DOI:
EDN:

Научная статья / Research article

Пути противодействия информационной преступности: состояние и перспективы международного сотрудничества России

Е.Н. Пашенцев, Д.Ю. Базаркина, Е.А. Михалевич
Санкт-Петербургский государственный университет, Санкт-Петербург, Российская Федерация

Аннотация. Актуальность проблемы информационной преступности растет на фоне процессов цифровизации и нарастающего глобального кризиса, усугубленного пандемией коронавирусной инфекции, а затем ситуацией на Украине. Транснациональный характер угрозы, ее стремительное развитие требует тесной координации усилий национальных правительств, международных организаций и интеграционных объединений на международной арене. При этом как в России, так и за рубежом еще не сложилось единого подхода к систематизации информационных преступлений, что снижает возможности международного сотрудничества.

Целью данной статьи является определение спектра действий, подпадающих под понятие информационной преступности, а также оценка возможных институтов и направлений международного сотрудничества России в противодействии информационной преступности.

Системный подход и качественный анализ публикаций международных организаций, национальных правоохранительных структур, научных публикаций, а также материалов СМИ позволяет дать характеристику текущего состояния международного сотрудничества России по направлению противодействия информационной преступности.

Несмотря на то, что понятие «информационная преступность» часто отождествляется с понятием «компьютерная преступность», авторы соглашаются с более широкой трактовкой данного термина. В соответствии с ней, информационные преступления можно разделить на четыре группы: 1) использование информации, информационных технологий (в том числе СМИ) как средства совершения преступления; 2) неправомерный доступ и распространение охраняемой законом информации; 3) неправомерное сокрытие информации; 4) неправомерное использование информации, полученной законным путем. Наибольшая актуальность отмечается для преступлений первой группы, к которой относятся экономические киберпреступления, незаконная торговля оружием, наркотиками, порнографией, оказание других незаконных услуг посредством зашифрованных информационно-телекоммуникационных каналов и сетей, кибертравля (кибербуллинг) и «группы смерти» в социальных сетях, киберэкстремизм.

Рост угроз информационной преступности требует координации борьбы с ней на глобальном уровне через дипломатические, экономические/финансовые, оперативные, правоохранительные, технические и образовательные механизмы. Научная новизна работы заключается в предложении авторами ряда мер на данном направлении: дипломатические меры (вынесение вопросов борьбы с информационной преступностью на повестку дня глобальных и региональных организаций); международное сотрудничество в устранении пробелов в развивающейся экосистеме криптовалюты; международные кампании по срыву преступных операций; инвестирование в информационную и кибергигиену; совместные программы обучения граждан.

Ключевые слова: информационная преступность, киберпреступность, ИКТ, ООН, Интерпол, БРИКС, ШОС, кибербуллинг, киберэкстремизм

Заявление о конфликте интересов. Авторы заявляют об отсутствии конфликта интересов.

Благодарности: Работа выполнена при поддержке СПбГУ, шифр проекта 116471555.
Для цитирования: *Пашенцев Е.Н., Базаркина Д.Ю., Михалевич Е.А.* Пути противодействия информационной преступности: состояние и перспективы международного сотрудничества России // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2024. Т., №. С.. https://doi.org/

Ways to combat information crime: the state and prospects of international cooperation in Russia

Evgeny N. Pashentsev, Darya Yu. Bazarkina, Ekaterina A. Mikhalevich
St. Petersburg State University, Saint Petersburg, Russian Federation

Abstract. The relevance of the problem of information crime is growing against the backdrop of digitalization processes and global crisis aggravated by the coronavirus pandemic, and then the situation in Ukraine. The transnational nature of the threat and its rapid development require close coordination of the efforts of national governments, international organizations and integration associations in the international arena.

The aim of this article is to determine the range of actions that fall under the concept of information crime, as well as to assess possible institutions and areas of international cooperation in Russia in combating information crime.

A systematic approach and qualitative analysis of publications of international organizations, national law enforcement agencies, scientific publications, as well as media materials make it possible to characterize the current state of international cooperation in Russia in the area of combating information crime.

Despite the fact that the concept of "information crime" is often identified with the concept of "computer crime," the authors agree with a broader interpretation of this term. In accordance with it, information crimes can be divided into four groups: 1) the use of information, information technologies as a means of committing a crime; 2) unlawful access and dissemination of information protected by law; 3) unlawful concealment of information; 4) unlawful use of information obtained legally. The greatest relevance is noted for crimes of the first group, which include economic cybercrimes, illegal trade in weapons, cyberbullying, cyber extremism.

The scientific novelty of the work lies in the authors' proposal for a number of measures in this area: diplomatic measures (putting the issues of combating information crime on the agenda of global and regional organizations); international collaboration to address gaps in the evolving cryptocurrency ecosystem; international campaigns to disrupt criminal operations; investing in information and cyber hygiene; joint citizen education programs.

Key words: information crime, cybercrime, ICT, UN, Interpol, BRICS, SCO, cyberbullying, cyber extremism

Conflicts of interest. The authors declared no conflicts of interest.

Acknowledgments: The authors acknowledge Saint-Petersburg State University for a research project 116471555.

For citation: Pashentsev, E. N., Bazarkina, D.Yu., Mikhalevich, E.A. (2024). Ways to combat information crime: the state and prospects of international cooperation in Russia. *Vestnik RUDN. International Relations,*. https://doi.org/

Введение

Актуальность проблемы информационной преступности растет на фоне процессов цифровизации и нарастающего глобального кризиса, усугубленного пандемией коронавирусной инфекции, а затем ситуацией на Украине. Транснациональный характер угрозы, ее стремительное развитие требует тесной координации усилий национальных

правительств, международных организаций и интеграционных объединений на международной арене, а также тесного сотрудничества правительственных структур (включая законодательные и правоохранительные органы), бизнес-субъектов и институтов гражданского общества на национальном и международном уровнях. При этом как в России, так и за рубежом еще не сложилось единого подхода к систематизации информационных преступлений, что снижает возможности международного сотрудничества.

