ВЛИЯНИЕ ДИВЕРСИФИКАЦИИ ЦИФРОВОЙ ИНФРАСТРУКТУРЫ НА ЭКОНОМИЧЕСКОЕ РАЗВИТИЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

INFLUENCE OF DIVERSIFICATION OF DIGITAL INFRASTRUCTURE ON THE ECONOMIC DEVELOPMENT OF THE RUSSIAN FEDERATION

УДК 002.304

Трибунцев Никита Александрович, студент, 4 курс, факультет «Политологии», СПБГУ, Россия, г. Санкт-Петербург

Tribuntcev Nikita, e-mail: tribuntcev@yandex.ru

Аннотация

Статья посвящена проблеме диверсификации цифровой инфраструктуры. Кардинальные изменения в области информационных технологий и смещением приоритетов в сторону киберпространства привели к тому, что компьютерные технологии и сеть Интернет, активно используются для реализации общественных, экономических и политических целей. Развитие экономики Российской Федерации в настоящее время невозможно без развитой в достаточной степени информационной инфраструктуры. Однако существует и обратная сторона данного явления. Очевидно, что вовлечение информационных технологий во все сферы жизнедеятельности, делает общество, зависимым от новейших технологий. Экономическая безопасность Российской Федерации, в настоящее время, напрямую зависит от надежности функционирования ее информационно-телекоммуникационной составляющей.

Annotation

The article is devoted to the problem of diversification of digital infrastructure. Fundamental changes in the field of information technology and the shift of priorities towards cyberspace have led to the fact that computer technology

and the Internet are actively used to implement social, economic and political goals. Economic development of the Russian Federation is currently impossible without a sufficiently developed information infrastructure. However, there is a flip side to this phenomenon. Obviously, the involvement of information technology in all spheres of life makes the society dependent on the latest technology. The economic security of the Russian Federation, at present, directly depends on the reliability of its information and telecommunications component.

Ключевые слова: Киберпространство, диверсификация цифровой инфраструктуры, кибербезопасность, экономическое развитие, критическая инфраструктура, экономическая безопасность.

Keywords: Cyberspace, diversification of digital infrastructure, cybersecurity, economic development, critical infrastructure, economic security.

Настоящий период развития Российской Федерации, напрямую связан с процессами цифровизации, связанными, прежде всего с развитием и внедрением информационных технологий в различные сферы жизни российского общества. [9] Утвержденные российским правительством национальные проекты в таких сферах как: здравоохранение, образование, наука, цифровая экономика и ряда других, создают основу для разработки, создание и внедрение современных информационных технологий практически во все направления деятельности российского государства. [9]

Развитие экономики Российской Федерации в настоящее время невозможно без развитой в достаточной степени информационной инфраструктуры. Согласно доктрине информационной безопасности Российской Федерации, информационная инфраструктура - совокупность объектов информатизации, информационных систем, сайтов в сети "Интернет" и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации. [4] Наибольшее значение для современной

экономики представляют следующие составляющие цифровой инфраструктуры: центры обработки данных, сервисы облачных вычислений, цифровые платформы, услуги с использованием новых цифровых технологий— аналитики данных, искусственного интеллекта. Предоставление повсеместного широкополосного доступа, в особенности с использованием интеллектуальных мобильных устройств является основополагающей технологической тенденцией. [1] В российской экономике информационные технологии и информационные услуги стали значимой статьей не сырьевого экспорта, так в период с 2000 по 2010 год отрасль информационных технологий развивалась высокими темпами с ежегодным приростом около 25 процентов. [2] По данным государственной программы Российской Федерации «Информационное общество (2011 - 2020 годы)», утвержденной распоряжением Правительства Российской Федерации от 20 октября 2010 г. № 1815-р, на период начала программы, только 34 процента российских домашних хозяйств имели широкополосный доступ в сеть Интернет, доля органов государственной власти и местного самоуправления, имевших скорость передачи данных через информационно телекоммуникационную сеть "Интернет" не менее 2 Мбит/сек составляла 22 процента, то к 2019 году, число российских домашних хозяйств имеющих широкополосный доступ в сеть Интернет выросло до 75% , а доля органов государственной власти и местного самоуправления, имевших скорость передачи данных через информационно телекоммуникационную сеть "Интернет" не менее 2 Мбит/сек составила 85 %. [2] Учитывая всестороннее развитие цифровой инфраструктуры Российской Федерации, уместно говорить о происходящих в ней процессах диверсификации.

