Научная статья С. 62–68
УДК 343.9.01

РОЛЬ ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ В. В. ПУТИНА В ОБЪЕДИНЕНИИ УСИЛИЙ МИРОВОГО СООБЩЕСТВА ПО СОВЕРШЕНСТВОВАНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ

Петр Николаевич Кобец
Всероссийский научно-исследовательский институт МВД России, Москва, Россия
pkobets37@rambler.ru, https://orcid.org/0000-0001-6527-3788

Аннотация. Актуальность проведенного исследования обусловлена тем, что в настоящее время частные лица, предприятия и организации, системы критической инфраструктуры правительств большинства государств мира активно используют цифровые технологии. Эти технологии предоставляют возможности на многих уровнях, включая экономический и социальный. Однако, по мере роста и возможностей доступности цифровых информационных технологий, и телекоммуникационных сетей, киберугрозы становятся все более скоординированными и серьезными. В этой связи, по мере того, как вредоносные кибер-инструменты становятся все более доступными, а уровень мировой киберпреступности продолжает расти, существует реальная угроза экономическому и политическому благополучию многих мирровых держав. Поскольку большая часть критической инфраструктуры большинства экономически развитых государств может управляться удаленно, а основные услуги управляются онлайн, кибер-инциденты могут поставить под угрозу не только общественную, но и в целом национальную безопасность многих стран. Для устранения этих рисков Президентом Российской Федерации В. В. Путиным, на регулярной основе выдвигаются предложения по объединению усилий мирового сообщества для совместной деятельности по обеспечению информационной безопасности в киберпространстве. Проведенное исследование предусматривает дальнейшее его использование в качестве методического материала, для принятия различных управленческих решений, как на национальном, так и на международном уровнях борьбы с киберпреступлениями, а также при создании необходимых условий для эффективного и надежного международного сотрудничества по борьбе с преступностью в киберпространстве.

Ключевые слова: национальная безопасность, информационное пространство, международное сотрудничество, правовое регулирование, мировое сообщество, стратегическое планирование, киберпространство, киберпреступность

Для цитирования: Кобец П. Н. Роль Президента Российской Федерации В. В. Путина в объединении усилий мирового сообщества по совершенствованию информационной безопасности в киберпространстве // Правопорядок: история, теория, практика. 2022. № 2 (33). С. 62–68.

Research article

THE ROLE OF THE PRESIDENT OF THE RUSSIAN FEDERATION V. V. PUTIN IN COMBINING THE EFFORTS OF THE WORLD COMMUNITY TO IMPROVE INFORMATION SECURITY IN CYBERSPACE

Peter N. Kobets
National Research Institute of the Ministry of Interior of the Russian Federation, Moscow, Russia
pkobets37@rambler.ru, https://orcid.org/0000-0001-6527-3788

Abstract. The relevance of the study is due to the fact that at present individuals, enterprises and organizations, critical infrastructure systems of governments in most countries of the world are actively using digital technologies. These technologies provide opportunities at many levels, including economic and social. However, with the growth and availability of digital information technology and telecommunications networks, cyber threats are becoming more coordinated and serious. In this regard, as malicious cyber tools become more and more available, and the level of global cybercrime continues to grow, there is a real threat to the economic and political well-being of many world powers. Since most of the critical infrastructure of most economic development states can be managed remotely, and the main services are managed online, cyber incidents can threaten not only the public, but also the overall national security of many countries. To eliminate these risks, the President of the Russian Federation V. V. Putin, on a regular basis there are proposals to unite the efforts of the world community for joint activities to ensure information security in cyberspace. The study provides for its further use as a methodological material for making various management decisions, both at the national and international levels of combating cybercrime, as well as creating the necessary conditions for effective and reliable international cooperation in combating cyberspace.

Keywords: national security, information space, international cooperation, legal regulation, world community, strategic planning, cyberspace, cybercrime

For citation: Kobets PN. The Role of the President of the Russian Federation V. V. Putin in Combining the Efforts of the World Community to Improve Information Security in Cyberspace. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2022;(2):62-68. (In Russ.)