Первостепенную важность сохраняет международное сотрудничество России в рамках СНГ, БРИКС и ШОС. В частности, в июне 2021 г. Совет Федерации России одобрил ратификацию соглашения о сотрудничестве в борьбе с преступлениями в сфере информационных технологий в рамках СНГ. Антитеррористический центр государств — участников Содружества Независимых Государств (АТЦ СНГ) совместно с партнерами – органами безопасности, спецслужбами и правоохранительными органами стран Содружества – на постоянной основе работает на следующих направлениях: 1) совершенствование правовой базы сотрудничества; 2) формирование стратегии согласованной антитеррористической деятельности; 3) координация взаимодействия компетентных органов государств Содружества. В рамках БРИКС продолжает работу проект CyberBRICS. Сотрудничество стран ШОС в сфере информационной безопасности осуществляется с 2006 г. В Декларации двадцатилетия ШОС (Душанбинская декларация 2021 г.) государства-члены резко осудили милитаризацию ИКТ и поддержали запуск разработки под эгидой ООН всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях.

ООН остается одной из важнейших площадок международного сотрудничества. В составе Управления ООН по наркотикам и преступности (ЮНОДК) действует Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях (учрежден 27 декабря 2019 г.). В комитет включен представитель России. В 2019 г. 193 государства-члена ЮНЕСКО поддержали учреждение Международного дня против насилия и буллинга в школе и Интернете. Особую значимость в данной сфере приобретают инициативы технологических и медиакорпораций.

Несмотря на несформированность общего подхода к определению информационной преступности и основных направлений борьбы с ней на глобальном уровне, международное сотрудничество в этой сфере развивается как на уровне ООН или таких специализированных глобальных организаций, как Интерпол, так и в рамках региональных организаций и объединений. Вместе с тем наблюдается определенная неравномерность усилий в противодействии разным видам информационных преступлений. Кроме этого, стоит отметить, что ситуация с сотрудничеством в рамках противодействия информационной преступности ухудшается. Это происходит, во-первых, по мере развития технологий, а во-вторых, по мере усиления военно-политического противоборства на международной арене.

Информационная преступность как транснациональная угроза: определение и современное состояние

Несмотря на то, что понятие «информационная преступность» часто отождествляется с понятием «компьютерная преступность», авторы настоящей статьи прибегают к более широкой трактовке данного термина. В соответствии с ней, информационные преступления можно разделить на четыре группы в зависимости от роли, которую играют в них информация и информационные технологии: 1) использование информации, информационных технологий (в том числе СМИ) как средства совершения преступления; 2) неправомерный доступ и распространение охраняемой законом информации (государственной и коммерческой тайны, персональных данных, сведений о частной жизни лица и т.д.); 3) неправомерное сокрытие информации, в том числе: той, которая должна быть доступна широкому кругу пользователей (например, об обстоятельствах, создающих опасность для жизни или здоровья людей); 4) неправомерное использование информации, полученной законным путем, например: неправомерное использование инсайдерской

информации; незаконный экспорт научно-технической информации; выдача иностранному государству, иностранной или международной организации сведений, составляющих государственную тайну[1]. Наибольшая актуальность отмечается для преступлений первой группы, в которой объектами внимания правоохранителей, политических органов и общественных структур, а также СМИ чаще всего становятся экономические киберпреступления, незаконная торговля оружием, наркотиками, порнографией, а также оказание других незаконных услуг посредством зашифрованных информационно-телекоммуникационных каналов и сетей (в даркнете), кибертравля (кибербуллинг) и «смертельные игры», или «группы смерти», в социальных сетях, киберэкстремизм (вовлечение в террористическую и экстремистскую деятельность, оправдание терроризма, а также кибератаки на критическую инфраструктуру) [2]. Таким образом, понятие «информационная преступность» несколько шире, чем «компьютерная преступность».

В силу несформированности общего международного подхода к информационным преступлениям, практические структуры относят их к разным группам преступной деятельности. К примеру, Интерпол рассматривает торговлю детской порнографией в Интернете в контексте преступлений против детей, выделяет в отдельные направления экономические преступления, в том числе с помощью ИКТ, и киберпреступность[3]. ФБР, в частности, относит похищения детей, в которых преступник общается с будущей жертвой онлайн, к киберугрозам [4]. Киберпреступления в Европейской конвенции о киберпреступности (принята Советом Европы в 2001 г.) классифицируются следующим образом: 1) преступления против конфиденциальности, целостности и доступности компьютерных данных и систем; 2) правонарушения, связанные с использованием компьютерных средств; 3) преступления, связанные с содержанием данных – преступления, связанные с детской порнографией; 4) правонарушения, связанные с нарушением авторского права и смежных прав. Дополнительный протокол к Конвенции включает следующие виды преступлений: 1) распространение расистских и ксенофобских материалов посредством компьютерных систем; 2) мотивированная угроза расизма и ксенофобии; 3) расистское и ксенофобское мотивированное оскорбление; 4) отрицание, чрезвычайная минимизация, одобрение или оправдание геноцида или преступлений против человечества[5], расширяя список преступлений за счет большого количества угроз информационно-психологической безопасности.

