Научная статья
Социологические науки
УДК: 32.019.51; 316.77
https://doi.org/ 10.53658/RW2022-2-2(4)-100-131

Информационный суверенитет: материалы научной дискуссии

Николай Петрович Грибин[1a]✉, Ирина Николаевна Кохтюлина[2b]✉, Денис Игоревич Седунов[3c]✉, Егор Ильич Соболев[4d]✉

[1] Московский государственный институт международных отношений (Университет) МИД России, Москва, Россия
[2] Национальный институт исследований глобальной безопасности, Москва, Россия
[3] Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Москва, Россия
[4] Национальный исследовательский институт развития коммуникаций, Москва, Россия
[a] n.gordin40@gmail.com, htpps://orcid.org/0000-0001-9141-445
[b] expobroker@yandex.ru
[c] DenisSedunov@list.ru
[d] 1032193499@rudn.ru

Аннотация. Статья содержит наиболее значимые и интересные материалы научной дискуссии, проведенной Национальным исследовательским институтом развития коммуникаций по проблемам информационного суверенитета и информационной безопасности России. Авторами обозначены основные угрозы и риски устойчивости и стабильности Российской Федерации в эпоху цифровизации; рассмотрены подходы к определению понятия «информационный суверенитет», определены его критерии, выявлены проблемы обеспечения информационного суверенитета России, в частности, связанные с технологической зависимостью России от зарубежных

ISSN 2782-3067 (Print)

технологий и оборудования, слабой защищенностью российской информационной инфраструктуры. В ходе дискуссии были выработаны рекомендации: 1) значительно увеличить финансирование российской высокотехнологичной промышленности, поддержать российские исследования в области компьютерных технологий, чтобы свести зависимость от иностранной продукции к минимальным значениям и повысить защищенность объектов критической инфраструктуры; 2) продолжать развитие отдельного направления в области кибербезопасности в Вооруженных Силах РФ, наращивать военный потенциал в области цифровых технологий; 3) проводить активную политику в информационной сфере, направленную на борьбу с ложными сообщениями; 4) отслеживать распространение противоправной информации в социальных сетях; 5) начать реализацию государственной политики в сфере просвещения населения по вопросам информационной безопасности, правилам безопасного взаимодействия граждан с цифровыми технологиями; 6) усилить контроль за противоправной деятельностью в Интернете.

Ключевые слова: государство, информационный суверенитет, информационная безопасность, угрозы информационному суверенитету

Для цитирования: Грибин Н.П., Кохтюлина И.Н., Соболев И.И., Седунов Д.И. Информационный суверенитет: материалы научной дискуссии // Россия и мир: научный диалог. 2022. № 2(4). С. 100-131. https://doi.org/10.53658/RW2022-2-2(4)-100-131

Original article
https://doi.org/10.53658/RW2022-2-2(4)-100-131

Sociological sciences

Information sovereignity: materials of scientific discussion

Nikolai P. Gribin[1a]✉, Irina N. Kohtyulina[2b]✉, Denis I. Sedunov[3c]✉, Egor I. Sobolev[4d]✉

[1] Moscow State Institute of International Relations (University) Russian Foreign Ministry, Moscow, Russia
[2] National Institute for Global Security Studies, Moscow, Russia
[3] Russian Presidential Academy of National Economy and Public Administration, Moscow, Russia
[4] National Research Institute for the Development of Communications, Moscow, Russia
[a] n.gordin40@gmail.com, htpps://orcid.org/0000-0001-9141-445
[b] expobroker@yandex.ru
[c] DenisSedunov@list.ru
[d] 1032193499@rudn.ru

ISSN 2782-3067 (Print)

Abstract. The article contains the most significant and interesting materials of the scientific discussion on the problems of information sovereignty and information security in Russia held by the National Research Institute for the Communications Development. The authors identify the main threats and risks to the stability of the Russian Federation in the era of digitalization. Approaches to the definition of the concept of «information sovereignty» are considered, its criteria are defined. Problems of ensuring the information sovereignty of Russia are identified, in particular, relating to Russia's technological dependence on foreign technologies and equipment, weak security of the Russian information infrastructure. During the discussion, recommendations were developed: 1) significantly increase the financing of the Russian high-tech industry, support Russian research in the field of computer technology in order to reduce dependence on foreign products to a minimum and increase the security of critical infrastructure facilities; 2) to continue the development of a special direction in the sphere of cybersecurity in the Russian Armed Forces, increase military potential in the sphere of digital technologies; 3) to pursue an active information policy aimed at combating false messages; 4) to monitor the dissemination of illegal information in social networks; 5) to begin the implementation of state policy in the field of public education on information security, rules for safe interaction with digital technologies; 6) to strengthen control over illegal activities on the Internet.

Keywords: state, information sovereignty, information security, threats to information sovereignty

For citation: Nikolai P. Gribin. Irina N. Kohtyulina, Denis I. Sedunov, Egor I. Sobolev. Information sovereignty: materials of scientific discussion. Russia & World: Scientific Dialogue. 2022. No. 2(4). pp. 100-131. https://doi.org/10.53658/RW2022-2-2(4)-100-131

Введение

Актуальность научной дискуссии о проблемах и критериях информационного суверенитета обусловлена рядом причин, связанных и с усилением международного информационного противоборства, ужесточением техники информационных войн, все более недружественной информационной политикой ряда зарубежных стран в отношении России. Несмотря на то, что не первый год ведется работа по созданию правовой базы, которая бы регулировала международное информационное пространство и место в нем государств, проблематика информационного суверенитета только обостряется. Цель нашей дискуссии – определить критерии информационного суверенитета, обозначить риски и угрозы информационному суверенитету России, рассмотреть опыт его обеспечения в других странах, определить возможные пути решения проблем информационного суверенитета.

Материалы и методы

Авторы научной дискуссии в своих исследованиях применяли системный, институциональный подходы, опирались на концепции политического реализма, использовали метод сравнительного анализа. Эмпирическую базу исследования составили статистические данные, материалы аналитических отчетов, решения и нормативные правовые акты: международные доклады ООН (доклады группы правитель-

ственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2013[1] и 2015[2] годов), национальные стратегии и доктрины (Национальная стратегия безопасности КНР в киберпространстве[3], Национальная киберстратегия США[4], Киберстратегия Министерства обороны США[5], Доктрина информационной безопасности Российской Федерации[6], Стратегия национальной безопасности Российской Федерации[7], Военная доктрина Российской Федерации[8]), законы, связанные с обеспечением информационного суверенитета.

Результаты исследования

Угрозы и риски устойчивости и стабильности Российской Федерации в эпоху цифровизации (Грибин Н.П.)

В современной обстановке турбулентных геополитических процессов, непредвиденных взрывоопасных событий и международных конфликтов, отражающих нарастание межгосударственных противоречий, противоборство глобальных и региональных стран-лидеров за гегемонию в установлении правил и принципов мироустройства, бескомпромиссное продвижение собственных национальных интересов, нередко в ущерб других субъектов международного права, все более заметную роль играют передовые технологии. Наряду с раскрытием неограниченных возможностей для ускоренного развития человеческой цивилизации и быстрого решения множества сложнейших проблем в государственном управлении, экономике, бизнесе и социальной сфере технологический инструментарий становится ключевым средством достижения преимуществ в вооруженных столкновениях, экономической и торговой экспансии, информационно-психологическом противостоянии соперничающих государств и их коалиций.

Именно на эту сторону феномена происходящей в наши дни научно-технической революции обратил внимание Президент Российской Федерации В.В. Путин,

1 Доклад группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. A/68/98. URL: //http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=R.

2 Доклад группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. A/70/174. URL: //https://documents-ddsny.un.org/doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf?OpenElement.

3 Национальная стратегия безопасности в киберпространстве. URL: http://www.cac.gov.cn/2016-12/27/c_1120195926.htm.

4 National Cyber Strategy of the United States of America. URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

5 Department of Defense Cyber Strategy – 2018. URL: https://www.cybercom.mil/About/Mission-and-Vision/.

6 Доктрина информационной безопасности Российской Федерации. URL: http://www.scrf.gov.ru/documents/6/5.html.

7 Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации». URL: http://publication.pravo.gov.ru/Document/View/0001202107030001.

8 Военная доктрина Российской Федерации (утв. Президентом Российской Федерации 25.12.2014 № Пр-2976). URL: https://www.mchs.gov.ru/dokumenty/2940.

заявивший в 2019 году на Петербургском международном экономическом форуме о «первой технологической войне, наступающей в цифровой эпохе». Глава российского государства выделил квинтэссенцию этой войны:

> Попытки монополизировать новую технологическую волну, ограничить доступ к ее плодам выводят на совершенно новый, иной уровень проблемы глобального неравенства как между странами и регионами, так и внутри самих государств. Ну а это есть главный источник нестабильности в мире[9].

Усиление геополитической напряженности и неопределенные перспективы ее смягчения обусловили потребность в отвечающей современным реалиям защите жизненно важных интересов Российской Федерации от внешних и внутренних врагов, в том числе от недружественных действий иностранных государств. В результате была принята новая Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации 2 июля 2021 года № 400.

В Стратегии указано, что главной «целью научно-технического развития Российской Федерации является обеспечение технологической независимости и конкурентоспособности страны». Для достижения этой цели требуется разработка и внедрение перспективных высоких технологий, таких как нанотехнологии, робототехника, генная инженерия, информационно-коммуникационные технологии, искусственный интеллект, технологии обработки колоссальных массивов данных, создание новых материалов.

В Стратегии высказывается уверенность, что воплощение в жизнь намеченных амбициозных планов приведет к «укреплению обороноспособности, модернизации экономики и развитию промышленного потенциала, укреплению суверенной государственности России, способной проводить самостоятельную внешнюю и внутреннюю политику, эффективно противостоять попыткам внешнего давления».

Представляется, однако, что было бы поверхностно не замечать негативные сопутствующие проявления и недостатки в происходящем многообещающем, стремительно развивающемся технологическом рывке. По своей сути такие проявления и недостатки имеют очевидные признаки угроз и рисков в случае безоглядного внедрения во все сферы государства и общества цифровых технологий, идеи и достоинства которых сегодня преподносятся в массмедиа преимущественно в восторженных тонах. Нетрудно предположить, что уже сейчас просматривающиеся, пока еще не всегда явные угрозы и риски рано или поздно скажутся в той или иной мере на результативности применяемых технологических инноваций.