Введение

С каждым годом расширяется влияние и без того достаточно широкого спектра противоправных деяний, совершаемых в сети Интернет: мошенничество, вымогательство, различные злоупотребления, связанные с детской порнографией, педофилией, шпионаж, вандализм, всевозможные притеснения граждан, и т. д. Однако при этом вредоносная деятельность в киберпространстве, наряду с разнообразными преступными посягательствами, перечисленными выше, все чаще, включает в себя попытки хищения особо интересующих преступников, всевозможных массивов информационных данных [9, с. 150]. При этом важно отметить, что по мнению ряда экспертов, основная часть совершаемых киберпреступлений не может быть зафиксирована статистической отчетностью, в силу высокой латентности рассматриваемых противоправных деяний [3, с. 62]. А также потому, что часть пострадавших лиц не обращается в правоохранительные органы, полагая, что даже если преступники будут пойманы, возместить преступный вред им будет весьма непросто [1, с. 173].

В современном мировом сообществе, цифровые технологии и система Интернет приобретают все большее значение для инноваций и экономического роста. Цифровые технологии являются неотъемлемой частью нашей повседневной жизни. В соответствии с прогнозами, представленными Всемирной ассоциации представляющей интересы операторов мобильной связи во всем мире (GSMA), к 2025 году количество подключений к технологиям Интернет вещей — Internet of Things (далее — IoT) удвоится и достигнет почти 25 млрд, что обусловит риски возрастания кибератак[1]. По мере того, как вредоносные кибер-инструменты становятся все более доступными, а уровень киберпреступности продолжает расти,

[1] См.: Интернет вещей, IoT, M2M мировой рынок // TAdviser : [сайт]. UPL: https://www.tadviser.ru/index.php (дата обращения 14.03.2022).

существует реальная угроза экономическому благополучию большинства государств мира. Поскольку большая часть критической инфраструктуры государств может управляться удаленно, а основные услуги управляются онлайн, кибер-инциденты могут поставить под угрозу национальную безопасность и общественную безопасность в этих государствах.

Материалы и методы

В качестве объекта исследования выступили общественные отношения, складывающиеся вокруг предпринятых Президентом Российской Федерации В. В. Путиным всех необходимых усилий по объединению мирового сообщества для совместной деятельности по обеспечению информационной безопасности в киберпространстве. Предметом исследования послужили различные источники правовой и иной информации об основных направлениях и организационных мерах, направленных на повышение международного сотрудничества по креплению глобальной кибербезопасности. Методологической основой проведенного исследования выступили, общенаучные методы, в том числе формальной логики, анализа, синтеза и диалектический; частнонаучные методы, среди которых сравнительно-правовой, логико-юридический, анализа документов, системно-структурный. Данная работа может быть в дальнейшем использована в качестве методического материала, в процессе принятия решений управленческого характера, для борьбы с киберпреступностью, а также в процессе выстраивания международного сотрудничества по данному направлению деятельности.

Обсуждение проблемы

Отечественные эксперты отмечают, что в 2017 г. мировая экономика от деятельности киберпреступников получила ущерб «в 600 млрд долларов США в 2018 году 1,5 трлн долларов США, то уже в 2019 году — 2,5 трлн долларов США, а согласно прогнозу, Всемирного экономического форума, в 2022 г. сумма планетарного ущерба от кибератак вырастет до 8 трлн долларов США» [4, с. 168]. В этой связи является показательным выступление Генерального секретаря ООН Антониу Гутерриша на 14-й сессии Конгресса ООН по предупреждению преступности 2021 г. в г. Киото, где он высказался о необходимости предупреждении рассматриваемых преступлений, важности уголовного правосудия и верховенства права, которым отведена ключевая роль по обновлению общественного договора между странами и их обществом. Генсеком ООН также было добавлено, что соблюдение принципа верховенства права необходимо для устойчивого, социального, политического и экономического развития мирового сообщества, потому, как современное общество остро нуждается в инклюзивной не допускающей дискриминации системе правосудия, действующей в интересах всего социума[1].

