 2018. -131с.

3. Рябинская С. С. Информатизация общества в России: особенности формирования и сопутствующие угрозы // Научно-методический электронный журнал «Концепт». – 2013. – Т. 4. – С. 276–280. – URL: http://e-koncept.ru/2013/64057.htm и др.

4. Цифровая трансформация экономики и промышленности: проблемы и перспективы / под ред. д-ра экон. наук, проф. А. В. Бабкина. – СПб. : Изд-во Политехн. ун-та, 2017. – 807 с.