После оглашения итогов референдума 2016 г. в Великобритании, согласно которым страна выходит из ЕС, были рассмотрены проекты для определения статуса Северной Ирландии и ее дальнейших отношений с Республикой Ирландия после Брексита. Разработанные проекты установления границы с Республикой Ирландия не нашли широкой поддержки, а установление же жесткой границы противоречит Белфастскому соглашению, которое ко всему прочему предусматривает инициацию референдума о будущем Северной Ирландии.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. The Northern Ireland Peace Process [Electronic resource] // Council on Foreign Relations, 2019. – Mode of access: https://www.cfr.org/backgrounder/northern-ireland-peace-process. Date of access: 01.09.2019.

2. Smith, E. Brexit and the history of policing the Irish border [Electronic resource] // History&Policy, – 2016. – Mode of access: http://www.historyandpolicy.org/policy-papers/papers/brexit-and-the-history-of-policing-the-irish-border. – Date of access: 10.07.2019.

3. The Belfast Agreement / Good Friday Agreement 1998 [Electronic resource] // Government of the United Kingdom, – 1998. – Mode of access: https://www.gov.uk/government/publications/the-belfast-agreement. – Date of access: 10.07.2019.

4. EU referendum results [Electronic resource] // The Electoral Commission, 2016. – Mode of access: https://www.electoralcommission.org.uk/find-information-by-subject/elections-and-referendums/past-elections-and-referendums/eu-referendum/electorate-and-count-information. – Date of access: 11.04.2019.

5. The EU referendum Vote in Northern Ireland: Implications for our understanding of citizens' political views and behavior [Electronic resource] // Northern Ireland Assembly, 2017. – Mode of access: https://www.qub.ac.uk/brexit/Brexitfilestore/Filetoupload,728121,en.pdf. – Date of access: 01.09.2019.

6. Northern Ireland PEACE programme [Electronic resource] // Fact Sheets on the European Union, European Parliament, 2019. – Mode of access: http://www.europarl.europa.eu/factsheets/en/sheet/102/northern-ireland-peace-programme. Date of access: 01.09.2019.

7. Hayward, K. Bordering on Brexit: Views from Local Communities in the Central Border Region of Ireland / Northern Ireland [Electronic resource] // Irish Central Border Area Network, 2017. – Mode of access: https://www.qub.ac.uk/brexit/Brexitfilestore/Filetoupload,780606,en.pdf. Date of access: 01.09.2019.

8. The land border between Northern Ireland and Ireland [Electronic resource] // House of Commons Northern Ireland Affairs Committee, 2018. – Mode of access: https://publications.parliament.uk/pa/cm201719/cmselect/cmniaf/329/329.pdf. Date of access: 01.09.2019.

ДЕЯТЕЛЬНОСТЬ РЕСПУБЛИКИ БЕЛАРУСЬ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А. Р. Романовский[1)], С. Ф. Свилас[2)]

[1)] Белорусский государственный университет,
пр. Независимости, 4, 220030, г. Минск, Беларусь, aromanovsky35@gmail.com
[2)] Белорусский государственный университет,
пр. Независимости, 4, 220030, г. Минск, Беларусь, svilas@tut.b

В статье обоснована актуальность аналитических работ в области информационной безопасности, охарактеризованы подходы зарубежных государств, политиков и экспертов к этой проблеме, определен уровень развития цифровой экономики и сектора информационно-коммуникационных услуг в Беларуси. Объект исследования – национальная безопасность. Цель исследования – оценка акций Республики Беларусь по обеспечению своей информационной безопасности. Научная новизна исследования - анализ Концепции информационной безопасности Беларуси (2019 г.), а также инициативы республики по формированию «пояса цифрового добрососедства». Практическая значимость исследования – определение значения Концепции для укрепления информационного суверенитета и информационного нейтрали-

тета Республики Беларусь, положительного имиджа белорусского государства на международной арене.

Ключевые слова: Республика Беларусь; кибербезопасность; Концепция информационной безопасности Беларуси; информационный суверенитет; информационный нейтралитет; «пояс цифрового добрососедства»; Международная антитеррористическая конференция ООН.

