DOI 10.35775/PSI.2022.81.5.013
УДК 32.323
Д.А. ГОНЧАРОВА
аспирант факультета глобальных процессов
МГУ имени М.В. Ломоносова,
Россия, г. Москва

ЦИФРОВЫЕ ПАРАМЕТРЫ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Введение. *Независимо от политических и социальных систем, существование сектора и организаций национальной безопасности можно считать универсальным практически во всех государствах. Основной задачей организаций национальной безопасности в каждой стране является поддержка лиц, принимающих решения в стране, точной, актуальной информацией. Их основными задачами являются получение и анализ информации. В XX в. для осуществления этой деятельности в отрасли развивались специфические направления сбора информации (например, SIGINT – Signal Intelligence, HUMINT – Human Intelligence, OSINT – Open Source Intelligence и MASINT – Measurement and Signature Intelligence). В то же время, помимо своего специфического назначения и секретности, эти области претерпевают постоянные изменения, и одним из наиболее важных формирующих факторов является внешняя технологическая среда. Соответственно, мониторинг изменений внешней среды играет важную роль, и органы, принимающие решения в области национальной безопасности также реагируют на них, совершенствуя свои методы. Цифровые технологии, с одной стороны, позволяют ускорить и упростить процесс получения информации, с другой стороны, ведут к возникновению рисков.*

Методология исследования. *Методологическую основу исследования составляют общенаучные методы исследования, такие как синтез, анализ, сравнение, а также специальный метод исследования, такой как контент-анализ официальных документов.*

Результаты исследования. *В исследовании доказывается, что цифровизация несет в себе как выгоды, так и риски для национальной безопасности, поэтому каждой стране необходимо принимать ответные меры и поддерживать технологическое обеспечение национальной безопасности. Россия отстает от США по ключевым цифровым параметрам. Отставание России говорит о том, что требуется работа на уровне законодательства, а также на уровне разных подразделений для повышения конкурентоспособности экономики, развития ИКТ в разных регионах России, принятие соответствующих инициатив, которые бы способствовали*

более быстрому распространению широкополосного доступа в интернет, более активному внедрению электронных услуг на уровне разных секторов и органов власти.

Обсуждение. *Цифровизация как процесс создает значительные риски для сохранения текущего положения в системе национальной безопасности, ориентированной на физические угрозы. Основными угрозами новой социальной организации являются: цифровой терроризм; преступность в виртуальной среде; психоэмоциональная незащищенность человека, отсутствие личного пространства в цифровой среде; фальсификация информации; угроза национальному суверенитету в цифровом пространстве.*

Заключение. *В перспективе технологическое превосходство будет играть важную роль, обеспечивая непредсказуемые преимущества странам с самыми современными возможностями и решениями. Государственные органы власти осознают всю необходимость перехода на использование цифровых технологий, которые применяются для обеспечения национальной безопасности, но также и в смежных отраслях, в частности, для обеспечения информационной, технологической, финансовой и экономической безопасности.*

Ключевые слова: *цифровая экономика, цифровые технологии, вызовы, национальная безопасность, цифровизация, цифровая трансформация, индекс развития ИКТ, цифровой терроризм.*

Введение. Стремительное развитие и повсеместное внедрение цифровизации в последние годы ведет к нарастанию количества проблем, связанных с обеспечением национальной безопасности, и побуждает государства не только искать пути их нивелирования, но и осуществлять прогнозирование касательно возникающих угроз.

В идеальном мире государство является представителем граждан, которое способно защищать права и свободы, обеспечивать охрану жизни и здоровья и пр. Без доверия граждан нельзя говорить о выполнении государством своих функций. Такие случаи, как утечка информации, слежение за гражданами наносит вред и представляет собой угрозу потери доверия и национальной безопасности [7].

С увеличивающимся масштабом проникновения рассматриваемого процесса в структуру национальных экономик возрастает и зависимость государств от цифровой среды, что, в свою очередь, формирует целый ряд неопределенностей таких как кража данных и киберпреступления. Данные условия выводят на первое место деятельность, направленную на разработку стратегий цифровой безопасности, способствуют появлению специализированных органов и организаций, отвечающих за информационную безопасность.