В этой связи полагаю полезным заострить внимание на некоторых очевидных угрозах и рисках эпохи цифровизации, которые в конечном счете могут негативно отразиться на устойчивости и стабильности государства в случае непринятия мер по

9 Петербургский международный экономический форум. С.-Петербург, 7 июня 2019 года. URL: https://www.1tv.ru/news/2019-06-07/366537-vladimir_putin_vystupil_na_ekonomicheskom_forume_v_sankt_peterburge.

их нейтрализации, что напрямую затрагивает интересы обеспечения национальной безопасности Российской Федерации.

Угрозы и риски цифровизации, которая в научном обороте иногда заменяется термином «диджитализация» (от английского слова digitalization, digital, в качестве прилагательного оно переводится как «цифровой», a ization означает действие или процесс), условно можно подразделить на два разновеликих блока. Первый блок формируется на основании показателя масштабности применения цифровых технологий, порождающих угрозы и риски общего плана. Второй блок составляют угрозы и риски, возникающие в процессе использования цифровых технологий в конкретных сферах жизни государства и социума. С точки зрения внешнего проявления угрозы и риски могут быть реальные и потенциальные и проявляться в обоих блоках.

Главная угроза общего плана в осуществлении цифровой трансформации всей страны видится в том, что в сегментах электронного оборудования («железа») и программного обеспечения («софт») практически все потребности внутреннего российского рынка восполняются за счет импорта. Этот факт подтверждается в Стратегии развития информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года, утвержденной Правительством Российской Федерации 1 ноября 2013 года (№ 2036-р). По оценкам специалистов в сфере информационных технологий, на сегодняшний день ситуация существенно не изменилась. Вследствие этого иностранные производители такого класса продукции по-прежнему занимают доминирующие позиции на отечественном IT-рынке, и это дает им возможность диктовать свои условия. Сложившаяся ситуация особенно опасна ввиду обострения внешних угроз России, наращивания санкций против нашей страны, противозаконного съема информации из телекоммуникационных систем, реальной возможности блокировки приобретенного импортного оборудования и деформации программного обеспечения, участившихся кибератак на государственные структуры, корпорации и частный бизнес. В таких условиях правомерен вопрос о способности страны обеспечить отечественную суверенную цифровизацию.

Для парирования воздействия реальной угрозы IT-зависимости России от стран Запада представляется целесообразным усилить регулирующую роль государства по образцу мероприятий в электронной промышленности в США, КНР и Южной Корее, которые благодаря такому решению резко продвинулись вперед в этой отрасли. В частности, было бы желательно:

- увеличить прямую бюджетную поддержку российских IT-компаний, создать для них льготный налоговый режим, обеспечить доступными долгосрочными кредитами;
- ограничить и в перспективе запретить использование в Российской Федерации иностранных IT-технологий;
- законодательно обязать государственные структуры, корпорации и бизнес осуществлять закупки отечественных IT-технологий, которые, по данным экспертов, не уступают по качеству зарубежным.

Другая угроза общего плана связана с искусственным интеллектом, за которым сегодня закрепилось определение «главная технология XXI века», представляющая собой сквозные научно-технологические направления. Спектр применения искусственного интеллекта и производной от него роботизации неограниченно широк. Это в первую очередь производство, социальная сфера, образование, наука и культура. Искусственный интеллект открывает уникальные возможности для быстрого анализа огромного объема данных, улучшения качества жизни человека, совершенствования образования и медицинского обслуживания, повышения радикальным образом производительности труда практически во всех отраслях экономики. С помощью таких инноваций люди освобождаются от рутинных, тяжелых, трудоемких и опасных процессов в производстве, совершается меньше ошибок в трудовой деятельности, минимизируются издержки в ходе изготовления продукции. Например, алгоритмы искусственного интеллекта облегчают врачам быстрое обнаружение опасных болезней, позволяют с высокой точностью анализировать результаты медицинских исследований, дают возможность значительно увеличивать качество диагностики, что особенно важно в период продолжающейся пандемии.

Вместе с тем нельзя игнорировать вполне оправданные опасения, что уникальные технологии искусственного интеллекта и роботизация повлекут утрату многих рабочих мест и специальностей как в нашей стране, так и за рубежом. Предполагается, что во всем мире потеряют работу около 85 млн человек. Люди, лишенные работы и средств к существованию, могут пополнить ряды протестующих, незаконных вооруженных формирований, террористов и экстремистов, а также увеличить потоки неконтролируемой миграции, в том числе исходящей из иностранных государств, в Российскую Федерацию. Вряд ли будет приветствоваться обществом идея установления тотального контроля за каждым шагом человека с помощью «умных» технических средств. Высказывается даже фантастическое предостережение о возможном «восстании» машин, что, конечно, едва ли вероятно, поскольку человек всегда будет держать машины под контролем. Минусы в использовании искусственного интеллекта и роботизации видятся также в высокой стоимости поддержания в рабочем состоянии высокотехнологичных и сложных механизмов, созданных на базе таких инноваций, и в больших затратах на их ремонт.

Немаловажное значение имеет риск утечки персональных данных каждого человека вследствие участия искусственного интеллекта в обработке всего массива информации о населении страны, становящейся открытой и доступной. Важным шагом купирования такого риска является Федеральный закон «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации», принятый 8 июня 2020 года (№ 168-ФЗ). В законе установлены критерии допуска только компетентных государственных органов к такого рода информации. В настоящее время прорабатывается вопрос создания и других нормативно-правовых, технических и организационных барьеров, препятствующих утечке персональных данных российских граждан и противоправному их использованию.

И еще одна мысль, связанная с цифровыми технологиями, касается распространения информации о российских достижениях в сфере военных технологий, создании ультрасовременных ударных боевых систем, сверхзвуковых (со многими махами) летательных аппаратов и ракет, аналогов которым на Западе нет. Конечно, испытываешь гордость за такие успехи наших ученых, конструкторов, специалистов и страны в целом. Однако, наверное, нельзя упускать из виду и другую сторону вопроса – невольную подпитку недругов России аргументацией о якобы существующей угрозе западной цивилизации со стороны нашей страны. Путем соответствующей интерпретации этой темы, которая постоянно присутствует в новостных сводках стран Запада, недружественные государства психологически обрабатывают свое население и негативно настраивают его против Российской Федерации и ее граждан. Фокусирование внимания на псевдоугрозе со стороны России расширяет мотивацию правящих кругов государств Запада ежегодно наращивать свои и так уже огромные военные бюджеты, в разы превышающие российские расходы на оборону. Одновременно фейк об агрессивности нашей страны используется для оправдания перед внешним миром демонстрации собственных «оборонных» мероприятий и войсковых учений в сопредельных России странах и вдоль границ Российской Федерации.

Второй блок угроз и рисков проявляется, как отмечалось, в процессе использования цифровых технологий в конкретных сферах социально-экономической деятельности, прежде всего в государственном управлении, экономике, энергетике, образовании, здравоохранении, городском хозяйстве, культуре, науке и статистике.

В кратком выступлении невозможно глубоко и всесторонне осветить особенности и нюансы угроз и рисков от внедрения цифровых технологий во все области жизнедеятельности государства и общества. Поэтому для иллюстрации позволю себе остановиться лишь на некоторых из названных сфер. В частности, рассмотрим положение дел в экономике и связанной с ней науке.

В сфере экономики, к сожалению, наблюдается медленное внедрение цифровых технологий. Это особенно бросается в глаза, если вспомнить, что Президент Российской Федерации В.В. Путин еще в декабре 2016 года подписал Указ «О Стратегии научно-технологического развития Российской Федерации»[10], где были предусмотрены меры по созданию правовых, технических, организационных и финансовых условий для развития цифровой экономики в стране. Однако спустя более пяти лет цифровая экономика в России, по оценкам экспертов, составляет лишь 4% от ВВП, в то время как в США этот показатель равен 10%. Одной из причин такого положения является отсутствие стимулирующих механизмов, способствующих развитию инновационной деятельности субъектов хозяйствования, и это, в свою очередь, сохраняет в российской экономике крен на экспорт сырья.

10 Указ Президента Российской Федерации «О Стратегии научно-технологического развития Российской Федерации» от 01 декабря 2016 года № 642. URL: http://kremlin.ru/acts/bank/41449.

В этой связи перевод экономики страны на качественно новый уровень за счет цифровых технологий снова провозглашается приоритетом в политике освоения несырьевой модели развития. Но ограничиваться декларациями об ускоренном развитии цифровых технологий и быстром их внедрении в повседневную жизнь явно недостаточно, так как разработка, изготовление, апробация и популяризация в обществе и в деловых кругах преимуществ цифровых технологий требует усилий больших коллективов ученых и специалистов, а также современной дорогостоящей материально-технической базы. Приходится, однако, констатировать, что на сегодняшний день отечественная наука находится в положении, которое вряд ли можно назвать благополучным, и прежде всего по причине недофинансирования. Согласно сайту Счетной палаты Российской Федерации, расходы на науку в стране составляют в настоящее время около 1,1% ВВП. В США на науку выделяется 2,8% ВВП, в КНР – 2,2%, в Южной Корее – 4,8%[11]. За счет последних научно-технологических достижений американцы снижают цену на сланцевую нефть, и наша нефтедобыча на Севере, особенно на шельфе северных морей, может скоро оказаться неконкурентоспособной.

Буквально несколько слов об угрозах и рисках при использовании цифровых технологий в образовании. Так, при дистанционной форме обучения отсутствует непосредственное общение между обучающимися и преподавателями, не вырабатываются навыки социальной коммуникабельности, исчезает взаимообогащающий знаниями диалог между ними, снижается восприятие информации и затрудняется понимание материала. Такая система обучения технически не в состоянии контролировать самостоятельность выполнения заданий и тестов. Фиксируются также физические отклонения в здоровье участников дистанционного обучения: ухудшение зрения, головная боль, бессонница, раздражительность.