В период пандемии COVID-19 уровень киберпреступности в мире возрос на 600%. В 2020 г. 65% организаций в США подверглись фишинговым атакам, на которые приходится 90% утечек корпоративных данных. Преобладание методов социальной инженерии свидетельствует о том, что киберпреступники чаще пользуются эмоциями или халатностью людей, чем атакуют уязвимости компьютерной системы. В частности, растет компрометация корпоративной электронной почты (business email compromise – BEC) – фишинговые атаки, в которых злоумышленник отправляет электронное письмо руководителю высшего звена в крупной компании, чтобы тот перевел средства на банковский счет, контролируемый преступником[6]. Каждый второй подросток в возрасте от 11 до 18 лет в 11 европейских странах, 6 из 10 подростков в возрасте 13-17 лет в США и каждый третий ученик начальной и средней школы в ЮАР сообщили, что подверглись кибербуллингу. 44% опрошенных в 11

---

[1] *Пискунова Е. В.* Информационная преступность: уголовно-правовые и криминалистические аспекты // Государство и право в новой информационной реальности. 2018. № 1. С. 248-266. DOI:10.31249/pras/2018.01.12.

[2] Там же.

[3] The International Criminal Police Organization. 2022. URL: https://www.interpol.int/ (accessed: 19.02.2022).

[4] Cyber Crime. 2022. URL: https://www.fbi.gov/investigate/cyber (accessed: 19.02.2022).

[5] *Якимова Е. М., Нарутто С. В.* Международное сотрудничество в борьбе с киберпреступностью // Всероссийский криминологический журнал. 2016. № 2. С. 369-378.

[6] *Pitchkites M.* Cyber Security Statistics, Facts & Trends in 2022. 2022. URL: https://www.cloudwards.net/cyber-security-statistics/ (accessed: 19.02.2022).

европейских странах подростков, которые подвергались кибербуллингу до пандемии, сообщили о его усилении во время карантина в 2020 г.[7]

После начала СВО число информационных угроз преступлений как в России, так и за ее пределами выросло кратно. На заседании коллегии МИД России 2 апреля 2024 г. Президент РФ Владимир Путин заявил, что в 2023 году в России было совершено около 680 тыс. преступлений с использованием информационных технологий, что на 30% больше, чем годом ранее. Ущерб от них превысил 156 млрд рублей. Общий рост числа зарегистрированных преступлений с использованием ИТ обусловлен большим количеством разнообразных кибератак, совершаемых на информационные системы и инфраструктуру РФ[8].

Все вышеперечисленные явления представляют угрозу как международной безопасности, так и национальной безопасности России. К примеру, в Антитеррористическом центре государств – участников СНГ (АТЦ СНГ) отмечают рост угроз, связанных с использованием ИКТ террористами и экстремистами. Под давлением пандемии COVID–19 террористические группы сместили акценты своей деятельности в онлайн-формат: возрос объем экстремистского контента в социальных сетях, деятельность боевиков координируется дистанционно при помощи соцсетей, мессенджеров, IP-телефонии, для незаконных финансовых операций все чаще задействуются криптовалюты. В качестве источников финансирования терроризма широко применяются инструменты сбора коллективных пожертвований в сети Интернет (механизмы краудфандинга), доходы, получаемые от онлайн-казино, хищения денег через подставные интернет-магазины и сайты-двойники, от фишинговых и фарминг-атак, несанкционированного доступа к банковским ресурсам и криптовалютным биржам, иных видов краж и мошенничества в Интернете, в том числе через смартфоны[9]. Все это становится объективным основанием для углубления сотрудничества в рамках различных международных организаций и интеграционных объединений с целью противодействия информационной преступности.

Институты и направления международного сотрудничества в противодействии информационной преступности: возможности для России

Первостепенную важность сохраняет международное сотрудничество России в рамках СНГ, БРИКС и ШОС. В частности, в июне 2021 г. Совет Федерации России одобрил ратификацию соглашения о сотрудничестве в борьбе с преступлениями в сфере информационных технологий в рамках СНГ. Документ, подписанный в сентябре 2018 г., направлен на создание современных правовых механизмов взаимодействия российских компетентных органов с коллегами из других стран СНГ для эффективного предупреждения,

---

[7] Международный день против насилия в школе и Интернете и проект VK по борьбе с кибербуллингом. 2022. URL: https://iite.unesco.org/ru/news/den-protiv-nasiliya-kiberbulling-unesco-vk/ (дата обращения: 19.02.2022).

[8]Президент РФ Владимир Путин: Ущерб от ИТ-преступлений за год превысил 156 млрд рублей. 2023. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9F%D0%BE%D1%82%D0%B5%D1%80%D0%B8_%D0%BE%D1%82_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D0%B8#.2A_.D0.9F.D1.80.D0.B5.D0.B7.D0.B8.D0.B4.D0.B5.D0.BD.D1.82_.D0.A0.D0.A4_.D0.92.D0.BB.D0.B0.D0.B4.D0.B8.D0.BC.D0.B8.D1.80_.D0.9F.D1.83.D1.82.D0.B8.D0.BD:_.D0.A3.D1.89.D0.B5.D1.80.D0.B1_.D0.BE.D1.82_.D0.98.D0.A2-.D0.BF.D1.80.D0.B5.D1.81.D1.82.D1.83.D0.BF.D0.BB.D0.B5.D0.BD.D0.B8.D0.B9_.D0.B7.D0.B0_.D0.B3.D0.BE.D0.B4_.D0.BF.D1.80.D0.B5.D0.B2.D1.8B.D1.81.D0.B8.D0.BB_156_.D0.BC.D0.BB.D1.80.D0.B4_.D1.80.D1.83.D0.B1.D0.BB.D0.B5.D0.B9 (дата обращения: 20.07.2024).