Таким образом, многие страны ставят перед собой решение следующих задач:

– распознавание и недопущения произведения кибератак;

– ликвидация угроз с помощью разработки эффективных цифровых продуктов для использования в рамках государственных организаций и бизнес-сектора;

– усиленная защита объектов инфраструктуры;

– оказание стимулирования модернизации образовательного процесса в области цифровых технологий.

Основная цель – выявить угрозы и риски, нивелирование которых позволит обеспечить национальную безопасность в условиях перехода на цифровой путь развития. К задачам можно отнести: выявление рисков и угроз имплементации цифровизации и ее влияние на национальную безопасность.

Методология исследования. В работе использованы зарубежные и международные исследования в области построения модели цифровой экономики, а также официальная статистика. Исследование базируется на таких индексах, как Индекс сетевой готовности (Networked readiness index) [12], Индекс развития ИКТ (ICT Development Index) [11], Глобальный индекс инноваций (Global innovation Index) [8].

Автором используются общенаучные методы познания, такие как синтез, анализ, сравнение, а также специальные методы исследования, такие как контент-анализ официальных документов.

Результаты исследования. В Российской Федерации на информационную безопасность в бюджете заложено 19,85 млрд руб., однако МВД России свидетельствует о том, что ресурсов, в том числе и финансовых не хватает для борьбы с преступлениями в киберпространстве.

В 2020 г., по данным МВД РФ, количество преступлений, которые были совершены с использованием информационно-коммуникационных технологий, выросло почти на 74%. Среди факторов роста отмечают перевод процессов в онлайн-режим ввиду COVID-19. В 2021 г. зафиксирован рост на 1,4%, однако до сих пор ситуация с киберпреступностью остается напряженной [5]. Также планируется создать в Министерстве внутренних дел отдел по борьбе с киберпреступлениями [2].

В настоящее время наблюдается множество ответных мер в области национальной безопасности на уровне государств. Появились новые идеи и стратегии повышения кибербезопасности, сформировались организации, и в эпоху после Сноудена появились новые методы интерпретации разведывательных данных. Были опубликованы многочисленные исследования, в которых также подчеркивается роль технического развития и возможностей в области национальной безопасности, примером чего являются разработки в области национальной безопасности, CYBINT (кибербразведка), SOCMINT (разведка СМИ) или даже OSINT в Интернете [10].

Также появляются новые исследования, например, в области науки о данных, такие как исследования анонимизированных массовых данных, поскольку их результаты могут способствовать безопасности (например, кибербезопасности или даже правопорядку, повышая возможность регионального прогнозирования инцидентов безопасности). К ним относятся, например, приложения для отслеживания COVID, где новые мобильные приложения, использующие анонимизированные данные граждан, могут помочь в борьбе с распространением вируса. (В то же время, в связи с общественными и профессиональными дебатами, касающимися конфиденциальности, создаваемые приложения должны соответствовать законодательству о защите данных и конфиденциальности).

Возможности и организационные элементы, основанные на технических знаниях и обеспечивающие сбор открытой информации (например, OSINT), постепенно завоевывают позиции в структурах национальной безопасности каждой страны. Они стремятся собирать, анализировать и оценивать ценную для них информацию с помощью все более сложных решений.

Ввиду того, что события в киберпространстве могут напрямую влиять на безопасность стран, поэтому новые методы обязательно будут встроены в возможности организаций безопасности. Службы многих стран признают, что они могут получить чрезвычайно ценную информацию, используя киберпространство, поэтому важность Интернета как ресурса для организаций национальной безопасности возросла.

Обсуждение. Проблема цифровизации и ее связь с национальной безопасностью поднимается уже давно. Цифровизация как процесс создает значительные риски для сохранения текущего положения в системе национальной безопасности, ориентированной на физические угрозы. Большинство систем государственной безопасности основаны на предотвращении рисков, на попытке предсказать их, максимально локализовать последствия, если проблему не удастся устранить.

До масштабного внедрения технологий в экспертных кругах и на государственном уровне всегда в приоритете была концепция, что экономическая безопасность – один из важнейших элементов национальной безопасности страны, ключевым фактором обеспечения которой является государство, способное формировать для всех субъектов обязательства и требовать их выполнения [1. С. 132-134].

Основные угрозы стабильного положения национальной безопасности представлены на Рис. 1.