Международный союз электросвязи при ООН, в лице своих экспертов составляет рейтинги по странам мира, анализируя их уровень кибербезопасности, и на основе этого формирует Глобальный индекс кибербезопасности — Global Cybersecurity Index[2], который базируется на исследовании 195 государств. Составляя рейтинги государств, экспертами исследовались следующие показания: имеются ли в исследуемом государстве «правовые системы и структуры, которые занимаются проблемами кибербезопасности; какими техническими возможностями в сфере кибербезопасности обладает страна; существуют ли в стране на уровне государства, институты связанные с координацией политики и стратегии совершенствования кибербезопасности; имеются ли в стране научно-исследовательские, образовательные и подготовительные программы, а также сертифицированные специалисты и госучреждения, способствующие росту потенциала для обеспечения информационной безопасности; имеются ли в стране партнеры, механизмы сотрудничества и системы по обмену информационными данными» [8, с. 70].

В 2020 г. Российская Федерация заняла пятое место вместе с Малайзией и Объединенными Арабскими Эмиратами в рейтинге кибербезопасности ООН по версии Международного союза электросвязи, уступив Королевству Испании, Республики Корея и Республике Сингапур, которые разделили четвертое место, Эстонии находящейся на третьем месте Великобритании и Саудовской Аравии, которые делят второе место, и Соединенным Штатам Америки, находящимся на первом месте[3].

---

[1] См.: Глава ООН призвал обеспечить правовую защиту людей в киберпространстве // Организация Объединенных Наций : [сайт]. UPL: https://news.un.org/ru/story/2021/03/1398122 (дата обращения 14.03.2022).

[2] См.: Global Cybersecurity Index // ITU : [сайт]. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (дата обращения 14.03.2022).

[3] Россия заняла пятое место в международном индексе кибербезопасности // РИА Новости : [сайт]. UPL: https://ria.ru/20210705/kiberbezopasnost-1739871486.html (дата обращения 14.03.2022).

Сегодня частные лица, предприятия, системы критической инфраструктуры и правительства большинства государств мира активно используют цифровые технологии [5, с. 121]. Эти технологии предоставляют возможности на многих уровнях, включая экономический и социальный. Однако, по мере роста и возможностей доступности цифровых информационных технологий, и телекоммуникационных сетей, киберугрозы становятся все более скоординированными и серьезными. В этой связи, на десятом российском форуме по управлению Интернетом (RIGF-2019) президентом Российской Федерации В. В. Путиным была отмечена, необходимость по эффективному противодействию всем рискам и вызовам киберпреступности[1].

При этом нельзя не отметить, что киберпреступность и связанные с ней решения в области кибербезопасности могут быть такими же сложными и разнообразными, как и лежащие в их основе технологии [6, с. 47]. В то время, как кибербезопасность и конфиденциальность данных часто идут рука об руку, кибербезопасность в первую очередь связана с защитой данных от нежелательного доступа, в то время, как конфиденциальность связана с администрированием и использованием данных.

В рассматриваемом контексте, чрезвычайно важно отметить что, в основной дискуссии конференции по искусственному интеллекту Artificial Intelligence Journey 2020 на тему Искусственный интеллект — главная технология XXI века, которая проходила 4 декабря 2020 г. главой Сбербанка Г. Грефом было отмечено что много россиян особенно пожилого возраста стали жертвами киберпреступников, которые похищают данные пользователей, а также заняты вскрытием данных электронной почты, шантажом, хищением денежных средств. Г. Греф также отметил, что при этом государство слабо реагирует на указанные правонарушения в киберпространстве, польку, по его мнению, в уголовном и административном законодательстве в недостаточной степени прописаны все компьютерные преступления, а также предусмотрена небольшая санкция за их совершение в отличие от многих иностранных государств. Кроме того, Г. Греф указал на то, что уголовно-процессуальное законодательство в недостаточной степени регламентирует расследование киберпреступлений. Он также отметил, что правоохранительным органам не хватает законодательной базы, оборудования и специалистов для эффективного противодействия киберпреступности. Поэтому для успешной борьбы с киберпреступностью нужны новые государственные инициативы в рассматриваемой сфере, которые бы основывались на союзе правоохранителей, государственных органов и крупных компаний — операторов сотовой связи, работающих в сети Интернет. В связи этим высказыванием, Президент Российской Федерации В. В. Путин отметил, что разделяет позицию Г. Грефа о том, что противодействовать киберпреступности следует объединив все имеющиеся усилия, при этом не обязательно увеличивать и ужесточать санкции за совершение киберпреступлений, важно обеспечить эффективную борьбу с киберпреступниками и неотвратимость их наказания. При этом, по мнению Президента Российской Федерации, для обеспечения эффективности борьбы с киберпреступностью, необходимо чтобы все государственные сферы деятельности были пронизаны информационными технологиями[2].