[9] О деятельности Антитеррористического центра СНГ по координации взаимодействия национальных органов безопасности и специальных служб. 2022. URL: https://e-cis.info/news/566/96729/?sphrase_id=32834 (дата обращения: 19.02.2022).

выявления, пресечения, расследования и раскрытия преступлений в сфере ИКТ[10]. Речь идет о возможном сотрудничестве в обмене информацией о готовящихся или совершенных преступлениях и причастных к ним лицах, о содействии в предоставлении сведений, которые могут помочь в расследовании, а также о скоординированных операциях.

АТЦ СНГ совместно с партнерами – органами безопасности, спецслужбами и правоохранительными органами стран Содружества – на постоянной основе работает на следующих направлениях:

1. Совершенствование правовой базы сотрудничества. АТЦ СНГ подготовлены проекты модельных законов для государств СНГ «О государственной безопасности» и «Об общественной безопасности». Эти законопроекты направлены на рассмотрение в национальные органы безопасности и заинтересованные органы СНГ. Законопроект «Об общественной безопасности» концептуально поддержан на состоявшихся 15 апреля 2021 г. заседаниях Объединенной комиссии при Межпарламентской ассамблее государств – участников СНГ (МПА СНГ) по гармонизации законодательства в сфере безопасности и противодействия новым вызовам и угрозам и Постоянной комиссии по вопросам обороны и безопасности МПА СНГ. Проект модельного закона «О национальной безопасности» одобрен в целом комиссиями МПА СНГ и направлен в парламенты государств-участников для получения экспертных заключений.

2. Формирование стратегии согласованной антитеррористической деятельности АТЦ СНГ осуществляет на заседаниях Совета руководителей органов безопасности и специальных служб государств – участников СНГ. В 2018-2020 гг. АТЦ СНГ заключил меморандумы о взаимопонимании по вопросам сотрудничества и взаимодействия с ООН в лице ее Контртеррористического управления, а также между АТЦ СНГ, Секретариатом ОДКБ и РАТС ШОС. Подписан Протокол о сотрудничестве между АТЦ СНГ и Советом руководителей пенитенциарных служб СНГ.

3. Координация взаимодействия компетентных органов государств Содружества (сборы руководящего состава антитеррористических подразделений органов безопасности и специальных служб государств СНГ, совместные учения). В 2018 и 2019 гг. при проведении учений «Иссык-Куль-Антитеррор-2018» и «Арарат-Антитеррор-2019» отработаны вопросы по выявлению фактов вовлечения в противоправную деятельность негативно настроенной части населения с использованием социальных сетей. Выявлялись информационные платформы, используемые террористами, осуществлялось документирование и последующая блокировка противоправной деятельности. В целях организации совместной деятельности по противодействию финансированию терроризма АТЦ СНГ имеет статус организации-наблюдателя в Евразийской группе по противодействию легализации преступных доходов и финансированию терроризма (ЕАГ). В период 2018–2019 гг. 28 представителей спецслужб прошли под эгидой АТЦ СНГ обучение противодействию финансированию террористической и экстремистской деятельности в Интернете[11] (в 2020 г. запланированное обучение не проводилось в связи со сложной эпидемиологической обстановкой).

Сотрудничество в сфере кибербезопасности и цифрового развития всегда было одним из центральных звеньев механизма сотрудничества БРИКС. Очевидно, что между членами БРИКС существует много противоречий: страны имеют различные подходы к границам информационной открытости, а также к вопросу о пределах допустимого вмешательства систем технического контроля в частную жизнь граждан. Несмотря на то, что сфера ИКТ сегодня характеризуется высокой конкурентностью, основные приоритеты членов БРИКС в безопасном и справедливом развитии данной области, в целом, совпадают.

---

[10] СФ ратифицировал соглашение стран СНГ о сотрудничестве в сфере кибербезопасности. 2022. URL: https://vmeste-rf.tv/news/sf-ratifitsiroval-soglashenie-stran-sng-o-sotrudnichestve-v-sfere-kiberbezopasnosti (дата обращения: 23.02.2022).

[11] О деятельности Антитеррористического центра СНГ по координации взаимодействия национальных органов безопасности и специальных служб. 2022. URL: https://e-cis.info/news/566/96729/?sphrase_id=32834 (дата обращения: 19.02.2022).

Общим знаменателем развивающихся стран-участниц БРИКС в области кибербезопасности является то, что они стремятся сохранить национальный суверенитет, экономическую независимость и социальное единство в своем внутреннем киберпространстве, а также высказываются за построение мирного, стабильного, открытого и инклюзивного международного порядка в общем киберпространстве. Кроме того, у стран БРИКС есть реальные потребности в развитии цифровой экономики и сотрудничества в области безопасности данных, борьбы с киберпреступностью и кибертерроризмом, а также в укреплении технического сотрудничества.

Для России обеспечение безопасности в информационной среде является неотъемлемой частью системы общенациональной безопасности. Этот тезис закреплен в ряде государственных нормативно-правовых актов – в «Концепции внешней политики РФ»[12], «Стратегии развития информационного общества РФ»[13], «Доктрины информационной безопасности РФ»[14] и др.

В борьбе с киберпреступностью и кибертерроризмом у стран БРИКС также есть общие цели и требования. В 2018 году столкнувшись с ухудшением ситуации с международной сетевой безопасностью, Россия и Китай в рамках БРИКС заявили о разработке правовых инструментов, общепризнанных всеми сторонами, для борьбы с преступлениями в области информационных и коммуникационных технологий в рамках ООН. Обе страны приветствуют начало работы специального межправительственного экспертного комитета открытого состава ООН по разработке всеобъемлющей международной конвенции против использования информационных и коммуникационных технологий в преступных целях и продвигают Дорожную карту БРИКС по практическому сотрудничеству в обеспечении безопасного использования информационно-коммуникационных технологий[15]. В рамках саммита БРИКС 2022, Россия и Китай стали организаторами семинаров «Роль цифровой криминалистики в кибертерроризме и антитеррористических расследованиях» и «Цифровая криминалистика БРИКС»[16], тем самым заложив основу для углубления сотрудничества в области цифровой криминалистики.