Некоторые исследователи полагают, что цифровые же технологии не оказывают прямого влияния на национальную безопасность, так как это влияние осуществляется через динамику и вектор социально-экономического прогресса. В таком случае можно выделить угрозы национальной безопасности для стран, которые отстают по темпам внедрения цифровых технологий. К таким угрозам относят [6. С. 254-256]:

Рисунок 1. Структура национальной безопасности и ее угрозы [1. С. 73-79]

– догоняющая роль в мировой экономике;
– снижение перспектив инновационного развития;
– низкий уровень конкурентоспособности;
– ограниченность инструментария для обеспечения национальной безопасности.

Например, в качестве примера можно указать, что цифровые технологии сыграли важную роль в период, когда государства столкнулись с ухудшением санитарно-эпидемиологической обстановкой (COVID-19), ведь получение информации и ее распространение через Интернет, а также меры защиты с использованием цифровых технологий.

Для цифрового общества характерны совершенно иные подходы к формированию угроз: цифровые риски неосязаемы, локализовать их последствия можно только в реальном времени при наступлении события, а также практически невозможно создать систему предотвращения таких рисков, только защиту, которая обеспечит достаточно времени для реагирования. Таким образом, система цифровых угроз и цифровая безопасность требуют разработки новых подходов, направленных на предотвращение хаотических

угроз и создание достаточно мощной защиты для их сдерживания до момента реагирования. Эти характерные особенности определяют не только основные отличия цифровых угроз от материальных, но и свидетельствуют о несовершенстве современной системы борьбы с цифровыми угрозами в мире в целом.

Основными угрозами новой социальной организации являются [4. С. 63-67]:

– цифровой терроризм;

– преступность в виртуальной среде;

– психоэмоциональная незащищенность человека, отсутствие личного пространства в цифровой среде;

– фальсификация информации;

– угроза национальному суверенитету в цифровом пространстве.

Эти пять основных угроз нельзя рассматривать без комплексного подхода, поскольку наиболее значимая из них, цифровой терроризм, часто может быть спровоцирована желанием нарушить суверенитет государства (например, в этом обвиняют Россию в контексте выборов президента США). В то же время существование угроз эмоциональному и психологическому здоровью человека в Интернете, хотя сегодня и не представляет столь значительного ущерба как для экономики, так и для политической независимости страны, представляет значительную проблему в будущем в связи с массовым использованием цифровых технологий [9. С. 1231-246].

Страны во всем мире стремятся преодолеть эти угрозы, однако, не стоит забывать и о технологических возможностях. Для примера можно сравнить Россию и США. В Таблице 1 представлены основные индексы цифровой готовности США и России.

Оценивая результаты индексного подхода к сравнению двух стран, можем сделать вывод о том, что Россия сильно отстает от США. США же по всем индекса занимает позиции в ТОП-5 (за исключением Индекса развития ИКТ), что связано с разным уровнем развития от штата к штату.

Показатели, на основании которых были рассчитаны индексы, играют важную роль и в обеспечении перехода к использованию цифровых технологий в области национальной безопасности, а также и непосредственно поддержании национальной безопасности в условиях меняющейся цифровой среды. Отставание России говорит о том, что требуется работа на уровне законодательства, а также на уровне разных подразделений для повышения конкурентоспособности экономики, развития ИКТ в разных регионах России, принятие соответствующих инициатив, которые бы способствовали более быстрому распространению широкополосного доступа в интернет, более активному внедрению электронных услуг на уровне разных секторов и органов власти.

Таблица 1

Индикаторы цифровой готовности США и России

Название индикатора	США	Россия
Индекс сетевой готовности (Networked readiness index) – 2021 г. [12]	4 место	43 место
Индекс развития ИКТ (ICT Development Index) – 2017 г. [11]	16 место	45 место
Глобальный индекс инноваций (Global Innovation Index) – 2021 г. [8]	3 место	45 место
Рейтинг электронного правительства (E-government rating), 2020 г. [13]	9 место	36 место

Заключение. Таким образом, приходим к выводу о том, что цифровизация оказывает влияние на защищенность государства, личности и общества и влияет непосредственно на обеспечение национальной безопасности. Эволюция технологической среды и чрезвычайно быстрые изменения в киберпространстве напрямую влияют на будущее национальной безопасности, соответствующее мышление, разработку принципов и методов. В перспективе технологическое превосходство будет играть важную роль, обеспечивая непредсказуемые преимущества странам с самыми современными возможностями и решениями.