Пути решения проблемы

Осуществлять эффективную борьбу против киберпреступности возможно на основе объединения всех международных усилий. И первые шаги в рассматриваемом направлении были сделаны еще в 2005 г., когда крупнейшими мировыми провайдерами, предоставляющими интернет-услуги, было заявлено о том, что они заключают «глобальный антикризисный альянс, в рамках которого создается система раннего оповещения о проведении хакерской атаки в сети Интернет [2, с. 218].

В настоящее время кибербезопасность в информационной сфере представляет «технологии, процессы и политику, которые помогают предотвратить или уменьшить негативное влияние событий в киберпространстве, которые могут произойти в результате преднамеренных действий против информационных технологий со стороны враждебного или злонамеренного субъекта» [7, с. 21]. Поэтому в сентябре 2020 г. в одном из своих выступлений, Президентом Российской Федерации В. В. Путиным было предложено разработать документы о недопущении различных

[1] См.: Путин заявил о важности противодействия киберпреступности // РИА Новости : [сайт]. URL: https://ria. ru/20190408/1552468651.html. (дата обращения 14.03.2022).

[2] См.: Конференция по искусственному интеллекту // Сайт Президента России. UPL: http://www.kremlin.ru/events/president/news/64545 (дата обращения 14.03.2022).

инцидентов в информационной сфере (киберпространстве). Им также были озвучены различные предложения об осуществлении сотрудничества по кибербезопасности между Российской Федерацией и США, а также со всеми государствами мира. Особо В. В. Путиным подчеркивалось, что основным стратегическим вызовом является возникновение масштабных столкновений в цифровой сфере, и в этой связи важнейшая роль по их предотвращению отводится ключевым игрокам, осуществляющим международную информационную безопасность. В этой связи Президент Российской Федерации призвал продолжать осуществление непрерывной и эффективной работы между ведомствами Россией и США курирующими международную кибербезопасность. В. В. Путиным также было предложено проработать вопрос о разработке и подписании межправительственного документа по предотвращению инцидентов в информационном поле, составленному по аналогии с Договорами между Российской Федерацией и США по открытому морю и воздушному пространству от 1972 г. В. В. Путин обращаясь ко всем мировым державам, предложил провести переговоры о не нанесении первыми ударов в отношении друг друга, с применением информационных и телекоммуникационных технологий[1].

22 октября 2020 г. во время пленарного заседания дискуссионного клуба «Валдай», В. В. Путиным также было отмечено о необходимости помнить, что на нашей планете идет процесс формирования бесконечного цифрового пространства, а население Земли стремится к быстрейшему его освоению. При этом Президент Российской Федерации подчеркнул, что эпидемия COVID-19 стимулировала дальнейшее совершенствование дистанционных электронных технологий, а коммуникация на основе системы Интернет стала всеобщим достоянием. В этой связи важно, обеспечить бесперебойное и безопасное функционирование не только телекоммуникационной инфраструктуры, но и всего киберпространства[2].