ACTIVITIES OF THE REPUBLIC OF BELARUS TO PROMOTE INFORMATION SECURITY

A.R. Romanovsky[a], S.F. Svilas[b]

[a]Belarusian State University, Niezaliežnasci Avenue, 4, 220030, Minsk, Belarus
[b]Belarusian State University, Niezaliežnasci Avenue, 4, 220030, Minsk, Belarus
Corresponding author: A.R. Romanovsky (aromanovsky35@gmail.com)

The article justifies the relevance of analytical studies in the field of information security, characterizes the approaches of foreign states, politicians and experts to this problem, defines the level of development of the digital economy and the sector of information and communication services in Belarus. The object of the research is national security. The purpose of the study is to assess the actions of the Republic of Belarus to ensure its information security. The scientific novelty of the study consists in providing analysis of the Concept of Information Security of Belarus (2019), as well as of the initiative to form a "belt of digital neighborliness". The practical relevance of the study is in determining the significance of the Concept for strengthening the information sovereignty and information neutrality of the Republic of Belarus and the positive image of the Belarusian state in the international arena.

Keywords: Republic of Belarus, cyber security; Concept of information security of Belarus; information sovereignty; information neutrality; "belt of digital neighborliness"; UN International Anti-Terrorist Conference.

Человечество давно перешагнуло индустриальную эпоху и вступило в новую эру своего развития, когда информация и знания становятся ключевым фактором прогресса. Объемы производимой в мире информации стремительно увеличиваются: с двух зеттабайт в 2010 г. до 33 зеттабайт в 2018 г. По прогнозам, к 2025 г. эта цифра возрастет до колоссального значения в 175 зеттабайт [12]. Доступ к Интернету все чаще трактуется как неотъемлемое право человека. В нашу повседневность решительно входят такие ранее казавшиеся фантастическими понятия, как искусственный интеллект, блокчейн, «интернет вещей» и многие другие. Большие объемы информации широко используются в бизнесе и становятся орудием в политической борьбе.

Российский эксперт профессор МГИМО А. И. Смирнов указывает на то, что мир переходит к шестому технологическому укладу, в основе которого лежит «не двигательная сила, направленная на базовые элементы глобальной конкуренции, а интеллектуальные силы человека» [9, с. 48]. При этом сложно не согласиться с еще одним российским исследователем Е. С. Зиновьевой, которая отмечает, что развитие новых технологий, помимо очевидных выгод человечеству, создает новые и усугубляет существующие угрозы безопасности и устойчивому развитию, трансформирует природу и формы протекания международных конфликтов, порождает новые виды преступности и терроризма [4, с. 157].

Вышеуказанные факторы обусловливают исключительную важность принятия исчерпывающих мер по обеспечению информационной безопасности государства, общества и индивида, и высокую актуальность избранной темы исследования.

Вопросам информационной или, как ее называют на Западе, кибербезопаности придается большое значение во многих странах мира. США рассматривают ки-

берсферу как ключевое поле для своего доминирования. Так, в обновленной Стратегии кибербезопасности США, принятой в сентябре 2018 г. при президенте Д. Трампе, в качестве цели прямо провозглашается сохранение лидирующих позиций Соединенных Штатов в киберсфере [13].

М. Кастельс отмечает, что сегодня борьба за власть в глобальной информационной сфере обострилась. В России, Китае, развивающихся странах правительства стремятся защитить свое информационное пространство. Примерами такого обострения могут выступать цензура электронной почты в Китае; активное законодательное регулирование информационной сферы в Европейском союзе и т.д. Появление «цифровых границ» связано с легкостью доступа к информации в современном мире, что создает возможности воздействия на общественное мнение поверх государственных границ [6, с. 320].

Согласно Доктрине информационной безопасности России, под этим термином понимается «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз». Информационная безопасность обеспечивает реализацию конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое социально-экономическое развитие Российской Федерации, оборону и безопасность государства [3].

В Беларуси цифровая сфера получила интенсивное развитие с начала 2000-х годов. Согласно Индексу развития ИКТ, который составляет Международный союз электросвязи, Беларусь в 2017 г. занимала 32-ю позицию в мире, вплотную приблизившись к тридцатке наиболее развитых в плане информационных технологий стран и обогнав ряд государств-членов Евросоюза (Словения – 33 место, Латвия – 35, Хорватия – 36, Греция - 38), а также большинство стран СНГ (Россия – 45-е, Казахстан – 52-е и т.д.) [11].

