МЕЖДУНАРОДНО-ПРАВОВЫЕ НАУКИ
INTERNATIONAL LEGAL SCIENCES

DOI: 10.18287/2542-047X-2023-9-2-85-89

НАУЧНАЯ СТАТЬЯ

УДК 341.1, 341.3

Дата поступления: 29.12.2022
рецензирования: 19.02.2023
принятия: 30.05.2023

О безопасности киберпространства: Киберпанк 202..?

Ю. В. Самович
Казанский филиал Российского государственного университета правосудия, г. Казань, Российская Федерация
E-mail: juliasamovich@gmail.com

Аннотация: Информационная безопасность в настоящее время является ахиллесовой пятой для любого государства, поскольку никто не обладает абсолютными возможностями в этой сфере, да и совершенству предела нет. Постоянно модернизируемые технологии поражают воображение, как и создаваемые в качестве ответных мер, не говоря уже о суммах финансирования, потраченных на них. В настоящей статье проведен краткий обзор некоторых положений стратегий безопасности в киберпространстве основных игроков современного противостояния, из которого следует неутешительный прогноз – потенциальная возможность сферы военных действий расширяется.
Ключевые слова: Россия; США; Европа; НАТО; АСЕАН; информационная безопасность; кибербезопасность; право; политика.
Цитирование. Самович Ю. В. О безопасности киберпространства: Киберпанк 202…? // Юридический вестник Самарского университета. 2023. Т. 9, № 2. С. 85–89. DOI: http://doi.org/10.18287/2542-047X-2023-9-2-85-89.
Информация о конфликте интересов: автор заявляет об отсутствии конфликта интересов.

Юлия Владимировна Самович – доктор юридических наук, профессор, профессор кафедры государственно-правовых дисциплин, Казанский филиал Российского государственного университета правосудия (г. Казань), 420008, Российская Федерация, Республика Татарстан, г. Казань, ул. 2-я Азинская, 7а.

SCIENTIFIC ARTICLE

Submitted: 29.12.2022
Revised: 19.02.2023
Accepted: 30.05.2023

Cyberspace security: Cyberpunk 202..?

Yu. V. Samovich
Kazan Branch of the Russian State University of Justice, Kazan, Russian Federation
E-mail: juliasamovich@gmail.com

Abstract: Information security is currently the «Achilles' heel» for any state, since no one has absolute capabilities in this area, and there is no limit to perfection. Constantly improving technologies amaze the imagination, as well as those created as a response, not to mention the amount of funding spent on them. The article provides a brief overview of some provisions of Security Strategies in cyberspace of the main players in the modern confrontation, from which a disappointing forecast follows – the potential for the scope of military operations is expanding.
Key words: Russia; USA; Europe; NATO; ASEAN; information security; cybersecurity; law; politics.
Citation. Samovich Yu. V. *O bezopasnosti kiberprostranstva: Kiberpank 202…?* [Cyberspace security: Cyberpunk 202..?]. *Iuridicheskii vestnik Samarskogo universiteta* [Juridical Journal of Samra University], 2023, vol. 9, no. 2, pp. 85–89. DOI: http://doi.org/10.18287/2542-047X-2023-9-2-85-89 [in Russian].
Information about the conflict of interests: the author declares that there is no conflict of interest.

Yulia V. Samovich – Doctor of Laws, professor, professor of the Department of State-Legal Disciplines, Kazan branch of the Russian State University of Justice (Kazan), 7a, 2nd Azinskaya Street, Kazan, 420008, Republic of Tatarstan, Russian Federation.

Моделирование «образа врага» принесло свои плоды во многих областях обеспечения безопасности современного государства, но, вероятно, один из самых пугающих с позиции потенциальных последствий и прогнозируемых угроз – это возможность враждебного использования информационного пространства или информационно-коммуникационных технологий (ИКТ), в частности попытки взлома государственных информационных ресурсов, террористическая деятельность в киберпространстве и т. д.

Проблемы обеспечения информационной безопасности и кибербезопасности обсуждаются в международном сообществе с конца 90-х годов двадцатого века. Так, в 1998 году Российская Федерация начинает международные инициативы по обсуждению регулирования информационной безопасности, Darrel C. Menthe предлагает рассматривать киберпространство с позиции именно международного права как международную территорию [1], а «общая дискуссия» по данному вопросу переходит в предметное обсуждение после первых крупных кибератак. Например, в 2009–2010 годах сетевой вирус Win32/Stuxnet атаковал не только персональные компьютеры, но и автоматизированные системы управления производством. Позже возникла гипотеза, что Stuxnet был запущен с целью удара на блоки управления газовыми центрифугами, производящими обогащенный уран на стратегических объектах. В итоге главными подозреваемыми в кибератаке стали спецслужбы Израиля и США. В 2016 году китайская хакерская группа Whitehat Keen Security Lab взломала Tesla Model S через точку доступа Wi-Fi, и подобные примеры неисчерпаемы [2].