Подходы к определению термина «диверсификация» претерпевали изменения в результате исторического развития, но однозначного подхода не существует и по настоящее время, однако в контексте диверсификации цифровой инфраструктуры, целесообразно использовать определение, приведенное в работе Гуцева М.В., диверсификация – расширение видов

деятельности, проникновение в новые отрасли. [3] Шишкина Т. С. Пишет, что диверсификация является одним из важнейших инструментов развития, так как позволяет более результативно использовать возможности предприятия или организации. [13]

В результате, современная цифровая инфраструктура включает в себя: информационные центры, сети подвижной сотовой связи, подсистемы, банки данных и знаний, системы связи, центры управления, аппаратно-программные средства и технологии обеспечения сбора, хранения, обработки и передачи информации, центры обработки данных, сервисы облачных вычислений, цифровые платформы, услуги с использованием новых цифровых технологий— аналитики данных, искусственного интеллекта, технологии блокчейн. [1]

Цифровая инфраструктура рассматривается в различных сферах жизни российского общества. Цифровой сектор экономики, включает секторы ИКТ, производства контента и СМИ. В секторе государственного управления цифровая инфраструктура реализована прежде всего в направлениях государственного управления и регулирования, мобилизации и подготовки человеческого капитала, цифровых услуг, открытого правительства. В социальной сфере цифровая инфраструктура представлена: в медицине, в направлениях государственной политики в области здравоохранения, подготовки специалистов, национальные базы данных здравоохранения, цифровые медицинские технологии, система телемедицинских консультаций; в образовании в направлениях дистанционного образования, подготовки специалистов, цифровых образовательных ресурсов, образовательных платформ; в культуре, в форме цифровых платформ в сфере культуры, подготовки специалистов культурного сектора, электронных каталогов, виртуальных музеев.

Однако, следует учитывать различного рода риски и угрозы, возникающие при широкомасштабном развитии и распространении информационных технологий. К настоящему времени, вопросы безопасности

функционирования информационных технологий стоят в одном ряду с вопросами их эффективности. Говоря о безопасности цифровой инфраструктуры, необходимо рассмотреть составные части цифровой инфраструктуры и определить перечень угроз, скрытых за ними.

Составляющие части цифровая инфраструктуры могут быть разделены на следующие группы, согласно соответствующим им современным информационным технологиям:

1. Квантовые технологии;
2. Технологии искусственного интеллекта;
3. Облачные технологии;
4. Технологии больших данных;
5. Технологии киберфизических систем.

В настоящее время, современные квантовые технологии можно разделить по следующим направлениям: [5]

1. Квантовые компьютеры;
2. Квантовая сенсорика;
3. Квантовая связь;
4. Квантовые вычисления.

Квантовая передача данных или квантовая связь, в настоящее время является наиболее развитым направлением квантовых технологий, так как уже созданы и активно эксплуатируются квантовые каналы связи, защищающие передачу от большого числа «традиционных» атак. Вместе с тем большая часть квантовых протоколов распределения ключей на практике сталкивается с определенными техническими проблемами, что позволяет осуществлять некоторые специализированные атаки на квантовые каналы связи. [14]

Под квантовой сенсорикой понимается создание сенсоров, датчиков, измерительных приборов, основанных на квантовых эффектах. Планируется, что квантовые сенсоры, будут обладать высоким пространственным и временным разрешением, что позволит значительно увеличить точность и частоту измерений произвольных свойств заданных объектов. [5]