Выводы

В заключение хотелось бы отметить, что в данной дискуссии мной обозначены лишь некоторые, наиболее значимые реальные и потенциальные угрозы и риски государству и обществу в эпоху цифровизации. Кстати, часть из них только с натяжкой можно квалифицировать как угрозы. Скорее это недостатки или издержки развития цифровой цивилизации, которые человечество способно нейтрализовать или хотя бы снизить их отрицательное воздействие при условии выявления, глубокого изучения и всестороннего научного осмысления цифровой составляющей нашей жизни, а также продуманной разработки и реализации комплекса эффективных и достаточных мер превентивного противодействия.

11 Результаты экспертно-аналитического мероприятия «Определение основных причин, сдерживающих научное развитие в Российской Федерации: оценка научной инфраструктуры, достаточность мотивационных мер, обеспечение привлекательности работы ведущих ученых.» URL: https://ach.gov.ru/upload/iblock/89d/89d7d756dab6d050a260ecc55d3d5869.pdf.

Международная информационная безопасность в новых геополитических реалиях (Кохтюлина И.Н.)

Человечество вошло в зону тотальной ломки миропорядка. По мнению ряда экспертов, все большую подрывную роль в данном процессе и процессе десуверенизации национальных государств играют информационно-коммуникационные технологии (ИКТ) и инфогенный нарратив в целом.

Одновременно планета охвачена беспрецедентной цифровой трансформацией. Мощный импульс к обострению геополитического противоборства придала и пандемия коронавируса. Человечество с каждым днем все больше осознает ее гигантские масштабы, ведущие эксперты сравнивают это с Великой депрессией и называют величайшим глобальным вызовом со времен Второй мировой войны.

Пандемия COVID-19 стала триггером как многих преимуществ, так и угроз цифрового мира. С учетом особой остроты данной проблемы Генеральный секретарь ООН А. Гутерриш предложил 11 июня 2020 года Дорожную карту по цифровому сотрудничеству: осуществление рекомендаций Группы высокого уровня по цифровому сотрудничеству[12]. Ее драйвером стали интернет-технологии, которые вызвали и продолжают вызывать тектонические сдвиги в развитии цивилизации. По сути, человечество вступило в новый фазовый переход, сравнимый по значению, например, с созданием письменности. При этом на смену микроэлектронике пришел новый технологический уклад: нано-, био-, инфо- и когнитивные технологии, а на основе принципов Industry IV стремительно развивается цифровая экономика, киберфизические системы, искусственный интеллект, квантовые вычисления, блокчейн, связь поколения 5G и иные, кардинально меняющие мир, технологии.

В этих условиях ведущие страны разрабатывают и реализуют разнообразные доктрины и стратегии по внедрению данных технологий с целью геополитического доминирования.

В силу этого неоценимое значение и стратегическую важность в создании безопасного глобального информационного пространства имеют утвержденные Указом Президента Российской Федерации от 12 апреля 2021 года № 213 «Основы государственной политики в области международной информационной безопасности»[13] (далее – Основы). Данный документ направлен на продвижение российских подходов к формированию системы обеспечения международной информационной безопасности и российских инициатив в этой сфере, на содействие созданию международно-правовых механизмов предотвращения и урегулирования межгосударственных конфликтов в глобальном информационном пространстве и на организацию межведомственного взаимодействия.

12 Official Documents System of the United Nations. URL:https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/102/53/PDF/N2010253.pdf?OpenElement .

13 «Основы государственной политики в области международной информационной безопасности», утверждены Указом Президента Российской Федерации от 12 апреля 2021 г. № 213. URL:http://kremlin.ru/acts/bank/46614 .

Среди угроз международной информационной безопасности в Основах выделены следующие:

> а) использование информационно-коммуникационных технологий в военно-политической и иных сферах в целях подрыва (ущемления) суверенитета, нарушения территориальной целостности государств, осуществления в глобальном информационном пространстве иных действий, препятствующих поддержанию международного мира, безопасности и стабильности;
>
> б) использование информационно-коммуникационных технологий в террористических целях, в том числе для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;
>
> в) использование информационно-коммуникационных технологий в экстремистских целях, а также для вмешательства во внутренние дела суверенных государств;
>
> г) использование информационно-коммуникационных технологий в преступных целях, в том числе для совершения преступлений в сфере компьютерной информации, а также для совершения различных видов мошенничества;
>
> д) использование информационно-коммуникационных технологий для проведения компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру;
>
> е) использование отдельными государствами технологического доминирования в глобальном информационном пространстве для монополизации рынка информационно-коммуникационных технологий, ограничения доступа других государств к передовым информационно-коммуникационным технологиям, а также для усиления их технологической зависимости от доминирующих в сфере информатизации государств и информационного неравенства.

В настоящее время США и их сателлитами против России развернута тотальная гибридная война. Это подтверждается, в частности, опубликованным 25 ноября 2020 года докладом «НАТО-2030»[14], смысл которого – усиление гибридного воздействия на Россию и ее союзников: политико-дипломатического, экономического, военного и информационного характера. При этом ключевую роль в информационно-психологическом манипулировании массовым сознанием россиян играют центры НАТО в Риге, Таллине, Хельсинки.

Развитие когнитивной и ментальной войны в ИКТ-среде повышает риск возникновения конфликтов, способных нарушить международный мир.

Ментальная война – война, направленная на изменение мировоззрения не только населения противника, но и в собственных странах, в странах союзников и партнеров, носящая «поколенческий» масштаб, главная угроза которой заключается в том, что ее последствия сказываются не сразу, а через поколения[15].

14 NATO-2030: Unaited for a New Era. 25 november 2020. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf

15 Ильницкий Андрей. Ментальная война за будущее России. URL: https://zvezdaweekly.ru/news/20214211636-jxgHZ.html

В отличие от кибервойн и прямых информационных операций, ментальная война направлена и реализуется с учетом фактически формирующегося мира «постправды», когда людей «отучают» от критического мышления, от стремления к истине.

Сегодня уже активно ведется манипулирование общественным сознанием и на уровне смысла, и на уровне эмоций, и на уровне подсознания.

В этом контексте представляется актуальным проанализировать документы, касающиеся информационной работы Великобритании на территории бывшего СССР. Данный архив[16], предположительно взломанный хакерской группировкой Anonymous, содержит бумаги с отсылками на внутренние документы внешнеполитического ведомства Великобритании, касающиеся его деятельности в Европе и Азии, при этом часть из них имеет прямое отношение к Украине и России.

Так, в документах отмечается, что британский МИД выпустил секретный формуляр, в котором говорится о запуске программы по противодействию информационного влияния России в странах Балтии, Белоруссии, Украины, Грузии и др.

Цель данной программы – ослабить влияние РФ на ее ближайших соседей, а ее макроцель – снизить уровень доверия населения к руководству России.

Задача взаимодействия, коммуникации между этническими русскими и местными сообществами, а также обучение, вовлечение в различные проекты новых участников была возложена на Британский совет, деятельность которого прекращена в России в 2018 году.

МИД Британии сосредоточился на поддержке независимых СМИ на постсоветском пространстве, особенно русскоязычных изданий. Как следует из документов, с 2018 года в Лондоне были готовы дискредитировать любую информацию, распространяемую российскими государственными СМИ, если она не соответствовала британским интересам.

Антироссийские публикации в СМИ сегодня – лишь часть той масштабной информационной операции, реализуемой Великобританией на всем постсоветском пространстве.

На реализацию плана информационной экспансии и связанные с ним гранты с марта 2019 года по март 2021 года Великобританией потрачено порядка £9 млн.

Примечательно, что с начала военной операции России на Украине тема информационного противостояния получила новое развитие: ключевым элементом информации становится именно ее «антироссийскость», вопрос подлинности или ложности оказывается вторичным.

Всего, по данным Лиги безопасного Интернета, с 24 февраля 2022 года в сети Интернет появилось порядка 6,5 млн фейковых сообщений о проведении специальной военной операции на Украине, а также о России. Сумма расходов информационной атаки на РФ достигла $1,5 млрд[17]. Ежедневно на кампанию тратится

16 Ослабить влияние России»: как Британия готовила Украину к информационной войне. URL: https://russian.rt.com/world/article/988503-britaniya-ukraina-finansirovanie-utechka-anonimus

17 Лига безопасного интернета выявила порядка 6,5 млн фейков о спецоперации на Украине. URL: https://tass.ru/obschestvo/14463169?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru

примерно $25 млн, что составляет около 2 млрд рублей в сутки. Сообщения распространяются с территории Украины, Польши, Латвии, США, Великобритании и других стран.

При этом, как отметил в своем выступлении на пленарной сессии «Международные отношения в условиях цифровизации общественной жизни» Международной научно-практической конференции «Цифровые международные отношения 2022» 14 апреля 2022 года министр иностранных дел Российской Федерации С.В. Лавров, Запад, присвоив себе титул «светоча демократии», грубейшим образом нарушает взятые на себя международные обязательства по обеспечению свободы выражения мнений, равного доступа к информации, перекрывая доступ к ней из соответствующих источников. Тем самым Запад демонстрирует тоталитарную нетерпимость к альтернативным точкам зрения[18].

Под «каток» западных репрессий попадают как отдельные пользователи социальных сетей, так и крупные СМИ со всей создававшейся годами инфраструктурой распространения новостей и оценок. Под действие нелегитимных санкций подводят руководителей отечественных медиаоператоров и рядовых сотрудников. Глобальные западные, в первую очередь американские, интернет-платформы веерно блокируют по всему миру российский информационный ресурс. Делают это демонстративно, не стесняясь.

Так, видеохостинг YouTube, принадлежащий американской ИТ-компании Google, ограничил доступ к брифингу официального представителя МИД России М.В. Захаровой 17 марта с.г.[19] М. Захарова назвала случившееся очередным актом цензуры в отношении российских ресурсов, а также предположила, что блокировка может быть связана с данными о биолабораториях на Украине, о которых шла речь на брифинге и которые скрывают на Западе. Необоснованные рестрикции накладываются также на публикации МИД России и загранучреждений в сети «Твиттер» только за то, что в этих источниках публикуются правдивые сведения, подкрепленные фактами.

Блокировке без возможности восстановления подвергся и канал Государственной Думы Федерального Собрания Российской Федерации «Дума ТВ», на который были подписаны более 145 тыс. человек, а число просмотров видеоконтента превышало 100 млн[20].

Под ограничениями видеохостинга YouTube находятся порядка 36 аккаунтов, в числе которых RT, «Россия 24», Sputnik, «Звезда», РБК, НТВ и др.