Важным направлением сотрудничества БРИКС в области обеспечения кибербезопасности стал проект по созданию объединенной киберполиции БРИКС, предложенный на X Саммите БРИКС в 2018 году и закрепленный в итоговой декларации. По мнению члена Научного совета при Совете Безопасности РФ Андрея Манойло, основная идея декларации сосредоточена вокруг сотрудничества государств-членов БРИКС в области обеспечения коллективной безопасности в киберпространстве: «реальные проблемы в плане обеспечения информационной безопасности и защиты от операций информационной войны есть у всех, даже у Китая, стремящегося отгородиться от этих угроз своими «Золотыми щитами» и сравнительно недавно принятым новым законом о кибербезопасности 2016 года, копирующем «пакет Яровой». При всей высокой степени накачанности кибермускулатуры, у России, Китая, Индии, Бразилии и ЮАР по-прежнему остаются проблемы, связанные с

---

[12] Концепция внешней политики Российской Федерации (утверждена Президентом Российской Федерации В. В. Путиным 30 ноября 2016 г.). 2016. URL: https://www.mid.ru/foreign_policy/official_documents//asset_publisher/CptICkB6BZ29/content/id/2542248 (дата обращения: 18.05.2020).

[13] Указ Президента Российской Федерации от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы». 2017. URL: http://kremlin.ru/acts/bank/41919 (дата обращения: 25.05.2020).

[14] Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». 2016. URL: http://kremlin.ru/acts/bank/41460 (дата обращения: 25.05.2020).

[15] XIV BRICS Summit Beijing Declaration. 2022. URL: http://brics2022.mfa.gov.cn/eng/dtxw/202206/t20220624_10709295.html (accessed: 15.07.2024).

[16] Ibid.

обеспечением безопасности и защитой государственного суверенитета, которые в принципе невозможно решить на национальном уровне»[17].

Создание объединенной киберполиции может стать наднациональным коллективным механизмом по предупреждению и предотвращению киберугроз, к которым относят информационный терроризм, информационные войны и хакерские атаки. Проблемным местом является определение подведомственности данной структуры, рамок сферы деятельности и полномочий, вопросы финансирования и управления.

С момента проведения первого официального саммита группы БРИКС 16 июня 2009 года, объединение БРИКС стало важной площадкой для продвижения сотрудничества и развития стран-участниц, особенно сотрудничества в области сетевой безопасности и цифрового развития. Однако под воздействием нынешней обострившейся международной геополитической конкуренции, последствий коронавирусной пандемии и конфликта между Россией и Украиной, глобальное сотрудничество в цифровой сфере сталкивается с большими трудностями, и организация БРИКС не стала исключением. Так, с 2018 года обсуждение проекта объединенной киберполиции БРИКС так и осталось на уровне инициативы. С расширением БРИКС в 2024 г. реализация этой инициативы становится еще более трудной, но не менее значимой.

Тем не менее, в рамках БРИКС продолжает работу проект CyberBRICS, запущенный с целями: «составить карту существующих правил [регулирования киберпространства]; выявить передовой опыт и разработать предложения в сфере политики кибербезопасности (включая регулирование персональных данных), политики доступа в Интернет и стратегий цифровизации государственного управления в странах БРИКС»[18].

Данный проект реализуется Центром технологий и общества при Юридической школе Фонда Жетулиу Варгаса (Бразилия) в партнерстве с Высшей школой экономики (Россия, Москва), Глобальной юридической школой Джиндал и Центром Интернета и общества (Индия), Университетом Фудань Гонконгским университетом (Китай), а также Университетом Нельсона Манделы (Южная Африка).

Проект исходит из того, что в течение следующего десятилетия прогнозируемое распространение и развитие Интернета будет происходить преимущественно в странах Азии, Латинской Америки и Африки и, в частности, в странах БРИКС. В свете этого соображения страны БРИКС расширяют свое сотрудничество в области науки и технологий и содействуют синергии в отношении цифровой политики. Как подчеркивают сами лидеры БРИКС: «Информационно-коммуникационные технологии предоставляют гражданам новые инструменты для эффективного функционирования экономики, общества и государства […]. Использование и развитие ИКТ посредством международного сотрудничества и общепризнанных норм и принципов международного права имеет первостепенное значение для обеспечения мирного, безопасного и открытого цифрового и интернет-пространства»[19].

Хотя расширение возможностей подключения и появление новых информационно-коммуникационных технологий создали новые возможности для физических и юридических лиц, они также создают ряд проблем, особенно в сфере регулирования персональных данных и управления кибербезопасностью. Поэтому CyberBRICS стремится предложить ответы на такие проблемы, предоставляя ценную информацию о цифровой политике БРИКС, основанную на тщательно собранных фактах, которые могут быть использованы как исследователями, регулирующими органами, так и бизнесом. Так, последней опубликованной работой (на 10 мая 2024 г.) участниками проекта является аналитическая

---

[17] *Манойло А.* Сотрудничество стран ШОС и БРИКС в информационной сфере может содействовать росту доверия в отношениях России и Запада. 2018. URL: http://infobrics.org/post/27324 (дата обращения: 27.05.2020).

[18] CyberBRICS. About us. 2022. URL: https://cyberbrics.info/about-us/ (accessed: 20.02.2022).

[19] Ibid.