Квантовые вычисления и, необходимый для их реализации, квантовый компьютер находятся в стадии разработки прототипа. Квантовые вычисления достаточно глубоко проработаны теоретически, однако, реализовать данную вычислительную модель на традиционной архитектуре современных компьютеров невозможно. На текущий момент имеется информация только о прототипах с числом кубитов порядка 72. [8] Этого числа кубитов недостаточно, чтобы реализовать какой-либо полноценный квантовый алгоритм.

Полноценный квантовый компьютер позволит решать задачи самых различных направлений, начиная от дешифровки криптографических систем, заканчивая моделированием и симуляцией квантовых систем произвольного уровня сложности. С точки зрения киберугроз, квантовый компьютер в значительной степени затронет область криптографии, с одной стороны дискредитируя существующие системы защиты информации, а другой стороны парируя эти угрозы механизмами квантовой криптографии.

Термин «искусственный интеллект» используется для обозначения большого направления научных и прикладных исследований. Исследователи выделяют две основные цели своей работы – это создание компьютерных моделей, имитирующих процессы решения человеком тех или иных интеллектуальных задач, и автоматизация интеллектуального направления человеческой деятельности.

Сфера искусственного интеллекта довольно неоднородна. В ней существуют различные направления исследований, которые различаются или задачей, требующей интеллектуального анализа, или используемыми инструментами, или развитой моделью мышления. Сферы, определенные на основе решенной проблемы, включают: [10]

1) машинный перевод;
2) автоматическое реферирование и информационный поиск;
3) системы речевого общения;

4) игровой интеллект, доказательство теорем и автоматизация научных исследований;

5) компьютерное зрение;

6) извлечение данных.

Технологии искусственного интеллекта, сами по себе, не расширяют пространство киберугроз для информационной инфраструктуры, тем не менее, они в значительной степени влияют на эффективность различного рода кибератак, исходящих от связанных с ними технологий.

Под облачными технологиями, как правило, понимается предоставление пользователю компьютерных ресурсов и мощностей в виде интернет-сервисов. При это, пользователь может не иметь информации о том, какие вычислительные машины обрабатывают его запросы, какая при этом используется операционная система. Вычислительные облака состоят из тысяч серверов, размещенных в центрах обработки данных. Они единовременно обеспечивают миллионы пользователей необходимыми вычислительными мощностями. [9]

Учитывая, что облачные технологии, как правило, используются для хранения, передачи данных, а также или выполнения вычислительных задач, они значительно расширяют спектр киберугроз информационно й инфраструктуры, особенно в части конфиденциальности информации и доступности информационных ресурсов. [7]

Общепринятой терминологии в области обработки больших данных еще не сложилось. Однако, термину «большие данные» можно дать следующее определение - это массивы данных такого объема и структуры, которые превышают возможности традиционных программных инструментов по сбору, хранению и обработке данных за приемлемое время. При этом данные могут быть структурированными, слабоструктурированными и неструктурированными, что не позволяет эффективно управлять ими и обрабатывать традиционным образом. [6]

Проблема обеспечения безопасности больших данных заключается в противоречии между возрастающими потребностями в обработке таких данных с одной стороны, и недостаточными возможностями гарантировать конфиденциальность, целостность, доступность обрабатываемых данных и компонентов инфраструктуры с другой. Проблемы обеспечения кибербезопасности вызывают необходимость выработки принципиально иных подходов, базирующихся на концепции защиты распределенной, крупномасштабной вычислительной среды больших данных, а не единой физической сущности. [6]

Киберфизическая система – представляет собой сложную распределенную систему, управляемую или контролируемую компьютерными алгоритмами, тесно интегрированную с Интернетом и его пользователями, где физические и программные компоненты тесно взаимосвязаны. [12]