Роскомнадзор назвал Youtube одной из ключевых площадок для распространения «лживого контента» о специальной военной операции России на Украине. А ограничительные меры, введенные администрацией видеохостинга YouTube в от-

18 Выступление Министра иностранных дел Российской Федерации С.В. Лаврова на пленарной сессии «Международные отношения в условиях цифровизации общественной жизни» международной научно-практической конференции «Цифровые международные отношения 2022», Москва, 14 апреля 2022 года. URL: https://www.mid.ru/ru/press_service/video/view/1809294/

19 В Google назвали причину блокировки записи брифинга Захаровой на YouTube. URL: https://www.m24.ru/news/politika/07042022/448857

20 Google заблокировал YouTube-канал «Дума ТВ». URL: https://dumatv.ru/news/google-zablokiroval-youtube-kanal--duma-tv

ношении российских СМИ, в корне нарушают ключевые принципы свободного распространения информации и беспрепятственного доступа к ней[21].

Одновременно практически ежедневно серьезным кибератакам с применением новейших информационных технологий подвергаются российские государственные учреждения, СМИ, объекты критической информационной инфраструктуры, системы жизнеобеспечения. Все это – часть скоординированной информационной агрессии против России, которая требует особого внимания к задачам защиты информационных ресурсов органов государственной власти.

В этой связи Россия предпринимает конкретные законодательные и практические шаги по дальнейшему укреплению технологического цифрового суверенитета страны. 25 апреля 2022 года глава Комитета Совета Федерации Федерального Собрания Российской Федерации по обороне и безопасности Виктор Бондарев провел круглый стол на тему: «Ментальные войны: проблемы и способы противодействия»[22]. Участники круглого стола констатировали, что атаки Запада на нашу страну носят характер постоянно усиливающегося гибридного воздействия, антироссийские информационно-пропагандистские кампании осуществляют дискредитацию руководства государства и проводимой им внутренней и внешней политики, формируют предпосылки для дестабилизации общественно-политической обстановки, в экстремистскую и протестную деятельность вовлекают молодежь, в том числе несовершеннолетних детей.

Складывающаяся обстановка требует активности всех институтов гражданского общества и органов власти, подчеркнули участники круглого стола. Отмечено, что базовым принципом стратегии обеспечения безопасности в ментальной сфере следует считать действия на опережение, в рамках единой системы прогнозирования и предупреждения гибридных угроз и вызовов в информационной сфере.

Россия неизменно выступает за скорейшую разработку универсальных норм и принципов ответственного поведения государств в информационном пространстве, за разработку под эгидой ООН Конвенции по противодействию преступлениям в сфере использования информационно-коммуникационных технологий, а также за интернационализацию управления сетью Интернет.

Информационный суверенитет государства: критерии и показатели (Соболев Е.И.)

Идея государственного суверенитета существует уже довольно давно. Без суверенитета сложно представить себе современное государство, успешно и активно действующее на мировой арене. Его основную суть можно свести к независимости и верховенстве власти в принятии и исполнении решений как внутри страны, так и за ее пределами. Понятие информационного суверенитета долго отсутствовало

21 Роскомнадзор требует незамедлительно снять ограничения с youtube-каналов российских государственных СМИ. URL: https://rkn.gov.ru/news/rsoc/news74284.htm

22 В Комитете Совета Федерации по обороне и безопасности обсудили способы противодействия ментальной войне. URL: http://council.gov.ru/events/main_themes/135291/

в мировой юридической практике. Первые шаги к выработке определения информационного суверенитета были предприняты лишь в последние десятилетия XX века. Это было связано в первую очередь с активным развитием и внедрением в жизни людей технологических инноваций, среди которых на замену традиционных и простых в использовании источников информации пришли более сложные – средства сотовой и спутниковой связи. Венцом развития этих технологий стала всемирная «паутина» – Интернет. Интернет предоставил человечеству новую площадку для взаимодействия – виртуальное пространство, в котором люди могли бы свободно общаться друг с другом независимо от расстояния, обмениваться и получать нужную им информацию. Юридические механизмы по регулированию деятельности участников этого пространства, равно как и находящиеся в нем объемы данных, выработать было довольно сложно. Тем не менее в этой области велась активная работа не только по созданию законодательных инициатив, но и по осмыслению государственного присутствия в виртуальном пространстве. А. Ефремов выделяет четыре основных этапа в формировании концепции информационного суверенитета (2).

Первый этап пришелся на 1980-е годы. В это время Интернет еще находился на стадии разработки и тестирования, поэтому исследования этих лет его не затронули. В связи с тем, что обмен информацией благодаря использованию спутников, телевидения и радио приобрел трансграничный характер, исследователями было решено рассмотреть соотношение национального суверенитета и права на свободу информации (8). После сравнения Всеобщей декларации прав человека (1948), Международного пакта о гражданских и политических правах (1966) с государственными ограничениями потоков информации ими был сделан вывод о том, что в толковании аспектов государственного суверенитета у развитых и развивающихся стран есть различия (2, с. 205). Так, для первой категории стран неограниченный обмен информацией является компонентом, укрепляющим их суверенитет, в то время как для второй свобода в распространении данных представляет опасность для суверенитета (8, p. 267). Стоит отметить, что это различие прослеживается и в наши дни.

Второй этап связан с рассмотрением непосредственно самого Интернета в контексте угрозы суверенитету государства. Его бурное развитие в 1990-е годы позволило более детально проанализировать взаимосвязь этой международной сети и государства и опубликовать ряд работ по данной теме. Например, один из китайских исследователей В. Гонг выдвинул идею о двух компонентах информационного суверенитета: внешнем и внутреннем. Внешний включает в себя юридическое равенство государств и их независимость в создании и распространении информации. Внутренний отображает правовое верховенство в обеспечении информационного порядка и осуществлении информационной политики (9). Говорится о продолжении тенденции развивающихся государств охранять собственный суверенитет, а развитых – призывать к свободному обмену данными. Стоит также обратить внимание на взгляды американских исследователей касательно информационного суверенитета. В их работах не делается акцент на степени развитости государства, так как за основу берется уверенность в том, что подавляющая часть стран предпринимает активные

действия по защите и укреплению своего суверенитета. Более того, в их работах отмечается, что большинство граждан поддерживают данные инициативы (2).

В третий этап, который продолжается и в наше время, исследователи выделяют концепцию суверенитета данных. Согласно этой концепции, в ряде стран (Россия, Франция, Германия, Австралия) были приняты законодательные акты, которые обязывали хранить персональные данные граждан на серверах той страны, к которой они принадлежат (10). Отсюда можно сделать вывод о том, что взаимодействие с объемами данных в этих государствах стало подчинено юрисдикции государства, в котором находились эти данные. Современные исследователи считают желание государств по развитию суверенитета данных вполне объяснимым и разумным, поскольку оно направлено главным образом на сохранение конфиденциальности информации, защиту и охрану интересов государства в области обеспечения целостности и доступности данных. Стоит отметить, что развитие этой концепции получило свое распространение не только среди западных государств, но и в научных трудах Китая, Южной Кореи, Индонезии. Не осталась без внимания и работа в области создания технологии больших данных (big data), которая с начала 2010-х годов стала связываться с концепцией суверенитета данных.

Четвертый этап развития концепции информационного суверенитета находится на стадии исследования и пока не изучен научным миром достаточно глубоко. В первую очередь он связан не столько с регулированием потоков информации, сколько с контролем над информационно-коммуникационной инфраструктурой (ИКТ-инфраструктурой). Он нашел свое отражение в ряде международных исследований. Например, согласно докладу группы правительственных экспертов 68-й сессии Генеральной Ассамблеи ООН, которая была проведена в 2013 году, на любую деятельность государства в области ИКТ и ИКТ-инфраструктуры, включая их использование, распространяются государственный суверенитет и исходящие из него принципы и международные нормы[23]. В дополнение к этому докладу двумя годами позже, на 70-й сессии Генеральной Ассамблеи ООН, был выработан и предложен подход, который позволил бы на деле применять нормы международного права в вопросах использования информационно-коммуникационных технологий государством. В этом подходе было обозначено, что государство обладает юрисдикцией над той ИКТ-инфраструктурой, которая находится на его территории. Помимо этого, были подчеркнуты принципы невмешательства в дела других государств, суверенного равенства, государственного суверенитета и разрешения спорных вопросов при помощи мирных средств[24].

В работах исследователей используются различные термины информационного суверенитета: цифровой суверенитет, киберсуверенитет, суверенитет в информа-

23 Доклад группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. A/68/98. URL: // http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=R.

24 Доклад группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. A/70/174. URL: // https://documents-ddsny.un.org/doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf?OpenElement.

ционной сфере, Интернет суверенитета. Аналогично этому приводятся и разные его критерии. Например, Е. Зорина выделяет два аспекта информационного суверенитета – идеологический и технический. Идеологический аспект включает в себя разработанную национальную идею либо же национальную идеологию, достижение массовой культуры высокого уровня, наличие активной пропаганды и проработанного в информационной сфере законодательства. Технический аспект включает в себя существование национального программного обеспечения, собственных социальных сетей, поисковиков, национальную электронную платежную систему (4). В. Бухарин в своей работе дополняет технический аспект наличием микроэлектроники, сетевого оборудования, национальным сегментом в сети Интернет, криптографическими алгоритмами и протоколами, функционирующей навигационной системой и собственными средствами защиты (1).