В правовом поле Российской Федерации термины «информационная безопасность» и «кибербезопасность» нередко употребляются как синонимы либо в соотношении целого и части. В частности, термин «кибербезопасность» появлялся в проекте Концепции стратегии кибербезопасности Российской Федерации 2013 года, авторы которого подчеркивали, что в сфере российских актов, посвященных информационной безопасности, должно быть определение кибербезопасности, что позволит согласовать отечественные и иностранные правовые акты, в том числе для адекватного участия в работе над международными [3]. Однако указанный проект был раскритикован Федеральной службой безопасности России, и в настоящее время в правовом поле Российской Федерации действует понятие «информационная безопасность», включающее контент Интернета [4].

Дефиниция раскрывается в Доктрине информационной безопасности Российской Федерации [5], в том числе за счет понятия «информационное пространство», определяемого как совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети Интернет, сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также как совокупность механизмов регулирования соответствующих общественных отношений.

Терминология в настоящей статье основана на действующих международно-правовых формулировках и нормах Российской Федерации и позволяет в целом приемлемо обсуждать вопросы, не будучи специалистом в области IT.

В принятой 2 июля 2021 года Стратегии национальной безопасности России информационная безопасность (ИБ) впервые фигурирует как национальный интерес и стратегический национальный приоритет [6].

В Глобальном индексе кибербезопасности (Global Cybersecurity Index, GCI) специалисты Международного союза электросвязи (МСЭ) проводят сравнение стран по уровню развития технологий, индустрии ИБ и участию в защите глобального виртуального пространства. В 2020 году из 194 стран Российская Федерация на пятом месте с баллом 98,06 из 100 возможных, это на 21 позицию выше по сравнению с предыдущим результатом. Для сравнения, Республика Корея находится на 4-м месте с результатом в 98,52 балла [7].

В отличие от России новая (2022) Стратегия национальной безопасности США конкретно говорит именно об обеспечении безопасности киберпространства, обвиняя другие страны в кибератаках на важнейшие инфраструктуры (кстати, в качестве «названной» в Стратегии фигурирует именно Россия), которые становятся все более цифровыми и уязвимыми для сбоев или разрушения в результате кибератак [8]. США намерены «решительно реагировать всеми соответствующими инструментами национальной власти на враждебные действия в киберпространстве, включая те, которые нарушают или ухудшают жизненно важные национальные функции или критическую инфраструктуру» [8].

Североатлантический союз в последней Стратегии [9] указывает на киберпространство как новую сферу оборонительной среды даже с некоторой агрессией: «Обеспечение безопасного использования и беспрепятственного доступа к космосу и киберпространству является ключом к эффективным сдерживанию и обороне. Мы будем укреплять нашу способность эффективно действовать в космосе и киберпространстве, для того чтобы предотвращать, обнаруживать, противодействовать и реагировать на весь спектр угроз, используя все доступные инструменты. Единичные действия в киберпространстве или их совокупный набор, или враждебные операции, проводимые в направлении космоса, из космоса или внутри него, могут достичь уровня вооруженного нападения и могут привести к тому, что Североатлантический совет прибегнет к статье 5 Североатлантического договора. Мы признаем применимость международного права и будем поощрять ответственное поведение в киберпространстве и космосе. Мы

также будем повышать устойчивость космических и кибернетических потенциалов, от которых зависит наша коллективная оборона и безопасность» [9, п. 25].

Как отмечает Александр Бартош, киберпространство объявлено новой оперативной средой, выпущено руководство по вариантам стратегического реагирования на киберактивность [10].

По предположениям аналитиков, самым быстрорастущим рынком в течение 2021–2026 гг. станет Азиатско-Тихоокеанский регион, в котором основное место занимает Китай.