записка, посвященная цифровому суверенитету[20]. В данном труде цифровой суверенитет определяется как механизм управления ИКТ, при котором государственные правительства имеют суверенное право осуществлять контроль над таковыми в пределах своих границ, включая политическую, экономическую, культурную, технологическую и иные виды деятельности. При этом данная концепция не предполагает разделение общего киберпространства на отдельные сегменты, а способствует созданию безопасного «киберсообщества с общей судьбой», в котором государства смогут осуществлять свои права по управлению Интернетом на принципах равенства, справедливости, сотрудничества, мира и верховенства права, не боясь вмешательства извне.

Сотрудничество стран ШОС в сфере информационной безопасности осуществляется с 2006 г. В Декларации двадцатилетия ШОС (Душанбинская декларация 2021 г.) государства-члены резко осудили милитаризацию ИКТ и поддержали запуск разработки под эгидой ООН всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях[21].

ООН остается одной из важнейших площадок международного сотрудничества. В составе Управления ООН по наркотикам и преступности (ЮНОДК) действует Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях. Комитет учрежден Резолюцией 74/247 [22] Генеральной Ассамблеи ООН от 27 декабря 2019 г. Это межправительственный комитет экспертов из всех регионов мира. Организационная сессия состоялась 10-12 мая 2021 г. в Нью-Йорке. В резолюции 75/282 от 26 мая 2021 г. «Противодействие использованию информационно-коммуникационных технологий в преступных целях» Генеральная Ассамблея ООН постановила, в частности, что Специальный комитет должен созвать не менее шести сессий продолжительностью 10 дней каждая, начиная с первой сессии в Нью-Йорке (28 февраля-11 марта 2022 г.), и по итогам их представить проект конвенции Генеральной Ассамблее на ее 78-й сессии[23]. Помимо того, что в комитет уже включен представитель России, Резолюция 75/282 рекомендует[24] председателю комитета запрашивать мнения у различных заинтересованных сторон и подтверждает, что представители неправительственных организаций, имеющих консультативный статус при Экономическом и социальном совете (ЭКОСОС) ООН, могут зарегистрироваться в секретариате для участия в сессиях. В документе излагаются условия участия (на принципах справедливой географической представленности) других неправительственных организаций, научных учреждений и бизнес-структур, в том числе имеющих опыт борьбы с киберпреступностью.

В 2019 г. 193 государства-члена ЮНЕСКО поддержали учреждение Международного дня против насилия и буллинга в школе и Интернете. Основной темой Международного дня в 2021 г. стал поиск возможностей для предотвращения кибербуллинга и других форм онлайн-насилия в отношении детей и молодежи. Особую значимость в данной сфере приобретают инициативы технологических и медиакорпораций. Запущенный при поддержке российской технологической корпорации VK портал kiberbulling.net информирует

---

[20] Demambro J. Digital Sovereignty In The BRICS: Structuring Self-Determination, Cybersecurity, And Control. 2024. URL: https://cyberbrics.info/digital-sovereignty-from-the-brics-structuring-self-determination-cybersecurity-and-control/ (accessed: 10.05.2024).

[21] Душанбинская декларация двадцатилетия ШОС от 17 сентября 2021 г. 2021. URL: http://rus.sectsco.org/load/779610/ (дата обращения: 20.02.2022).

[22] Резолюция, принятая Генеральной Ассамблеей 27 декабря 2019 года 74/247. Противодействие использованию информационно-коммуникационных технологий в преступных целях. 2019. URL: https://undocs.org/ru/A/Res/74/247 (дата обращения: 19.02.2022).

[23] Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. 2022. URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home (accessed: 19.02.2022).

[24] Резолюция, принятая Генеральной Ассамблеей 26 мая 2021 года 75/282. Противодействие использованию информационно-коммуникационных технологий в преступных целях. 2021. URL: https://undocs.org/ru/A/Res/74/247 (дата обращения: 19.02.2022).

аудиторию русскоязычного Интернета о недопустимости кибербуллинга, его последствиях, и о том, куда можно обратиться за помощью[25].

Интерпол создал две платформы связи между полицией и другими акторами, вовлеченными в борьбу с киберпреступностью. Рабочее пространство обмена знаниями о киберпреступности (Cybercrime Knowledge Exchange (CKE) workspace) открыто для правоохранительных органов, правительств, международных организаций и экспертов в области кибербезопасности для обмена оперативной информацией (не принадлежащей полиции) о киберпреступлениях. CKE будет способствовать созданию международной сети профильных экспертов для обмена знаниями. Присоединиться к CKE приглашены сотрудники правоохранительных органов и национальных центральных бюро (НЦБ) Интерпола. Международные организации и частные компании могут запросить присоединение к CKE, обратившись в Управление Интерпола по киберпреступности. Платформа для совместной работы по борьбе с киберпреступностью – Операции (Cybercrime Collaborative Platform – Operation, CCP – Operation) – первый в своем роде централизованный информационный центр для координации глобальных операций правоохранителей по борьбе с киберпреступностью. Платформа призвана предоставить специалистам-практикам более широкую картину киберугроз и помочь эффективнее сосредоточить ресурсы и избежать дублирования усилий. В силу конфиденциального характера информации, которой обмениваются через CCP – Operation, доступ к этой платформе ограничен. Проверенные участники из НЦБ Интерпола и правоохранительных органов, а также международных или региональных организаций и частных компаний, с которыми Интерпол имеет соглашения о сотрудничестве, получают доступ к конкретным частям базы для поддержки конкретных операций Интерпола[26].