В работе Е. Зориной можно выделить следующие критерии информационного суверенитета (3). Первый – высокая оснащенность государства компьютерными и коммуникационными системами. Именно они отвечают за создание и распространение информации. Без должного уровня обеспечения данными системами потенциал суверенитета в сетевом пространстве сильно ограничен. Следующий критерий – наличие средств для защиты указанных выше систем: антивирусов, файрволлов и пр. Их отсутствие угрожает утечкой или кражей персональных данных пользователей и информации, составляющей государственную тайну. Отметим, что инструменты защиты данных должны быть созданы государством, иначе возникает риск зависимости от внешних поставщиков. Существование национальной интернет-инфраструктуры является важным показателем наличия у государства устойчивого информационного суверенитета, поскольку собственные поисковые системы и социальные сети открывают широкое поле для государственного контроля за процессами в киберпространстве. Одним из критериев также считается национальная платежная система, которая позволяет избежать рисков внешнего политического давления. В России такая платежная система уже существует и продолжает развиваться. Также государство должно обладать развитым механизмом пропаганды и развитой сетью СМИ, причем не только внутри страны, но и обладающей каналами внешней коммуникации для вещания в иностранных государствах. Основная цель этих каналов заключается в предоставлении собственной и зарубежной аудитории информации, отвечающей национальным интересам. Роль СМИ в вопросах формирования повестки дня – как через привычные формы вещания, так и посредством использования Интернета – сложно переоценить. Недаром СМИ многие называют четвертой властью. Стоит отметить, что, несмотря на нейтральную подачу основных новостей, они часто могут дать им собственную оценку, а про некоторые значительные происшествия, обладающие потенциально негативным эффектом на официальную линию, – умолчать. Поэтому именно СМИ находятся в авангарде пропагандистской политики (как наиболее зарекомендовавший себя политический инструмент).

Следующим критерием является создание и распространение продукции, имеющей отличительные культурные признаки государства. Например, ими могут об-

ладать продукты кинематографа или музыкальной индустрии. Популяризация этих продуктов может способствовать формированию положительного образа среди граждан иностранных государств. Сюда же можно отнести создание имиджа государства и его продвижение посредством привлечения массовой культуры и Интернета. Удачно сформированный имидж аналогично выпуску брендовой продукции позволяет развивать положительное впечатление у иностранных государств. Хорошими примерами служат зимние Олимпийские игры в Сочи в 2014 году или чемпионат мира по футболу в 2018 году. Повышение привлекательности страны не только отвечает интересам информационной безопасности, но и позволяет привлекать дополнительный объем инвестиций, завести новых партнеров. В дипломатии формирование положительного образа государства вышеуказанными методами называется «мягкой силой». Еще одним критерием информационного суверенитета можно назвать активное использование интернет-пространства для распространения в нем отвечающих интересам государства идей. Они могут быть заложены в видеороликах и других публикациях. Их направленность заключается в дискредитации негативной информации и воздействии на массовое сознание людей. В качестве примера Е. Зорина приводит «Википедию», один из самых популярных источников информации в Интернете (3). Говоря о критериях, нельзя забывать о вопросах институционализации. Информационное поле требует от государства создания институтов, наделенных закрепленными за ними обязанностями, например министерств и ведомств. Для институционализации необходима правовая база – это следующий критерий. Юридические механизмы воздействия обеспечивают не только охранительные функции, но и позволяют государству предпринимать адекватные действия по обеспечению целостности своего информационного суверенитета.

Анализ опыта обеспечения информационного суверенитета в Китае, США и России показывает наличие ряда отличительных черт. КНР обладает рядом специфичных признаков в отношении информационно-коммуникационных технологий. На сегодняшний день Китай является одним из лидеров в области использования киберпространства. Характерной особенностью китайского развития сетевого сегмента является активное заимствование иностранных технологий. Лишь в последнее десятилетие КНР перешла к разработке собственной продукции. Тем не менее тенденция по активному привлечению зарубежных инноваций сохраняется и по сей день. Интернет для китайского правительства – это не только часть суверенного пространства, но и средство для осуществления почти тотального контроля над собственными гражданами, активного культивирования онлайн-этики в духе конфуцианства и китайской модели социализма. Национальная стратегия безопасности в киберпространстве, утвержденная в 2017 году[25], выделяет как значительные возможности, так и угрозы, которые предоставляет эволюция информационных технологий. Согласно ей, безопасность является приоритетом в любых формах развития киберпространства: «безопасность является необходимым условием развития, и любое развитие,

25 Национальная стратегия безопасности в киберпространстве. URL: http://www.cac.gov.cn/2016-12/27/c_1120195926.htm.

которое происходит в ущерб безопасности, является неустойчивым. Развитие – это основа безопасности, а неспособность развиваться – это величайшая опасность». Вопросами обеспечения безопасности Китай занимается основательно с начала 2000-х годов. Потрясшие мир террористические акты 11 сентября 2001 года заставили многие страны, включая КНР, пересмотреть и ужесточить свою политику в информационной среде. Интернет в Китае находится под бдительным надзором соответствующих структур. Существует даже интернет-полиция, отслеживающая поступающий поток данных на сайты, форумы и социальные сети (5). Одним из самых известных китайских изобретений по охране информационного суверенитета является так называемый «Золотой Щит», известный больше на Западе как «Великий китайский файрволл». Данный проект, действующий с 2004 года, отвечает за фильтрацию контента в Интернете и блокировку опасных сайтов. Он состоит из трех технологических компонентов. Первый – технология накопления статистической информации, проверки и фильтрации сетевых пакетов по их содержимому. Второй – это его модернизация в виде слияния механизма фильтрации и прокси-сервера. Третий компонент – усовершенствованный механизм фильтрации данных, отличающийся более широким спектром анализа информации. Проект «Золотой Щит» успешно ведет борьбу с террористами, оперативно обнаруживая их ячейки в сети. О его эффективности говорит число террористических актов в Китае и соседних азиатских государствах (7).

Китайский Интернет блокирует иностранные сайты и социальные сети, такие как Wikipedia, Facebook, Twitter. Западные СМИ тоже недоступны для китайских пользователей. Более того, с 2017 года анонимность в Интернете была запрещена. Пользование его услугами становилось доступным только после регистрации с указанием своего реального имени и контактной информации. Анонимное комментирование, обсуждение или создание интернет-постов теперь стало невозможным. Более того, технологии для защиты информационного суверенитета активно используются для контроля за общественным поведением. В 2020 году на всей территории Китая была введена ранее экспериментальная система социальных кредитов, поощряющая или наказывающая граждан в зависимости от характера их активности как в жизни, так и в Интернете. Для ее исполнения по всей стране планируется установить несколько сотен миллионов камер нового поколения. В зависимости от высокого или низкого количества социальных кредитов человек будет получать льготы при использовании транспорта, покупок, путешествий по стране либо же ограничения в пользовании Интернетом, качественной медицины, приобретении дорогой недвижимости соответственно. Те, кто растеряет значительное число своих кредитов, рискует вовсе оказаться в изоляции, поскольку за общение с такими маргинализированными новой социальной системой лицами поощрения со стороны правительства явно не последует. Сами китайцы относятся к введению новой системы спокойно, так как они достаточно дисциплинированны в вопросах контроля за своей личной жизнью. Стоит отметить, что Китай использует не только средства защиты своего информационного суверенитета, но и пытается действовать на опережение за счет активных наступательных действий по предупреждению потенциальных угроз. В стране существуют

собственная армия интернет-троллей, состоящих из финансируемых правительством блогеров (всего их численность составляет от 300 тыс. до 2 млн человек), и отдельно от них – кибервойска. Первые отвечают за поддержание провластной линии в спорных вопросах в Интернете в непростые для страны времена, в периоды различных кризисов и потрясений. Интернет-тролли оставляют множество комментариев в поддержку руководящей партии, умело меняют тему обсуждения и никогда не атакуют оппонента напрямую. Более серьезно действуют в интернет-пространстве китайские кибервойска. Их деятельность часто освещается иностранными СМИ. Основной род деятельности этого вида вооруженных сил – кибершпионаж и хакерские атаки. Таким образом, Китай, несмотря на технологическое отставание от ведущих стран мира, обеспечил свой информационный суверенитет очень серьезной защитой, основанной на послушном обществе, находящемся под надзором государства, тотальной фильтрации информации в Интернете и упреждающих действиях силовых структур. Однако авторитарные методы этой страны подойдут далеко не для всех.

Соединенные Штаты, будучи одним из лидеров в технологиях и глобальном контроле за информационными потоками, на протяжении длительного времени занимались разработкой концепций по обеспечению собственного информационного суверенитета. Сегодня основным документом, отвечающим за практическое применение мер в его отношении, является Стратегия национальной кибербезопасности[26], принятая президентом Дональдом Трампом в 2018 году, и Стратегия Министерства обороны США в киберпространстве[27] того же года. Во главу угла эти документы ставят защиту американских демократических ценностей, поэтому отличительной особенностью информационного суверенитета США (согласно официальной правительственной линии) является открытость и доступность в получении и обмене информацией. Правительство США гарантирует свободный доступ к сети Интернет, другим каналам социальной коммуникации. Именно неограниченное движение данных, по мнению авторов стратегии, обеспечивает безопасность американского общества, его стабильное развитие, финансовое благополучие и технологическое превосходство. Основная роль по обеспечению информационного суверенитета возложена на федеральное правительство. В стратегии описаны перспективы дальнейшей централизации управления и контроля безопасности гражданского сектора в киберпространстве путем увеличения прозрачности в межведомственных делах, ликвидации дублирующих действий, осложняющих процедуру исполнения поставленных перед правительством задач в информационной среде. Стратегия наделяет равным уровнем ответственности правительство и частный сектор в вопросах обеспечения безопасности критически уязвимой инфраструктуры. Поставщики ИКТ играют важную роль в народном хозяйстве США, поэтому для поддержания их высокой производительности федеральное правительство обязывается активно сотрудничать с ними, совмест-