Также следует сказать о том, что помимо укрепления глобального международного сотрудничества по совершенствованию информационной безопасности в киберпространстве, нашей страной предлагаются меры по укреплению двустороннего сотрудничества между правительствами, государственным, и частным секторами. Киберпреступники могут безнаказанно действовать в некоторых странах, которые не располагают ресурсами, возможностями или правовой базой для борьбы с ней. Скоординированные усилия по закрытию этих безопасных убежищ усилит положительный эффект от предпринятых мер. Так в частности в заявлении, сделанном 13 июня 2021 г. Президентом Российской Федерации В. В. Путиным программы в эфире программы «Москва. Кремль» на телевизионном канале «Россия 1» о готовности Российской Федерации выдавать киберпреступников США, было отмечено, что такие действия нашей страны возможны при достижении соответствующих двусторонних договоренностей. Кроме того, Президентом Российской Федерации проблема кибербезопасности была обозначена, как одна из самых важных на сегодняшний день, поскоку, по его мнению, отключение целых систем, может привести к весьма нежелательным последствиям[3].

Современная индустрия кибербезопасности охватывает широкий спектр профилактических и корректирующих оперативных функций (идентификацию, защиту, обнаружение, реагирование и восстановление) практически на всех носителях (например, устройствах, приложениях, сети, данных и пользователях) [10, с. 143]. В каждом сегменте есть много игроков, начиная от тех, кто борется с традиционными формами кибератак, такими как вымогатели, фишинговые мошенничества и распределенный отказ в обслуживании — Distributed Denial of Services, и заканчивая теми, кто создает решения для зарождающихся или недавно появившихся технологических инфраструктур, таких, как Облако или Интернет вещей — различные физические объекты, подключенные к сети Интернет и имеющие возможность обмениваться данными. Независимо от их места в отрасли, поставщики решений в области кибербезопасности должны развиваться, чтобы справиться с постоянно растущей изощренностью киберпреступности.

В это связи важно отметить, что на заседании Совета Безопасности, проходившего 26 марта 2021 г. Президентом Российской

[1] См.: Путин предложил странам мира договориться не наносить киберудары // РБК : [сайт]. UPL: https://www.rbc.ru/politics/25/09/2020/5f6dd2589a794776d7fc32ae (дата обращения 14.03.2022).

[2] См.: Путин призвал добиваться бесперебойной и безопасной работы киберпространства // ТАСС : [сайт]. UPL: https://tass.ru/politika/9790943 (дата обращения 14.03.2022).

[3] См.: Путин: Россия готова выдать США киберпреступников при взаимности // Коммерсантъ : [сайт]. URL: https://www.kommersant.ru/doc/4856510 (дата обращения 14.03.2022).

Федерации В. В. Путиным, была высказана необходимость формулирования универсальных правил поведения стран в информационном пространстве. Так, в частности, российский лидер полагает, что всемирные правила помогут в деле выстраивания взаимовыгодного партнерства при осуществлении взаимодействия в сети Интернет не прибегать к конфликтным ситуациям. По мнению В. В. Путина принятие подобных правил поможет созданию благоприятных условий по научному поиску, быстрому внедрению передовых решений и предотвращению возможных рисков в рассматриваемой сфере. Кроме того, Президентом Российской Федерации было отмечено, что наша страна является одним из первых государств, которое призывает мировое сообщество объединить усилия в совместной деятельности по обеспечению информационной безопасности в киберпространстве[1].

Таким образом, несмотря на то, что киберпространство поддерживает мировой экономический рост, оно стало местом конфликтов и недобросовестной конкуренции, которая до сих пор характеризовалась низкой интенсивностью с точки зрения информационных технологий, политической дестабилизации и экономической гегемонии. Российская Федерация смогла выявить эти проблемы, и с помощью диалога пытается предложить идеи и решения, которые в большей степени учитывают устойчивое цифровое развитие, как с точки зрения управления Интернетом, так и с точки зрения защиты персональных данных или кибербезопасности операторов, имеющих важное значение для устойчивого функционирования всего мирового сообщества. Наша страна в дальнейшем намерена играть активную роль в продвижении безопасного, стабильного и открытого киберпространства.