Также, следует отдельно рассмотреть объекты информационной инфраструктуры, представляющие особенную значимость в системе обеспечения национальной безопасности Российской Федерации, так называемую критическую информационную инфраструктуру. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" подчеркивает важность обеспечения безопасности критической информационной инфраструктуры Российской Федерации. Согласно закону, критическая информационная инфраструктура - объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов. [11] В свою очередь, объекты критической информационной инфраструктуры - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры. Критическая информационная инфраструктура Российской Федерации представлена в сферах здравоохранения, науки, транспорта, связи, энергетики, банковской сферы,

топливно-энергетического комплекса, атомной энергии, оборонного комплекса, ракетно-космической промышленности, горнодобывающей промышленности, металлургической промышленности, химической промышленности. В зависимости от соответствия критериям значимости объекту критической информационной инфраструктуры присваивается одна из трех категорий значимости. Категорирование осуществляется исходя из: [11]

1) социальной значимости, выражающейся в оценке возможного ущерба, причиняемого жизни или здоровью людей, возможности прекращения или нарушения функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также максимальном времени отсутствия доступа к государственной услуге для получателей такой услуги;

2) политической значимости, выражающейся в оценке возможного причинения ущерба интересам Российской Федерации в вопросах внутренней и внешней политики;

3) экономической значимости, выражающейся в оценке возможного причинения прямого и косвенного ущерба субъектам критической информационной инфраструктуры и (или) бюджетам Российской Федерации;

4) экологической значимости, выражающейся в оценке уровня воздействия на окружающую среду;

5) значимости объекта критической информационной инфраструктуры для обеспечения обороны страны, безопасности государства и правопорядка.

Подводя итог, можно сделать вывод, что происходящие в Российской Федерации процессы диверсификации цифровой инфраструктуры, приводят к проникновению последней в различные сферы жизни российского общества, в частности в экономику, в сферу государственного управления, в культурный сектор, а также в критические инфраструктуры Российской Федерации, что ввиду новизны таких технологий, несомненно расширяет перечень потенциальных угроз для национальной безопасности России в целом.

Приведенные выше анализ процесса диверсификации информационной инфраструктуры позволяет сделать вывод, что, хотя не все современные информационные технологии и процессы информационной трансформации, происходящие в современном российском государстве, неизбежно расширяют перечень угроз и вызовов национальной и экономической безопасности РФ, это положение остается верным для большинства из них.

Литература

1. Анализ текущего состояния развития цифровой экономики в России. М.: Институт развития информационного общества, 2018. — С. 50-56.
2. Государственная программа Российской Федерации «Информационное общество (2011 - 2020 годы)», утвержденная распоряжением Правительства Российской Федерации от 20 октября 2010 г. N 1815-р. ИСС Консультант +
3. Гуцев М.В. Диверсификация на высокотехнологичных предприятиях / М.В. Гуцев // Журнал Актуальные проблемы гуманитарных и естественных наук. – 2019. – №10/2011 – С.13.
4. Доктрина информационной безопасности Российской Федерации [Электронный ресурс] // ФГБУ «Редакция «Российской газеты», 1998-2020. – Режим доступа: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html. (дата обращения: 17.03.2020). – Загл. с экрана.
5. Душкин Р. В. Обзор текущего состояния квантовых технологий / Р.В. Душкин // Компьютерные исследования и моделирование 2018 Т. 10 № 2 С. 165-167
6. Запечников С.В. Проблемы обеспечения информационной безопасности больших данных / С. В. Запечников, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой // Безопасность информационных технологий. - 2014. - Т. 21. - №. 3. - С. 9.