Киберпространство Китайской Народной Республики – уже длительное время важнейшая сфера деятельности Народно-освободительной армии Китая (НОАК) и других силовых структур, однако работа ведется в тесном сотрудничестве с гражданским сектором. В этом контексте стоит упомянуть и «Великий китайский файрвол» (Great Firewall of China) – «Золотой щит», одну из самых совершенных систем по ограничению интернет-контента в мире [11]. Как отмечают специалисты, китайская модель «немасштабируема», поскольку вряд ли какое-либо еще государство сумело бы разработать и претворить в реальность настолько цельный и независимый внутренний интернет, обладающий абсолютной системой управления и блокировок без нанесения ущерба собственной экономике, не говоря уже о том, что национальные версии глобальных интернет-сервисов превратились из американских копий в оригинальные интернет-платформы (Taobao, AliPay, WeChat, Weibo и др.), в результате чего национальный интернет-рынок стал самым мощным в мировом сообществе.

Несмотря на тот факт, что Южная Корея становится одной из главных мишеней кибератак из-за огромного числа подключенных устройств, использования мобильных механизмов и интеллектуальной собственности, она пребывает в положении одной из ведущих мировых держав в сфере информационных технологий и информатизации общества.

5 мая 2022 года Государственное разведывательное управление Южной Кореи заявило, что присоединилось к группе киберзащиты при Организации Североатлантического договора (НАТО) в качестве первого азиатского члена, а Национальная разведывательная служба (NIS) Южной Кореи была официально принята в Центр передового опыта совместной киберзащиты НАТО (CCDCOE), базирующийся в Таллине (Эстония) [12]. По сообщению шпионского агентства, NIS два года подряд, начиная с 2020 года, участвовала в крупнейших в мире международных учениях по киберзащите с боевыми стрельбами Locked Shields [13].

16 мая 2022 года японское агентство Nikkei Shimbun объявило, что Соединенные Штаты, Япония, Южная Корея и четыре других члена Азиатско-Тихоокеанского экономического сотрудничества (АТЭС) согласились сделать правила передачи персональных данных независимыми от нынешних рамок регионального форума, стремясь исключить Китай и Россию. В Правилах трансграничной конфиденциальности (CBPR) участвуют девять членов АТЭС: Япония, США, Южная Корея, Канада, Тайвань, Филиппины, Сингапур, Австралия и Мексика. Исключая Австралию и Мексику, остальные семь членов согласились создать новую глобальную систему CBPR. Она будет независима от АТЭС и активно примет участие стран, не входящих в АТЭС. Семь членов АТЭС будут опираться на существующую CBPR и создадут новую корпоративную систему сертификации. Если добавить Бразилию и Великобританию, это может вырасти в новую систему передачи данных, аналогичную системе Европейского союза [14].

Ответ долго ждать не пришлось. 30 июня Администрация киберпространства Китая опубликовала проект положения о стандартном контракте на трансграничную передачу личной информации, который вводит стандартные договорные положения для консультаций с общественностью.

7 июля CAC дополнительно опубликовал долгожданные меры по оценке безопасности трансграничной передачи данных, которые вступают в силу с сентября [15].

Многие китайские эксперты прогнозируют, что американо-китайское противостояние в киберпространстве при наличии ряда обстоятельств может достичь «точки невозврата» и повлечь катастрофические последствия для обеих сторон. И хотя, по их мнению, «достаточно глубокое осознание этого может стать фактором взаимного сдерживания в этом противостоянии и в совместном поиске «правил поведения» в данной области» [16], такого исхода стоит ожидать с минимальной вероятностью.

На Форуме в Давосе эксперты прогнозируют, что 2023 год станет годом кибербезопасности. Тем не менее, хотя профессор кибербезопасности Оксфордского университета Сэди Криз и говорит о надвигающемся «кибер-шторме», предложения о совместных действиях для «спасения» попрежнему не дают нужного эффекта. В вопросах поиска образа врага, однако наблюдается редкое согласие: широко распространено опасение, что правительства усилят свою поддержку или прямое участие в подрывных кибероперациях, особо изощренные кибератаки в будущем приписываются России и Северной Корее [17].

Текущая ситуация в мире не является оптимистичной. Расширение сфер военного пространства под предлогом соблюдения принципов международного права демонстрирует лишь нежелание начинать конструктивный диалог и целеустремленно приближает всех к точке невозврата. Отдельной проблемой является тот факт, что распространение норм международного гуманитарного права на действия в киберпространстве, *a priori* предполагаемое международниками, может встретить жесткое сопротивление уже на стадии квалификации кибератак как военных операций.