Заключение

В заключении хотелось бы особо подчеркнуть, что угрозы, с которыми сталкивается мировое сообщество в киберпространстве, сложны и быстро развиваются. Правительства, предприятия, организации, и в целом население планеты с каждым годом становятся все более уязвимы, поскольку все больше экономического сектора и основных услуг переходит в онлайн. При таком развитии технологий, когда международный характер киберпространства стал объективной реальностью для предотвращения и судебного преследования киберпреступности требуется многоуровневое сотрудничество между правительствами и правоохранительными органами большинства государств. В сложившейся ситуации важнейшим и ключевым вопросом является характер и качество обмена информацией между государственным и частным секторами разных стран о киберпреступниках. Сегодня существует гораздо больше информации о ландшафте угроз кибербезопасности, чем в настоящее время доступно частному и государственному секторам большинства странах. Для решения растущей проблемы киберпреступности потребуется более активное участие всех заинтересованных сторон, а значит всего мирового сообщества. Сегодня становится абсолютно очевидно, что обеспечение глобальной кибербезопасности это не самоцель, это та необходимость, которую все международное сообщество должно добровольно взять на себя, чтобы гарантировать, что инновации в сфере кибертехнологий будут продолжать процветать, стимулируя рынки и улучшать нашу жизнь.

[1] См.: Путин предложил принять всемирные правила поведения в киберпространстве // 5-tv.ru : [сайт]. UPL: https://www.5-tv.ru/news/333046/putin-prizval-vystroit-strategiu-pozasite-rfvcifrovoj-sfere/ (дата обращения 14.03.2022).

Список источников

1. Абсатаров Р. Р. Противодействие компьютерному терроризму // Современная юриспруденция: актуальные вопросы, достижения и инновации : сборник статей VI Международной научно-практической конференции, Пенза, 25 февраля 2018 года. Пенза : МЦНС Наука и Просвещение, 2018. С. 172–174.

2. Акопов Г. Л. Правовая информатика: современность и перспективы : учебное пособие. Ростов-на-Дону : Феникс, 2005. 314 с.

3. Григорьева Н. В., Карпенко Л. К. Латентность преступлений в сфере компьютерной информации // Донецкие чтения 2017 : Русский мир как цивилизационная основа научно-образовательного и культурного развития Донбасса : материалы Международной научной конференции студентов и молодых ученых. Посвящена 80-летию ДонНУ (Донецк, 17–20 октября 2017 г.) / под общ. ред. С. В. Беспаловой. Донецк : Издательство Донецкого национального университета, 2017. С. 61–63.

4. Жадан И. Э., Мамаева Л. Н. Киберпреступность как угроза международной безопасности // Математическое и компьютерное моделирование в экономике, страховании и управлении рисками. 2020. № 5. С. 166–169.

5. Зарубин С. В. К вопросу об оценке эффективности мероприятий по противодействию информационному терроризму // Вестник Воронежского института МВД России. 2008. № 4. С. 118–122.

6. Карпова Д. Н. Киберпреступность: глобальная проблема и ее решение // Власть. 2014. № 8. С. 46–50.

7. Кобец П. Н. Противодействие терроризму в информационной сфере: опыт и проблемы // Научный портал МВД России. 2021. № 3 (55). С. 18–26.

8. Мамаева Л. Н., Бехер В. В. Угрозы кибербезопасности в цифровом пространстве // Вестник Саратовского государственного социально-экономического университета. 2019. № 4 (78). С. 68–70.

9. Номоконов В. А., Тропина Т. Л. Киберпреступность: прогнозы и проблемы борьбы // Библиотека криминалиста. Научный журнал. 2013. № 5 (10). С. 148–160.

10. Поляков В. В. Профилактика экстремизма и терроризма, осуществляемого с помощью сети Интернет // Известия Алтайского государственного университета. 2016. № 3 (91). С. 142–144. DOI 10.14258/izvasu(2016) 3-26

Дата поступления статьи / Received: 14.03.2022.
Дата рецензирования статьи / Revised: 04.04.2022.
Дата принятия статьи к публикации / Accepted: 10.06.2022.