В республике заметными темпами развивается цифровая экономика и сектор информационно-коммуникационных услуг. Локомотивом этого процесса выступает Парк высоких технологий, резидентами которого по состоянию на 3 октября 2019 г. являлись 684 компании из 67 стран мира. [10]. Экспорт ПВТ в 2018 г. составил 1,4 млрд долл. США, львиная доля которого идет в США и страны Европейского союза [5]. Доля ИКТ в ВВП страны составляет 5,5%, что сопоставимо с сельским и лесным хозяйством (6,4%), строительством (5,4%), транспортом (5,8%). Ожидается, что к 2022 г. доля ИТ в ВВП Беларуси вырастет до 10% [11]. Столь высокие темпы цифровизации обусловили принятие соответствующих мер регулирования на законодательном уровне, в том числе по обеспечению информационной безопасности Беларуси.

В марте 2019 г. Совет Безопасности Республики Беларусь одобрил Концепцию информационной безопасности (КИБ) Беларуси. В этом документе информационная безопасность определяется как «состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере».

Основной целью обеспечения информационной безопасности обозначено достижение и поддержание такого уровня защищенности информационной сферы, который обеспечивает реализацию национальных интересов Республики Беларусь и ее прогрессивное развитие. В числе целей государственной политики в сфере информационной безопасности выделяются такие, как предупреждение и нейтрализация информационных рисков, вызовов и угроз, в том числе киберпреступности и кибертерроризма, разработка средств обеспечения информационной безопасности и др.

КИБ оперирует такими новыми для политического и дипломатического дискурса категориями, как «информационный суверенитет» и «информационный

нейтралитет». Предусматривается также введение государственно-частного партнерства с целью привлечения компетенций, кадров, технологий, капитала частных предприятий, повышения отдачи использования бюджетных средств и активов предприятий, совместной разработки и реализации инвестиционных и иных проектов в области информационной безопасности.

При этом документом гарантируется конституционное право граждан свободно искать, получать, передавать, производить, хранить и распространять информацию любым законным способом, право на тайну личной жизни и иную охраняемую законом тайну, защиту персональных данных и авторских прав, а также соблюдение баланса прав с ограничениями, связанными с обеспечением национальной безопасности.

Несмотря на то, что «высокотехнологичные» угрозы международной безопасности не всегда исходят от государств, именно последние играют ключевую роль в обеспечении международной стабильности, при этом большинство современных угроз носят глобальный характер и бороться с ними невозможно без принятия согласованных мер, эффективного международного сотрудничества.

Характерно, что в число целей КИБ входит осуществление усилий по повышению действенности международного права и соблюдению моральных норм ответственного поведения в информационном пространстве, содействие разработке и внедрению мер по укреплению доверия в информационном пространстве. КИБ предусматривает налаживание каналов международного обмена опытом в области обеспечения информационной безопасности, а также информацией об угрозах национальным интересам, в том числе уязвимостях информационных систем, инцидентах в информационной инфраструктуре [7].

Выступая в общей дискуссии на 74-й сессии Генеральной Ассамблеи ООН в Нью-Йорке в сентябре 2019 г., Министр иностранных дел Беларуси В. Макей отметил, что мир находится на начальном этапе долгосрочного глобального процесса, именуемого технологической гонкой вооружений. Опасность в том, что эту гонку могут использовать как силы добра, так и силы зла, и задача мирового сообщества – сделать все, чтобы зло не получило шансов на доминирование. Руководитель внешнеполитического ведомства республики подчеркнул в этой связи необходимость расширения межгосударственного цифрового сотрудничества, повышения взаимного доверия в информационной сфере» [2].

Поэтому не случайно вслед за принятием Концепции информационной безопасности Республикой Беларусь была выдвинута инициатива о формировании «пояса цифрового добрососедства» путем заключения двусторонних и многосторонних соглашений об обеспечении международной информационной безопасности, которая была озвучена Главой белорусского государства А. Г. Лукашенко на Международной антитеррористической конференции под эгидой ООН, состоявшейся 3 сентября 2019 г. в Минске [8].

Белорусская дипломатия в качестве ключевых элементов таких договоренностей рассматривает идеи цифрового суверенитета и нейтралитета, а также невмешательства стран в информационные ресурсы друг друга. Цифровой суверенитет должен гарантировать способность государства контролировать свое информационное поле, предупреждать и блокировать кибератаки, обеспечивать надежную защиту критической инфраструктуры. Он предполагает, что страны не будут предпринимать в киберпространстве действия, наносящие ущерб безопасности иных государств. В конечном итоге такие соглашения станут основой для выработки международных правил ответственного поведения в виртуальном пространстве, укрепят связи между странами, повысят эффективность совместного противодействия террористическим угрозам в киберпространстве [1].