Интерпол также наращивает сотрудничество со странами Азии. Так, в июне 2024 г. в Тяньцзине (Китай) состоялось офлайн-совещание глобальной кампании Интерпола по борьбе с электронным мошенничеством «Операция Рассвет-2024» с целью укрепления международного сотрудничества правоохранительных органов Интерпола и азиатских стран. На встрече представители Интерпола и 11 стран и регионов, включая Китай, Австралию и Намибию обменялись мнениями и выступлениями по вопросам борьбы с мошенничеством в Интернете, провели круглые столы и дискуссии по укреплению сотрудничества между правоохранительными органами по борьбе с транснациональной преступностью. «Операция Рассвет-2024» была направлена на раскрытие и предотвращение трансграничных преступлений в киберпространстве. На протяжении нескольких лет Тяньцзиньское бюро общественной безопасности сотрудничало со многими странами Юго-Восточной Азии на уровне правоохранительных органов. На встрече отмечалось, что в течение операции китайские оперативники совершили 11 выездов заграницу с целью участия в акциях по задержанию информационных преступников в 5 странах и регионах, в том числе на Филиппинах, в Лаосе, Испании, Индонезии и северной Мьянме. 9 китайских чартерных рейсов доставили 522 иностранных преступника в Тяньцзинь, что было отмечено как положительный результат в ходе операции[27].

В то же время отношения России с Интерполом накаляются, а сотрудничество рискует быть полностью прекращенным. Несмотря на то, что статья 2 Устава Интерпола призывает поддерживать сотрудничество между странами организации и обеспечивать

---

[25] Международный день против насилия в школе и Интернете и проект VK по борьбе с кибербуллингом. 2022. URL: https://iite.unesco.org/ru/news/den-protiv-nasiliya-kiberbulling-unesco-vk/ (дата обращения: 19.02.2022).

[26] Cybercrime Collaboration Services. 2022. URL: https://www.interpol.int/Crimes/Cybercrime/Cybercrime-Collaboration-Services (accessed: 19.02.2022).

[27] 国际刑警组织打击电诈犯罪全球行动 “曙光行动 2024”线下总结会在津成功举办 [The International Interpol Organization to fight the global action of electrical fraud "Dawn Action 2024" offline summary meeting was successfully held in Jinjin]. 2024. URL: https://www.thepaper.cn/newsDetail_forward_27882775 (accessed: 28.07.2024).

открытость каналов связи, а Мандат Интерпола не включает в себя положения о введении санкций, принятии карательных мер, приостановлении или исключении страны-члена[28], тем не менее постоянно звучат политические призывы по исключению России из Интерпола после начала СВО[29].

Президент «Международного бюро расследований», профессор Ю. Жданов отмечает, что после начала боевых действий в Украине взаимное сотрудничество правоохранителей разных стран весьма осложнилось. Для России это заключается в пристрастном контроле всех запросов об организации международного розыска, а также в проведении аудита предыдущих запросов России с целью обнаружить в них политическую составляющую. «Интерпол демонстрирует свою ангажированность блоку западных стран и тем самым подрывает декларируемый Организацией нейтралитет», – заключает Ю. Жданов[30].

Представитель МИД РФ М. Захарова отмечает, что от исключения России из Интерпола пострадают, в первую очередь, обычные люди: «Кто страдает? Страдают обыватели в первую очередь на европейском континенте в целом, потому что не могут правоохранители отслеживать соответствующую информацию. Почему это делается? Только потому, что есть политизированный заказ...»[31].

Очевидно, что на данном направлении для России в настоящее время больше ограничений, чем возможностей. Потенциальное исключение России из Интерпола может стать беспрецедентным событием, оценить последствия которого в полном объеме не представляется возможным.

Помимо межгосударственных площадок, существуют возможности международного сотрудничества бизнес-субъектов в борьбе с информационной преступностью. Так, Виртуальная глобальная оперативная группа (The Virtual Global Taskforce – VGT), международный альянс правоохранительных органов, работает с неправительственными организациями и отраслевыми партнерами в области защиты детей от сексуальной эксплуатации в Интернете и других преступлений на сексуальной почве в отношении детей. Одна из задач VGT – обмен информацией с частными компаниями. Хотя Россия не входит в число государств-членов организации, с VGT опосредованно сотрудничает российское отделение ТНК “Accor Hotels” (“Accor Russia – Russian Management Hotel Company LLC”), подписавшее Кодекс поведения для защиты детей от сексуальной эксплуатации в сфере путешествий и туризма (The Code of Conduct for the Protection of Children from Sexual Exploitation in Travel and Tourism)[32].

Кроме этого, международное сотрудничество выстраивается на проектном уровне при проведении совместных операций. Так, в конце марта 2024 г. была запущена глобальная совместная операция «Скайнет-2024», целью которой является интеграция глобальных правоохранительных ресурсов для борьбы с транснациональной преступностью. Союзники считают, что операция укрепит обмен разведданными, совместные расследования,

---

[28] Ukraine: INTERPOL General Secretariat statement. 2022. URL: https://www.interpol.int/News-and-Events/News/2022/Ukraine-INTERPOL-General-Secretariat-statement (accessed: 28.06.2024).

[29] В МВД заявили о «закулисных дебатах» об исключении России из Интерпола. 2023. URL: https://www.rbc.ru/politics/07/09/2023/64f91d6a9a7947d6241c4bbb (дата обращения: 18.06.2024);

MEPs ask to exclude Russia from Interpol. (2023). URL: https://ecrgroup.eu/article/meps_ask_to_exclude_russia_from_interpol (accessed: 10.06.2024);

Russia Wrongly Escapes Suspension From Interpol. 2022. URL: https://www.heritage.org/global-politics/commentary/russia-wrongly-escapes-suspension-interpol (accessed: 19.06.2024).