7. Калашников А.О. новых технологий на информационную безопасность критической информационной инфраструктуры/ А.О. Калашников, Е.В. Аникина // Информация и безопасность – 2019. – № 2 – С. 56.
8. Лучший из лучших? Как создают мощнейший квантовый компьютер [Электронный ресурс] // Газета.ru от 23.09.2019 Режим доступа: https://www.gazeta.ru/science/2019/09/23_a_12670717.shtml (дата обращения: 06.02.2020).
9. Мурзин Ф.А. Облачные технологии: основные понятия, задачи и тенденции развития / Ф.А. Мурзин, Т.В. Батура, Д.Ф Семич // Программные продукты, системы и алгоритмы. - 2014. - № 1. - С. 64.
10. Потапов А.С. Технологии искусственного интеллекта / А.С. Потапов – СПб: СПбГУ ИТМО, 2010. С.3
11. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"
12. Цветков В.Я. Кибер физические системы / В. Я. Цветков // Международный журнал прикладных и фундаментальных исследований. – 2017. – № 6-1. – С. 64
13. Шишкина Т.С. Преимущества и недостатки внедрения стратегии диверсификации / Т.С. Шишкина // Актуальные проблемы экономики современной России. - 2015. - № 2. - С. 339-348.
14. Янковская Ю. Ю. Стойкость квантовых протоколов распределения ключей / Ю.Ю. Янковская, А. А. Марина // Computer sciences and telecommunications — 2013. — С. 2

Literature

1. Analysis of the current state of development of the digital economy in Russia. M.: Institute for the Development of the Information Society, 2018.- P. 50-56.
2. The state program of the Russian Federation “Information Society (2011 - 2020)”, approved by order of the Government of the Russian Federation of October 20, 2010 N 1815-r. ISS Consultant +

3. Gutsev M.V. Diversification in high-tech enterprises / M.V. Gutsev // Journal of Actual Problems of the Humanities and Natural Sciences. - 2019. - No. 10/2011 - C.13.
4. The doctrine of information security of the Russian Federation [Electronic resource] // Federal State Budgetary Institution "Edition of the" Russian newspaper ", 1998-2020. - Access mode: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html. (Date of treatment: 03/17/2020). - Zagl. from the screen.
5. Dushkin R.V. Review of the current state of quantum technologies / R.V. Dushkin // Computer Research and Modeling 2018 T. 10 No. 2 P. 165-167
6. Zapechnikov S.V. Problems of ensuring information security of big data / S.V. Zapechnikov, N.G. Miloslavskaya, M. Yu. Senatorov, A.I. Tolstoy // Security of information technologies. - 2014. - T. 21. - No. 3 .-- S. 9.
7. Kalashnikov A.O. new technologies for information security of critical information infrastructure / A.O. Kalashnikov, E.V. Anikina // Information and Security - 2019. - No. 2 - P. 56.
8. Best of the best? How to create a powerful quantum computer [Electronic resource] // Gazeta.ru on 09/23/2019 Access mode: https://www.gazeta.ru/science/2019/09/23_a_12670717.shtml (accessed: 02/06/2020).
9. Murzin F.A. Cloud technologies: basic concepts, tasks and development trends / F.A. Murzin, T.V. Batura, D.F.Semich // Software products, systems and algorithms. - 2014. - No. 1. - S. 64.
10. Potapov A.S. Artificial Intelligence Technologies / A.S. Potapov - St. Petersburg: St. Petersburg State University ITMO, 2010. P.3
11. Federal Law of July 26, 2017 N 187-ФЗ "On the Safety of Critical Information Infrastructure of the Russian Federation"
12. Tsvetkov V.Ya. Cyber physical systems / V. Ya. Tsvetkov // International Journal of Applied and Fundamental Research. - 2017. - No. 6-1. - S. 64

13. Shishkina T.S. Advantages and disadvantages of implementing a diversification strategy / TS. Shishkina // Actual problems of the economy of modern Russia. - 2015. - No. 2. - S. 339-348.
14. Yankovskaya Yu. Yu. Resistance of quantum key distribution protocols / Yu. Yu. Yankovskaya, A.A. Marina // Computer sciences and telecommunications - 2013. - C. 2