Государственные органы власти осознают всю необходимость перехода на использование цифровых технологий, которые применяются для обеспечения национальной безопасности, но также и в смежных отраслях, в частности, для обеспечения информационной, технологической, финансовой и экономической безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. *Волостнов Н.С.* Государство как ключевой фактор обеспечения экономической безопасности // Экономическая безопасность России: проблемы и перспективы. 2014.

2. МВД создаст подразделение по борьбе с киберпреступностью // https://pravo.ru/news/239261/.

3. *Савельева Н.К., Макарова М.В.* Исследование рисков экономической безопасности компаний в процессе цифровой трансформации // Экономика и управление: проблемы, решения. 2021. Т. 2. № 8 (116).

4. *Саханевич Д.Ю.* Роль цифровизации в развитии социально-экономических систем // Ученые записки Тамбовского отделения РоСМУ. 2020.

5. Цифровая безопасность личности: что изменилось за год // https://www.garant.ru/article/1528258/.

6. *Шинкарецкая Г.Г., Берман А.М.* Цифровизация и проблема обеспечения национальной безопасности // Образование и право. 2020. № 5.

7. Этические риски «цифры» для государства // https://ethics.cdto.center/2021/2-3-ehticheskie-riski-cifry-dlya-gosudarstva.

8. Global Innovation Index // https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2021.pdf.

9. *Gobareva Y.L., Gorodetskaya O.Y., Karp M.V., Kolesova I.V.* Digitalization and national security: economic and political aspects for Russia and the EAEU // International Journal on Emerging Technologies. 2020. № 11 (5)7.

10. *Dobak I.* Thoughts on the evolution of national security in cyberspace // Security&Defence. 2021 // https://securityanddefence.pl/pdf-133154-64170?filename=Thoughts%20on%20the%20evolution.pdf.

11. ICT Development Index // https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf.

12. Networked readiness index // https://networkreadinessindex.org.

13. UN E-government knowledge base // https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/141-Russian-Federation.

D.A. GONCHAROVA
Postgraduate, Faculty of Global Studies
Moscow State University,
Moscow, Russia

DIGITAL DIMENTION OF NATIONAL SECURITY

Introduction. *Regardless of political and social systems, the existence of the national security sector and organisations can be considered universal in almost all states. The main task of national security organisations in each country is to support decision makers in the country with accurate, up-to-date information. Their main tasks are to obtain and analyse information. In the 20th century, specific areas of information gathering (e.g. SIGINT – Signal Intelligence, HUMINT – Human Intelligence, OSINT – Open Source Intelligence and MASINT – Measurement and Signature Intelligence) were developed to carry out these activities. At the same time, apart from their specific purpose and secrecy, these fields are undergoing constant change, and one of the most important shaping factors is the external technological environment. Consequently, monitoring changes in the external environment plays an important role, and national security decision-makers are also responding to them by improving their methods. On the one hand, digital technology allows for faster and easier information acquisition, but on the other hand it also leads to the emergence of risks.*

Research methodology. *The methodological basis of the study comprises general scientific research methods, such as synthesis, analysis, comparison, as well as a special research method, such as content analysis of official documents.*

Results of the study. *The study argues that digitalization brings both benefits and risks to national security, so each country needs to respond and support technological support for national security. Russia lags behind the U.S. in key digital dimensions. Russia lags behind, and work needs to be done at the legislative and departmental levels to improve economic competitiveness, develop ICT in Russia's different regions, and introduce initiatives to accelerate broadband penetration and increase the adoption of e-services by different sectors and by different levels of government.*

Discussion. *Digitalization as a process poses significant risks to maintaining the current position in the national security system focused on physical threats. The main threats to the new social organization are: digital terrorism; crime in the virtual environment; human psycho-emotional insecurity, lack of personal space in the digital environment; falsification of information; and threat to national sovereignty in the digital space.*

Conclusion. *In the future, technological superiority will play an important role, providing unpredictable advantages to countries with the most advanced capabilities and solutions. State authorities are aware of all the need to adopt digital technologies, which are used for national security, but also in related sectors, in particular for information, technological, financial and economic security.*

Key words: *digital economy, digital technology, challenges, national security, digitalization, digital transformation, ICT development index, digital terrorism.*