Таким образом, Республика Беларусь как государство с развитой сферой информационно-коммуникационных технологий придает важное значение обеспечению информационной безопасности на национальном, региональном и глобальном уровнях. Формирующаяся в этой области законодательная база направлена на обеспечение безопасных условий для дальнейшего эффективного развития информационного сектора при одновременном обеспечении конституционных прав граждан на получение и распространение информации.

Логическим следствием IT-сектора и в целом миролюбивой внешней политики Беларуси можно считать выдвижение Республикой Беларусь такой крупной международной инициативы, как создание «пояса цифрового добрососедства», направленной на снижение напряженности и сближение позиций крупных мировых игроков в киберсфере.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. Беларусь призывает страны ООН принять меры для обеспечения международной информационной безопасности [Электронный ресурс]. – Режим доступа: https://www.belta.by/special/politics/view/belarus-prizyvaet-strany-oon-prinjat-mery-dlja-obespechenija-mezhdunarodnoj-informatsionnoj-363621-2019/. – Дата доступа: 07.10.2019.

2. Выступление Министра иностранных дел Беларуси В.Макея в общей дискуссии на 74-й сессии Генеральной Ассамблеи ООН 26 сентября 2019 г. [Электронный ресурс]. – 2019 – Режим доступа: http://mfa.gov.by/press/news_mfa/b698116bea64ee66.html. – Дата доступа: 07.10.2019.

3. Доктрина информационной безопасности РФ от 05.12.2016. Утверждена указом Президента № 646 [Электронный ресурс]. – 2016. – Режим доступа: http://static.kremlin.ru/ media/events/files/ru/tGeA1AqAfJ4uy9jAOF4CYCpuLQw1kxdR.pdf. – Дата доступа: 07.10.2019.

4. Зиновьева, Е. С. Международное сотрудничество по обеспечению информационной безопасности: проблемы, субъекты, перспективы : дис. ... докт. ист. наук: 23.00.04 / Е. С. Зиновьева. – М., 2017. – 332 л.

5. Как сработал ПВТ в 2018 году: экспорт, зарплаты, рабочие места [Электронный ресурс]. – 2019. – Режим доступа: https://news.tut.by/economics/628437.html. – Дата доступа: 07.10.2019.

6. Кастельс М. Могущество самобытности // Новая постиндустриальная волна на Западе. Антология / Под ред. В.Л. Иноземцева. М.: Academia, 1999.

7. Концепция информационной безопасности Республики Беларусь. Утверждена Постановлением Совета безопасности Республики Беларусь от 18.03.2019 № 1 [Электронный ресурс]. – 2019. – Режим доступа: http://president.gov.by/uploads/documents/2019/1post.pdf. – Дата доступа: 07.10.2019.

8. Лукашенко выступил с инициативой формирования "пояса цифрового добрососедства" [Электронный ресурс]. – 2019. – Режим доступа: https://www.belta.by/president/view/lukashenko-vystupil-s-initsiativoj-formirovanija-pojasa-tsifrovogo-dobrososedstva-360560-2019/. – Дата доступа: 07.10.2019.

9. Смирнов, А. И. Современные информационные технологии в международных отношениях: монография / А.И. Смирнов; Моск. гос. ин-т между- нар. отношений (ун-т) М-ва иностр. дел Рос. Федерации, Центр международной информационной безопасности и научно-технологической политики. — Москва: МГИМО-Университет, 2017. – 334 с.

10. Факты и цифры [Электронный ресурс]. – 2019. – Режим доступа: http://www.park.by/topic-facts/. – Дата доступа: 07.10.2019.

11. ICT Development Index 2017 [Электронный ресурс]. – 2017. – Режим доступа: https://www.itu.int/net4/ITU-D/idi/2017/index.html. – Дата доступа 07.10.2019.

12. Information created globally 2010-2025 [Электронный ресурс]. – 2019. – Режим доступа: https://www.statista.com/statistics/871513/worldwide-data-created. – Дата доступа: 07.10.2019.

13. National Cyber Strategy of the United States of America of September 2018 [Электронный ресурс]. – 2018. – Режим доступа: https://www.whitehouse.gov/wp-content/uploads/2018/09/ National-Cyber-Strategy.pdf. – Дата доступа: 07.10.2019.