Библиографический список

1. Menthe Darrel C. Jurisdiction in Cyberspace: A Theory of International Spaces // Michigan Telecommunications and Technology Law Review. 1998. Vol. 4, issue 1. URL: https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1163&context=mttlr.

2. Десять самых громких кибератак XXI века // РБК. URL: https://trends.rbc.ru/trends/industry/600702d49a79473ad25c5b3e.

3. Концепция стратегии кибербезопасности Российской Федерации. Проект. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2014_Orig_Draft_41d4b3dfbdb25cea8a73.pdf.

4. Концепция не подошла по понятиям. В части кибербезопасности СФ придется синхронизироваться с ФСБ // Коммерсантъ. № 221 от 30.11.2013. URL: https://www.kommersant.ru/doc/2357276?ysclid=lj2rjhkcuh850362884.

5. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102417017&rdk=&firstDoc=1&lastDoc=1.

6. Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации». Раздел III (5) // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001202107030001?index=8&rangeSize=1.

7. Россия разделила с Малайзией и ОАЭ пятое место в рейтинге кибербезопасности МСЭ // D-Russia.ru. 21.07.2021. URL: https://d-russia.ru/rossija-razdelila-s-malajziej-i-oaje-pjatoe-mesto-v-rejtinge-kiberbezopasnosti-msje.html?ysclid=lj2siwrt2k219834897.

8. National Security Strategy. October 2022. URL: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

9. Стратегическая концепция НАТО 2022 года. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept-ru.pdf.

10. Бартош А. Роботы воюют, умы атакованы, решения ускоряются // Независимое военное обозрение. 08.08.2022. URL: https://nvo.ng.ru/nvo/2022-08-04/1_1200_robots.html?ysclid=lj2swz76co887998600.

11. Цензура (контроль) в Интернете. Опыт Китая // Tadviser. Государство. Бизнес. Технологии. 21.11.2022. URL: https://www.tadviser.ru/index.php/Статья:Цензура_(контроль)_в_интернете._Опыт_Китая?ysclid=lj2t3lrj9t311105910.

12. S. Korea's spy agency joins NATO cyber defense group // Yonhap news agency. May 05, 2022. URL: https://en.yna.co.kr/view/AEN20220505001500315

13. He-rim Jo. South Korea’s intelligence agency joins NATO’s cyber defense center as first in Asia // The Korea Herald. URL: https://www.koreaherald.com/view.php?ud=20220505000162.

14. Several countries pursue new data transfer rules to keep out China, Russia // Caliber.Az, 17 May 2022. URL: https://caliber.az/en/post/79846/.

15. Ho D., Zhu M. The Privacy Advisor. China cross-border data transfer mechanism and its implications // IAPP. August 23, 2022. URL: https://iapp.org/news/a/china-cross-border-data-transfer-mechanism-and-its-implications/.

16. Кокошин А., Кашин В. О подходах руководства КНР и китайских силовых структур к противоборству в киберпространстве // РСДМ. 25.07.2022. URL: https://russiancouncil.ru/analytics-and-comments/comments/o-podkhodakh-rukovodstva-knr-i-kitayskikh-silovykh-struktur-k-protivoborstvu-v-kiberprostranstve/?ysclid=lj2toa3ffl714159643.

17. Experts at Davos 2023 call for a global response to the gathering «cyber storm» // World Economic Forum. January 18, 2023. URL: https://www.weforum.org/agenda/2023/01/cybersecurity-storm-2023-experts-davos23.

References

1. Menthe Darrel C. Jurisdiction in Cyberspace: A Theory of International Spaces. *Michigan Telecommunications and Technology Law Review*, 1998, vol. 4, issue 1. Available at: https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1163&context=mttlr.

2. *Desyat' samykh gromkikh kiberatak XXI veka* [Ten most sensational cyberattacks of the XXI century]. *Retrieved from the official website of RBC*. Available at: https://trends.rbc.ru/trends/industry/600702d49a79473ad25c5b3e [in Russian].

3. *Kontseptsiya strategii kiberbezopasnosti Rossiiskoi Federatsii. Proekt* [Concept of the cybersecurity strategy of the Russian Federation. Project]. Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2014_Orig_Draft_41d4b3dfbdb25cea8a73.pdf [in Russian].

4. *Kontseptsiya ne podoshla po ponyatiyam. V chasti kiberbezopasnosti SF pridetsya sinkhronizirovat'sya s FSB* [The concept did not fit the concepts. In terms of cybersecurity, the Federation Council will have to synchronize with the FSB]. *Kommersant"*, no. 221, 30.11.2013. Available at: https://www.kommersant.ru/doc/2357276?ysclid=lj2rjhkcuh850362884 [in Russian].