26 National Cyber Strategy of the United States of America. URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

27 Department of Defense Cyber Strategy – 2018. URL: https://www.cybercom.mil/About/Mission-and-Vision/.

но противостоя хакерским атакам. Соединенные Штаты активно ведут работу по совершенствованию своего законодательства с целью наделения правоохранительных органов дополнительными возможностями для отслеживания неправомерных действий в Интернете. К ним относятся как преступная активность с использованием компьютерных систем внутри страны, так и хакерские атаки извне в виде взлома, кражи данных, организации утечек, атак на информационную инфраструктуру. Соединенные Штаты открыты к сотрудничеству для иностранных государств в вопросах обеспечения безопасности в киберпространстве. Путем кооперации, совместных проектов со своими партнерами, включая как целые страны, так и представителей отдельных отраслевых групп (промышленников, ученых), гражданского общества, Америка не только может укрепить свой цифровой суверенитет, но и распространить свое влияние, которое бы обеспечило США лидирующее место в области развития информационно-коммуникационных технологий. Правительство активно содействует развитию творческого потенциала в информационной сфере, занимаясь финансовой поддержкой таких проектов, как искусственный интеллект и квантовая информатика. Для повышения эффективности цифрового суверенитета планируется обновить существующую ИКТ-инфраструктуру, снабдив ее технологиями следующего поколения. Действия США по обеспечению информационного суверенитета должны совпадать с содержанием всех международных норм. Правительство будет поощрять соблюдение данных норм и на собственном примере доказывать необходимость их соблюдения. В случае нарушения этих норм, а также угрозы цифровому суверенитету Соединенные Штаты вправе использовать все имеющиеся у них инструменты для воздействия на тех, чья деятельность в киберпространстве является опасной: дипломатические, информационные, военные (кинетические и цифровые), финансовые, разведывательные, возможности правоохранительных органов. Таким образом, защита собственного информационного суверенитета в США тесно переплетена с принципами сдерживания потенциальных противников в информационном поле на глобальном уровне. Большую роль в достижении этих задач играет американская разведка, которая в онлайн-режиме выявляет источники информационных кампаний, дезинформации, хакерских атак и передает эти сведения федеральному правительству. Самым громким примером по действиям США в информационном пространстве в последнее время стала кампания по обвинению России во вмешательстве в американские выборы в 2016 году как прямое посягательство на суверенитет страны в киберпространстве. Таким образом, Соединенные Штаты создали одну из самых сложных систем по обеспечению своего информационного суверенитета. Серьезная технологическая база, мощный разведывательный аппарат и геополитическое положение лидера западного мира позволяет американскому правительству достаточно эффективно реализовывать поставленные в доктринальных документах задачи по защите государственных интересов в киберпространстве, навязывать свои правила игры более слабым участникам и расширять свое влияние. Акцент осуществляемых США действий в Интернете делается на тесном сотрудничестве со своими партнерами, открытости и соблюдении прав человека. Однако после событий 11 сен-

тября американское правительство значительно расширило полномочия силовых структур в вопросах контроля за информацией, что стало равнозначно контролю за действиями своих граждан. На этой почве периодически случаются скандалы, самые громкие из которых связаны с признаниями сбежавшего сотрудника американских спецслужб Эдварда Сноудена и австралийского журналиста Джулиана Ассанжа. Данные, которые были предоставлены ими широкой общественности, сильно ударили по имиджу США и пошатнули позиции этой страны как лидера свободного мира.

Российская Федерация активно ведет разработку концепции государственного суверенитета в цифровом пространстве. Тем не менее на сегодняшний день такой детализированной стратегии, какая имеется у США или Китая, у России нет. Однако говорить о том, что информационному суверенитету не уделяется должного внимания, нельзя. Наоборот, совершенствование безопасности в этой области является одним из приоритетов нашей страны. В 2016 году была принята Доктрина информационной безопасности Российской Федерации[28], в которой подробно излагаются меры по защите своего информационного суверенитета, а также по отстаиванию национальных интересов России в информационной сфере. К национальным интересам отнесены действия по охране конституционных прав и свобод граждан в области получения и использования информации; по обеспечению бесперебойной работы информационно-коммуникационной инфраструктуры, где приоритет отдается объектам критической инфраструктуры; по развитию наукоемких отраслей информационных технологий и электронной промышленности, совершенствованию текущей деятельности; по донесению до внутренней и внешней аудитории актуальной и достоверной информации о проводимой Россией политике и официальной позиции страны касательно значимых вопросов; по применению ИКТ-технологий для обеспечения национальной безопасности в области культуры; по сотрудничеству в области создания системы международной цифровой безопасности, укреплению равноправного стратегического партнерства в информационной сфере. Указанные меры нацелены на создание устойчивой и защищенной от любых форм воздействия информационной инфраструктуры, стабильное развитие страны, защиту прав и свобод граждан. Защита информационного суверенитета достигается через обеспечение информационной безопасности в следующих областях:

- в области обороны посредством предотвращения конфликтов с использованием цифровых технологий, обнаружения информационных угроз;
- в области государственной и общественной безопасности посредством борьбы с пропагандой экстремизма, призывов к подрыву суверенитета и изменению конституционного строя с использованием информационных технологий; противодействия деятельности иностранных спецслужб на территории страны; повышения защищенности критической информационной инфраструктуры, ее функционирования; совершенствования механизмов защиты информации и увеличения эффективности реализации информационной политики;

28 Доктрина информационной безопасности Российской Федерации. URL: http://www.scrf.gov.ru/documents/6/5.html.

- в области экономики путем ликвидации технологической зависимости отечественной промышленности от иностранных государств; повышения конкурентоспособности российской информационной сферы услуг; развития собственной электронной базы;
- в области науки, технологий и образования посредством развития научных исследований в создании перспективных информационных технологий; формирования опытных кадров в области цифровых технологий;
- в области стратегической стабильности и партнерства посредством проведения независимой политики, отвечающей реализации национальных интересов; содействие в формировании международно-правовых механизмов в области информационных технологий и системы международной информационной безопасности; освещение позиции России по вопросам цифровой безопасности; развития национального сегмента Интернета.

В доктрине указаны уязвимые стороны информационного суверенитета России. К ним относятся: слабая конкурентоспособность отечественных цифровых технологий, зависимость государства от иностранных инноваций, особенно электронно-вычислительной базы, низкий уровень образованности граждан в вопросах личной информационной безопасности, слабые темпы оснащения производства российскими информационно-технологическими компонентами, серьезная борьба лидирующих в информационной сфере государств за сохранение их доминирующего положения в мире. В своей статье, где дается оценка государственной политики в области информационной безопасности, Д. Литвинов дополняет список слабых сторон введенными Западом санкциями, отсутствием упорядоченной структуры в нормативно-правовой базе, нехваткой бюджетных средств для реализации заявленных действий (6). Доктрина цифровой безопасности является составляющей Стратегии национальной безопасности Российской Федерации, принятой в 2021 году. В ней кратко изложены вышеперечисленные меры по достижению безопасной информационной среды. Таким образом, можно сделать вывод, что Россия считает защиту информационного суверенитета одним из компонентов обеспечения национальной безопасности. Несмотря на имеющийся на сегодняшний день ряд проблем в практической реализации закрепленных в доктринальных документах мер по государственной охране своего суверенитета во всех областях, можно считать, что развитием информационного суверенитета в нашей стране активно занимаются.

Обеспечение информационного суверенитета государств (Седунов Д.И.)

Потребность в обеспечении информационного суверенитета особо явно выразилась в событиях, связанных со спецоперацией России на Украине. Для сравнения западного и российского подходов к обеспечению информационного суверенитета мы предлагаем три основных критерия по применяемым технологиям: скорость воз-

действия (как быстро использованная технология), стоимость воздействия (ресурсы, необходимые для применения технологии), долгосрочность влияния (пролонгированность результата применяемой технологии).

В «западном» подходе обеспечения информационного суверенитета на примере текущего конфликта «коллективный Запад против России» возможно выделить три ключевые технологии обеспечения информационного суверенитета:

1) Жесткая цензура информации, блокирование любой информации, отличной от государственной информационной политики. Технологически это проявляется в запрете официальных СМИ, принадлежащих противоборствующей стороне (были закрыты RT, «Спутник», прочие каналы РФ); в жесткой цензуре социальных сетей (удаление и блокировка любой информации со стороны РФ из информационного поля в FB, YouTube, Twitter, Instagram); запрет на распространение в СМИ официальной информации со стороны РФ (блокировка интервью, трансляций, предоставление только выгодных для западных политиков трактовок в отрыве от контекста).

2) Создание заведомо ложного контента, направленного на дискредитацию России и ее союзников. Используются технологии фейков, публикаций сфабрикованной ложной аналитики и иной информации; активные провокации для формирования ложных сюжетов и инфоповодов в СМИ; ссылка на недостоверные и непроверенные источники, но содержащие информацию, необходимую для западных политиков, чтобы оправдать свои действия перед своими гражданами.

3) Эмоциональная подача информации: акцент на аффективной стороне вопроса, а не на рациональной, игнорирование логики и фактов.

Российский подход к обеспечению информационного суверенитета отличается от западного:

1. Детальное разоблачение и разбор фейков – как со стороны официальных органов государственной власти, так и со стороны патриотической блогосферы. В частности, речь идет о запуске каналов МИД РФ, Минобороны и других в «Телеграмм»; о максимальной подаче достоверной информации в виде сюжетов с мест событий и интервью с очевидцами, публикаций официальных документов зарубежных стран, подтверждающих враждебные намерения в отношении России и населения ДНР и ЛНР.

2. Россия блокирует враждебные действия, ограничивает работу антироссийских агрессивных СМИ и новых медиа. Мы видим блокировку социальных сетей, открыто проводящих агрессивную информационную политику в FB и Instagram; симметричные ответы на запрет российских СМИ за рубежом; расширение числа НКО и СМИ в группе иноагентов; принятие нормативно правовых актов, направленных на обеспечение информационного суверенитета России.

3. Активизация патриотически настроенной блогосферы.

Выводы

Сравнивая российский и западный подходы по ранее обозначенным критериям, можно сделать следующие выводы. Жесткая цензура информации работает очень быстро, до населения доводится только подготовленная точка зрения, и полностью исключаются альтернативные. При этом поддержание и обслуживание необходимой инфраструктуры требует существенных финансовых затрат. Нарушение информационной блокады в долгосрочном периоде приводит к нарушению информационного суверенитета (пример из истории – «железный занавес» СССР). Совместное использование технологий ложной информации с «эмоциональной мобилизацией» быстро приносит результат, но требует высоких финансовых затрат для подготовки и подачи информации. Аналогично, как и с жесткой цензурой информации, в долгосрочном периоде может приводить к нарушению собственного информационного суверенитета. Спецификой технологий, используемых в российском подходе, является работа на долгосрочный период при минимальных вложениях финансовых ресурсов. Данный подход позволяет в условиях финансовых ограничений выстраивать долгосрочную информационную политику и укреплять информационный суверенитет.