5. *Ukaz Prezidenta Rossiiskoi Federatsii ot 05.12.2016 № 646 «Ob utverzhdenii Doktriny informatsionnoi bezopasnosti Rossiiskoi Federatsii»* [Decree of the President of the Russian Federation dated 05.12.2016 № 646 «On

the approval of the Information Security Doctrine of the Russian Federation»]. *Retrieved from the official Internet portal of legal information*. Available at: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102417017&rdk=&firstDoc=1&lastDoc=1 [in Russian].

6. *Ukaz Prezidenta Rossiiskoi Federatsii ot 02.07.2021 № 400 «O Strategii natsional'noi bezopasnosti Rossiiskoi Federatsii». Razdel III (5)* [Decree of the President of the Russian Federation dated 02.07.2021 № 400 «On the National Security Strategy of the Russian Federation». Section III (5)]. *Retrieved from the official Internet portal of legal information*. Available at: http://publication.pravo.gov.ru/Document/View/0001202107030001?index=8&rangeSize=1 [in Russian].

7. *Rossiya razdelila s Malaiziei i OAE pyatoe mesto v reitinge kiberbezopasnosti MSE* [Russia shared the fifth place in the ITU cybersecurity rating with Malaysia and the UAE]. *Retrieved from the official website of D-russia.ru. 21.07.2021*. Available at: https://d-russia.ru/rossija-razdelila-s-malajziej-i-oaje-pjatoe-mesto-v-rejtinge-kiberbezopasnosti-msje.html [in Russian].

8. National Security Strategy. October 2022. Available at: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

9. *Strategicheskaya kontseptsiya NATO 2022 goda* [NATO Strategic Concept of 2022]. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept-ru.pdf [in Russian].

10. *Bartosh A. Roboty voyuyut, umy atakovany, resheniya uskoryayutsya* [Robots are at war, minds are attacked, decisions are accelerated]. *Nezavisimoe voennoe obozrenie*, 08.08.2022. Available at: https://nvo.ng.ru/nvo/2022-08-04/1_1200_robots.html?ysclid=lj2swz76co887998600 [in Russian].

11. *Tsenzura (kontrol') v Internete. Opyt Kitaya* [Censorship (control) on the Internet. The experience of China]. *Tadviser. Gosudarstvo. Biznes. Tekhnologii* [Tadviser. Government. Business. IT], 21.11.2022. Available at: https://www.tadviser.ru/index.php/Статья:Цензура_(контроль)_в_интернете._Опыт_Китая?ysclid=lj2t3lrj9t311105910 [in Russian].

12. S. Korea's spy agency joins NATO cyber defense group. *Yonhap news agency*, May 05, 2022. Available at: https://en.yna.co.kr/view/AEN20220505001500315.

13. *He-rim Jo.* South Korea’s intelligence agency joins NATO’s cyber defense center as first in Asia. *The Korea Herald*. Available at: https://www.koreaherald.com/view.php?ud=20220505000162.

14. Several countries pursue new data transfer rules to keep out China, Russia. *Caliber.Az*, May 17, 2022. Available at: https://caliber.az/en/post/79846/.

15. *Ho D., Zhu M.* The Privacy Advisor. China cross-border data transfer mechanism and its implications. *IAPP*, August 23, 2022. URL: https://iapp.org/news/a/china-cross-border-data-transfer-mechanism-and-its-implications/.

16. *Kokoshin A., Kashin V. O podkhodakh rukovodstva KNR i kitaiskikh silovykh struktur k protivoborstvu v kiberprostranstve* [On the approaches of the leadership of the People's Republic of China and Chinese law enforcement agencies to the confrontation in cyberspace]. *Retrieved from the official website of RIAC*, 25.07.2022. Available at: https://russiancouncil.ru/analytics-and-comments/comments/o-podkhodakh-rukovodstva-knr-i-kitayskikh-silovykh-struktur-k-protivoborstvu-v-kiberprostranstve/?ysclid=lj2toa3ffl714159643 [in Russian].

17. Experts at Davos 2023 call for a global response to the gathering «cyber storm». *World Economic Forum*, January 18, 2023. Available at: https://www.weforum.org/agenda/2023/01/cybersecurity-storm-2023-experts-davos23.