Обсуждение

Изучив подходы Китая, США и России к вопросу организации и защиты информационного суверенитета, можно определить актуальные на сегодняшний день тенденции. В первую очередь разработка различными странами комплекса мер по формированию устойчивой и безопасной информационной среды вызвана возросшей ролью информационно-коммуникационных технологий во всех сферах жизни людей одновременно. Если тридцать лет назад о существовании такой разветвленной, многофункциональной и высокотехнологичной системы обмена данными, как Интернет, задумывался только узкий круг специалистов, то сегодня использование Интернета стало для нас неотъемлемой частью ежедневной рутины. Его возможности в современном мире явно превосходят все ожидания тех, кто занимался разработкой этой инновации на начальных этапах. Повсеместная цифровизация экономических, социальных, политических, культурных процессов подразумевает наличие правовых и технологических механизмов их осуществления, а также инструментов по защите преобразованной информации. Во-вторых, начавшаяся два года назад пандемия коронавируса в разы ускорила внедрение информационных технологий в жизни людей, особенно это коснулось организации рабочих условий. Усиление информационного компонента в государстве потребовало дополнительных расходов и дополнительных решений по формированию его устойчивой структуры. Сегодня, когда смертность от новых штаммов вируса упала, многие эксперты высказали мнение, что пандемия скоро кончится. Однако конец эпидемии вряд ли повлияет на желание мировой элиты лишить себя всех преимуществ, созданных информационно-коммуникационными технологиями за последние годы, так как они ста-

 ISSN 2782-3067 (Print)

ли хорошей площадкой для дополнительного надзора за деятельностью собственных граждан. В-третьих, возросли случаи кибершпионажа, хакерских атак и использования возможностей социальных сетей по управлению социальным сознанием. Странам со слабо развитой ИКТ-инфраструктурой почти нечего противопоставить технологически развитым конкурентам.

Первое и, возможно, ключевое уязвимое место цифрового суверенитета России находится в технологической слабости перед внешними опасностями. В случае спланированной масштабной хакерской атаки объекты информационной инфраструктуры могут быть выведены из строя. Осложняет положение сильная зависимость государства от импорта высокотехнологичной продукции. В случае остановки этих каналов поставок не только дальнейшее совершенствование цифрового суверенитета, но и технологическое развитие страны в целом может существенно замедлиться и вызвать ряд проблем уже иного содержания. Потенциал производства отечественных аналогов западных компонентов электроники находится на весьма низком уровне. Не секрет, что в третьем десятилетии XXI века наиболее развитые страны активно ведут кибервойны по всему миру. Целями таких атак являются стратегически важные, уязвимые в цифровом пространстве объекты. Благодаря разработанным вредоносным программам, проникающим в устройства этих объектов, нарушается или вовсе останавливается их функционирование. Последствия могут затронуть сразу экономическую, политическую, энергетическую, оборонную сферы. Еще одной угрозой информационному суверенитету нашей страны можно считать информационную войну, которая на сегодняшний день активно ведется некоторыми иностранными государствами. Ее суть заключается в подтасовке фактов, манипулировании данными и формировании искаженной картины мира, где образ России выставляется в негативном ключе. Наглядным примером этой войны была пропаганда западных СМИ о скором начале крупномасштабной войны России против Украины. Назывались конкретные даты начала вторжения, однако в эти дни заявленного вторжения не произошло[29]. Несмотря на этот весомый просчет, информационная война все же приносит свои плоды в виде нестабильного рынка, роста антироссийских настроений в Европе и эскалации ситуации вокруг Украины. В качестве источника угрозы для информационного суверенитета стоит отметить и использование социальных сетей как платформу для организации противозаконной деятельности. Одним из примеров является использование мессенджера Telegram для координации протестных движений на территории Белоруссии летом-осенью 2020 года. Высокий уровень анонимности, предоставляемый этим мессенджером, позволяет не только скрыть свою личность, но и обеспечить относительную безопасность и конфиденциальность в передаче информации, что и было использовано организаторами протестов. Самым известным каналом в Telegram в период беспорядков был NEXTA[30]. Безусловно, даже хо-

29 Над Украиной безоблачное небо. Как Запад всю ночь ждал «вторжения» России. URL: https://www.gazeta.ru/army/2022/02/16/14541109.shtml.

30 Как четыре человека создали главный Telegram-канал белорусского протеста с аудиторией 2 млн подписчиков. URL: https://www.forbes.ru/tehnologii/407119-kak-chetyre-cheloveka-sozdali-glavnyy-telegram-kanal-belorusskogo-protesta-s.

рошую защиту Telegram можно обойти и определить реальных участников, но для этого требуются более высокие технологии и, главное, время. А в период политической нестабильности времени часто не хватает. Во время кризиса в Казахстане в январе этого года данный мессенджер тоже использовался, причем не только местными оппозиционными силами, но и зарубежными участниками, ведущими удаленный контроль за разгоравшимися беспорядками[31]. Проблема социальных сетей заключается не только в организации оппозиционных движений. Анонимностью также пользуются и террористические ячейки, торговцы запрещенными веществами; распространяется детская порнография и иной запрещенный контент[32]. Неконтролируемое обращение криптовалют является еще одной из угроз суверенитету России в киберпространстве. Одной из самых известных на сегодняшний день считается биткойн. Так как криптовалюта ничем не обеспечена, а значит, не способна управляться, то это создает определенный риск для экономики государства. Несмотря на снижение стоимости ключевых криптовалют, исходящая от них угроза никуда не исчезает, а их рынок требует оценки правового регулирования со стороны государства. Среди дополнительных угроз информационному суверенитету можно выделить мошенничество в Интернете, которое включает в себя разные по масштабу правонарушения и преступления. Киберпреступность продолжает развиваться, а убытки от нее расти.

Каждая из указанных выше угроз может быть либо решена, либо может быть снижен ее риск. Для этого было бы уместным принять следующие меры:

- значительно увеличить финансирование отечественной высокотехнологичной промышленности, а главное, поддержать российские исследования в области компьютерных технологий, чтобы свести зависимость от иностранной продукции к минимальным значениям; повысить защищенность объектов критической инфраструктуры;
- продолжать развитие отдельного направления в области кибербезопасности в Вооруженных Силах РФ, наращивать военный потенциал в области цифровых технологий, использовать опыт иностранных государств в аналогичных условиях и тем самым более успешно противостоять их атакам в киберпространстве;
- проводить активную политику в информационной сфере, направленную на борьбу с ложными сообщениями; формировать четко сформулированную официальную точку зрения по жизненно важным вопросам и своевременно доносить ее до широкой аудитории внутри страны и за ее пределами; опровергать провокационные заявления, взвешенно и аргументированно отстаивать свои интересы;
- внимательно относиться к публикациям в социальных сетях, которые могут угрожать информационному суверенитету; отслеживать в них противоправную и иную запрещенную законодательством деятельность;

31 По лекалам NEXTA: Кто стоит за телеграм-каналом из Киева, призывавшим к революции в Казахстане. URL: https://life-ru.turbopages.org/life.ru/s/p/1462931.

32 В России террористы активно используют Telegram для связи, заявили в ФСБ. URL: https://ria.ru/20170626/1497271423.html.

- обеспечить ясную и последовательную государственную политику в области оборота криптовалют;
- сформировать и приступить к реализации государственной политики в сфере просвещения населения по вопросам информационной безопасности, правилам безопасного взаимодействия граждан с цифровыми технологиями, умелого их использования (уделить особое внимание пожилым людям как группе, подверженной наибольшему риску интернет-мошенничества);
- усилить контроль за противоправной деятельностью в Интернете.

Выводы

Технологически-правовое осмысление концепции информационного суверенитета началось более 40 лет назад и продолжается по сей день. Ее развитие находится в тесной взаимосвязи с развитием технологий в целом – от сотовой и спутниковой связи до глобальной сети Интернет и технологии облачного хранения данных. Эта концепция затрагивает не только вопросы, связанные со всеми возможными видами информации, но и ее соотношение с международными нормами в области защиты прав человека, защиты и охраны государственного суверенитета, в вопросах использования информационно-коммуникационной инфраструктуры.

В XXI веке сложно представить себе страну, которая не позаботилась бы о своем информационном суверенитете и, в частности, о безопасности в киберпространстве. Несмотря на то, что на сегодняшний день информационному суверенитету пока еще не уделяется должного внимания ученых, участники научной дискуссии выражают уверенность, что в ближайшем будущем мы увидим новые, глубокие по содержанию исследования и научно аргументированные управленческие решения. Думается, что не обойдут стороной и морально-правовую сторону вопроса. Безусловно, суверенитет государства – неотъемлемая часть современного мира и залог безопасности общества. Однако в стремлении достичь этой безопасности важно не забывать про базовые права человека, закрепленные в десятках международных документов, и не пытаться обеспечить безопасность исключительно ради собственной односторонней выгоды.

Обобщая мнения участников дискуссии, сделаем ряд выводов:

- Концепция информационного суверенитета развивалась на протяжении сорока с лишним лет, преодолев четыре этапа своего становления – от технически-правового осмысления положения государства среди потоков данных до международных норм в области контроля за цифровой инфраструктурой.
- К критериям информационного суверенитета можно отнести наличие технологической базы и средств для ее защиты, существование национальной пла-

тежной системы, осуществление пропаганды и повышение имиджа страны в информационном пространстве, распространение в нем отвечающих интересам государства идей.

- Такие отличающиеся друг от друга страны, как Китай, США и Россия, предоставили для исследования различные подходы к организации своего информационного суверенитета. В Китае он достигается за счет тотального контроля за информацией, отсутствия полного доступа к иностранным источникам и мощной системы сетевой защиты. США пользуются своим лидирующим положением в сфере технологий, активно привлекают к сотрудничеству частный сектор и имеют оснащенные кибервойска для защиты информационного суверенитета. В России обеспечение государственного суверенитета в информационном пространстве достигается за счет Доктрины информационной безопасности и Стратегии национальной безопасности, в которых в качестве мер по его защите приводятся: развитие отечественного сегмента Интернета, повышение устойчивости стратегических объектов к хакерским атакам, развитие информационных технологий и международное сотрудничество с целью создания правовых документов, обеспечивающих справедливое и безопасное использование киберпространства.
- Среди тенденций, влияющих на развитие международным сообществом идей об информационном суверенитете государства, можно выделить: стремительный рост исследований в цифровой отрасли и создание высокотехнологичной продукции; пандемию коронавируса, вызвавшую скачок в использовании этой продукции в повседневной жизни, перемещение многих аспектов взаимодействия между людьми в онлайн-режим; использование киберпространства как площадки для ведения боевых действий в виде хакерских атак и шпионажа.
- Перед информационным суверенитетом России стоят такие серьезные вызовы, как технологическая зависимость, кибератаки, информационные войны, использование социальных сетей для обеспечения анонимности во время совершения противозаконных действий, нерегулируемые рынки криптовалют, интернет-мошенничество.
- Существующие для нашей страны угрозы вполне решаемы, если принять дополнительные меры в вопросах развития и внедрения отечественной высокотехнологичной продукции, оснащения Российской армии необходимыми средствами для отражения всех возможных видов атак в киберпространстве со стороны иностранных государств, борьбы с фейковыми новостями и информацией, мониторинга социальных сетей на предмет размещения в них угрожающей суверенитету информации, обеспечения политики в области криптовалют и пропаганды безопасного использования Интернета среди граждан.

Список источников

1. Бухарин В.В. (2016), Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности [Components of the Digital Sovereignty of the Russian Federation as a Technical Basis for Information Security], Вестник МГИМО-Университета. № 6. С. 76–91.

2. Ефремов А.А. (2017), Формирование концепции информационного суверенитета государства [Formation of the Concept of Information Sovereignity of the State], Право. Журнал Высшей школы экономики. № 1. С. 201–215.
3. Зорина Е.Г. (2017), Информационный суверенитет современного государства и основные инструменты его обеспечения [Information Sovereignity of the Modern State and the Main Tools to Ensure It], Известия Саратовского университета. Новая серия. Серия: Социология. Политология. Т. 17, № 3. С. 345–348. DOI: 10.18500/1818–9601–2017-17-3-345-348.
4. Зорина Е.Г. (2017), Искажение значений и смыслов политико-исторических событий в разноязычных версиях статей «Википедии» [Distortion of the Meanings and Senses of Political and Historical Events in Multilingual Versions of Wikipedia Articles], Власть. Т. 25, № 3. С. 211–214.
5. Ибрагимова Г. (2013), Стратегия КНР в киберпространстве: вопросы управления интернетом и обеспечение информационной безопасности [China's Strategy in Cyberspace: Issues of Internet Governance and Information Security Ensuring], Индекс безопасности. № 1 (104). С. 169–184.
6. Литвинов Д.А. (2019), Оценка политики России в области кибербезопасности и возможные варианты ее совершенствования [Assessment of Russia's Cybersecurity Policy and Possible Options for its Improvement], Вестник науки и образования. № 19–2 (73). С. 76–82.
7. Чекменева Т.Г., Ершов Б.А., Трубицын С.Д., Остапенко А.А. (2020), Стратегия Китая по обеспечению информационной безопасности: политический и технический аспекты [China's Information Security Strategy: Political and Technical Aspects], Bulletin Social-Economic and Humanitarian Research. № 7 (9). С. 78–97.
8. Damon L. (1986), Freedom of Information versus National Sovereignity: The Need for a New Global Forum for the Resolution of Transborder Date Flow Problems, Fordham International Law Journal. Vol. 10. Issue 2. P. 262–287.
9. Gong W. (2005), Information Sovereignty Reviewed, Intercultural Communication Studies. Vol. XIV. Issue 1. P. 119–135.
10. De Filippi P., McCarthy S. (2012), Cloud Computing: Centralization and Data Sovereignt, European Journal of Law and Technology. URL: http://ssrn.com/abstract=2167372.

Информация об авторах

ГРИБИН Николай Петрович. Доктор юридических наук. Профессор. Ведущий научный сотрудник Института международных исследований Московского государственного института международных отношений (Университет) МИД России. htpps://orcid.org/0000-0001-9141-445. Адрес: 119454, Российская Федерация, г. Москва, проспект Вернадского, 76. n.gordin40@gmail.com

КОХТЮЛИНА Ирина Николаевна. Кандидат политических наук. Ученый секретарь Научного совета Национального института исследований глобальной безопасности. Адрес: 127018, Российская Федерация, г. Москва, ул. Двинцев, 8, офис 1. expobroker@yandex.ru.

СЕДУНОВ Денис Игоревич. Аспирант Российской академии народного хозяйства и государственной службы при Президенте России. Адрес: 119571, Российская Федерация, г. Москва, проспект Вернадского, 82. DenisSedunov@list.ru.

СОБОЛЕВ Егор Ильич. Стажер Национального исследовательского института развития коммуникаций, студент Российского университета дружбы народов. Адрес: 119034, Российская Федерация, г. Москва, Коробейников переулок, 22, стр. 1. 1032193499@rudn.ru.

Вклад авторов

Грибин Н.П. Введение, материалы и методы, выводы совместные. Результаты исследования: Угрозы и риски устойчивости и стабильности Российской Федерации в эпоху цифровизации.

Кохтюлина И.Н. Введение, материалы и методы, выводы совместные. Результаты исследования: Международная информационная безопасность в новых геополитических реалиях.

Седунов Д.И. Введение, материалы и методы, выводы совместные. Результаты исследования: Информационный суверенитет государства: критерии и показатели.

Соболев Е.И. Введение, материалы и методы, выводы совместные. Результаты исследования: Обеспечение информационного суверенитета государств.

Авторы заявляют об отсутствии конфликта интересов.

Раскрытие информации о конфликте интересов

Авторы заявляют об отсутствии конфликта интересов.

Информация о статье

Поступила в редакцию: 28 марта 2022. Одобрена после рецензирования: 5 апреля 2022. Принята к публикации: 27 апреля 2022. Опубликована: 27.06.2022.

Авторы проичитали и одобрил окончательный вариант рукописи.

Информация о рецензировании

«Россия и мир: научный диалог» благодарит анонимных рецензентов за их вклад в рецензирование этой работы.

References

1. Buharin V.V. (2016), Components of the Digital Sovereignty of the Russian Federation as a Technical Basis for Information Security, MGIMO Review of International relations. No. 6. p. 76–91. (in Russian)
2. Efremov A.A. (2017), Formation of the Concept of Information Sovereignty of the State, Law. Journal of the Higher School of Economics. No. 1. P. 201-215. (in Russian)
3. Zorina E.G. (2017), Information Sovereignity of the Modern State and the Main Tools to Ensure It, Izvestiya of Saratov University. New Series. Series Sociology. Politology. Vol. 17, No. 3. P. 345–348. Doi: 10.18500/1818–9601–2017-17-3-345-348. (in Russian)
4. Zorina E.G. (2017), Distortion of the Meanings and Senses of Political and Historical Events in Multilingual Versions of Wikipedia Articles, Vlast. Vol. 25, No. 3. P. 211-214. (in Russian)
5. Ibragimova G. (2013), China's Strategy in Cyberspace: Issues of Internet Governance and Information Security Ensuring, Security Index. No. 1 (104). P. 169-184. (in Russian)
6. Litvinov D. A. (2019), Assessment of Russia's Cybersecurity Policy and Possible Options for its Improvement, Vestnik nauki I obrazovaniya. No. 19-2 (73). P. 76-82. (in Russian)
7. Chekmenyova T.G., Ershov B.A., Trubitsyn S.D., Ostapenko A.A. (2020), China's Information Security Strategy: Political and Technical Aspects, Bulletin Social-Economic and Humanitarian Research. No. 7 (9). P. 78-97. (in Russian)
8. Damon L. (1986), Freedom of Information versus National Sovereignty: The Need for a New Global Forum for the Resolution of Transborder Date Flow Problems, Fordham International Law Journal. Vol. 10. Issue 2. p. 262–287.
9. Gong W. (2005), Information Sovereignty Reviewed, Intercultural Communication Studies. Vol. XIV. Issue 1. p. 119–135.
10. De Filippi P., McCarthy S. (2012), Cloud Computing: Centralization and Data Sovereignt, European Journal of Law and Technology. URL: http://ssrn.com/abstract=2167372.

About the authors

GRIBIN Nikolai P. DSc (Law). Professor. Leading Researcher, Institute of International Studies of the Moscow State Institute of International Relations (University), Russian Foreign Ministry. htpps://orcid.org/0000-0001-9141-445. Address: 76 Vernadsky Avenue, Moscow, 119454, Russian Federation. n.gordin40@gmail.com.

KOKHTYULINA Irina N. CandSc (Polit). Scientific Secretary of the Scientific Council of the National Institute for Global Security Studies. Address: 8 Dvintsev str., office 1, Moscow, 127018. expobroker@yandex.ru.

SEDUNOV Denis I. Postgraduate student of the Russian Presidential Academy of National Economy and Public Administration. Address: 82 Vernadsky Avenue, Moscow, 119571. DenisSedunov@list.ru.

SOBOLEV Egor I. Intern of the National Research Institute for the Communications Development, student of the Peoples' Friendship University of Russia. Address: 119034, Moscow, korobeynikov lane, 22, p.1. 1032193499@rudn.ru.

Authors contributed

GRIBIN Nikolai P. DSc (Law). Professor. Leading Researcher, Institute of International Studies of the Moscow State Institute of International Relations (University), Russian Foreign Ministry. htpps://orcid.org/0000-0001-9141-445. Address: 76 Vernadsky Avenue, Moscow, 119454, Russian Federation, n.gordin40@gmail.com.

KOKHTYULINA Irina N. CandSc (Polit). Scientific Secretary of the Scientific Council of the National Institute for Global Security Studies. Address: 8 Dvintsev str., office 1, Moscow, 127018, , Russian Federation, expobroker@ yandex.ru.

SEDUNOV Denis I. Postgraduate student of the Russian Presidential Academy of National Economy and Public Administration. Address: 82 Vernadsky Avenue, Moscow, 119571, , Russian Federation, DenisSedunov@list.ru.

SOBOLEV Egor I. Intern of the National Research Institute for the Communications Development, student of the Peoples' Friendship University of Russia. Address: 22, p.1, Korobeynikov lane, 119034, Moscow, Russian Federation, 1032193499@rudn.ru.

Conflicts of Interest Disclosure

The authors declare that there is no conflict of interest.

Article info

Submitted: Mart 28, 2022. Approved after peer reviewing: April 5, 2022. Accepted for publication: April 27, 2022. Published: 27.06.2022.

The authors read and approved the final manuscript.

Peer review info

«Russia & World: Scientific Dialogue» thanks the anonymous reviewer(s) for their contribution to the peer review of this work.