[30] Что стало с сотрудничеством России и Интерпола на фоне украинского конфликта. 2023. URL: https://www.mk.ru/politics/2023/07/29/chto-stalo-s-sotrudnichestvom-rossii-i-interpola-na-fone-ukrainskogo-konflikta.html?ysclid=lxxdm6m63083590987 (дата обращения: 20.06.2024).

[31] От исключения России из Интерпола пострадают обычные люди, заявил МИД. 2024. URL: https://ria.ru/20240626/interpol-1955644906.html (дата обращения: 28.06.2024).

[32] The Code of Conduct for the Protection of Children from Sexual Exploitation in Travel and Tourism. 2022. URL: https://thecode.org/ourmembers/ (accessed: 19.02.2022).

использование современных технологий для повышения эффективности работы правоохранительных органов[33].

Заключение и рекомендации

Несмотря на несформированность общего подхода к определению информационной преступности и основных направлений борьбы с ней на глобальном уровне, международное сотрудничество в этой сфере развивается как на уровне ООН или таких специализированных глобальных организаций, как Интерпол, так и в рамках региональных организаций и объединений. Вместе с тем наблюдается определенная неравномерность усилий в противодействии разным видам информационных преступлений. Так, если пресечение экономических правонарушений, киберэкстремизма или злоупотреблений персональными данными пользователей чаще становятся предметом скоординированных усилий в рамках крупных межправительственных инициатив, то такие задачи, как борьба с кибербуллингом, решаются преимущественно в рамках сотрудничества гражданского общества и бизнес-субъектов. В то же время в контексте обеспечения информационно-психологической безопасности всем этим угрозам необходимо уделять пристальное внимание как факторам дальнейшего роста преступности и напряженности в обществе.

Рост угроз информационной преступности требует координации борьбы с ней на глобальном уровне через дипломатические, экономические/финансовые, оперативные, правоохранительные, технические и образовательные механизмы. На этих направлениях можно предложить ряд мер.

1. Дипломатические меры: вынесение вопросов борьбы с информационной преступностью на повестку дня глобальных и региональных организаций (ООН, БРИКС, ШОС и др.). В 2022 г. важной площадкой для обсуждения международного сотрудничества в борьбе с информационной преступностью представляются заседания Специального комитета ООН по разработке всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях.
2. Международное сотрудничество в устранении пробелов в развивающейся экосистеме криптовалюты. Криптовалютный сектор, которым пользуются экономические киберпреступники, должен регулироваться более строго. Органы государственной власти должны создавать условия, в которых такие механизмы, как криптовалютные биржи, будут работать в рамках правового поля, в том числе повышая прозрачность своей деятельности и принимая участие в борьбе с финансированием преступности и терроризма.
3. Международные согласованные кампании по срыву преступных операций, нацеленные на партнерские сети, посредников и самих исполнителей информационных преступлений. Усилия также должны быть сосредоточены на разрушении преступной инфраструктуры.
4. Инвестирование в информационную и кибергигиену – легкодоступные и бесплатные базовые инструменты, помогающие предотвратить или ограничить масштаб ущерба в случае информационного преступления, сделать его более дорогостоящим для злоумышленника. Международные усилия по распространению этих инструментов могут создать новую область сотрудничества.
5. Совместные программы обучения граждан, повышение их осведомленности о мотивах и способах совершения информационных преступлений.

Кибербезопасность является деликатным вопросом, затрагивающим основные интересы безопасности и развития всех стран, а соответствующее сотрудничество требует глубокого консенсуса и стратегического взаимного доверия.

---

[33] 全球瞩目！“天网 2024”行动正式开启，跨国犯罪将无处遁形 [Global attention! The "Skynet 2024" operation is officially opened, and multinational crimes will have nowhere to hide]. 2024. URL: https://baijiahao.baidu.com/s?id=1793967147369027642&wfr=spider&for=pc (accessed: 28.07.2024).

Поступила в редакцию / Received:
Принята к публикации / Accepted:

Библиографический список

В МВД заявили о «закулисных дебатах» об исключении России из Интерпола. 2023. URL: https://www.rbc.ru/politics/07/09/2023/64f91d6a9a7947d6241c4bbb (дата обращения: 18.06.2024).

Душанбинская декларация двадцатилетия ШОС от 17 сентября 2021 г. 2021. URL: http://rus.sectsco.org/load/779610/ (дата обращения: 20.02.2022).

Концепция внешней политики Российской Федерации (утверждена Президентом Российской Федерации В. В. Путиным 30 ноября 2016 г.). 2016. URL: https://www.mid.ru/foreign_policy/official_documents//asset_publisher/CptICkB6BZ29/content/id/2542248 (дата обращения: 18.05.2020).

Крутских А., Хамидуллин А. Мировое сообщество стало на шаг ближе к «вакцине» от киберпреступностию. 2021. URL: https://interaffairs.ru/news/show/31003 (дата обращения: 19.07.2024).

Манойло А. Сотрудничество стран ШОС и БРИКС в информационной сфере может содействовать росту доверия в отношениях России и Запада. 2018. URL: http://infobrics.org/post/27324 (дата обращения: 27.05.2020).

Международный день против насилия в школе и Интернете и проект VK по борьбе с кибербуллингом. 2022. URL: https://iite.unesco.org/ru/news/den-protiv-nasiliya-kiberbulling-unesco-vk/ (дата обращения: 19.02.2022).

О деятельности Антитеррористического центра СНГ по координации взаимодействия национальных органов безопасности и специальных служб. 2022. URL: https://e-cis.info/news/566/96729/?sphrase_id=32834 (дата обращения: 19.02.2022).

От исключения России из Интерпола пострадают обычные люди, заявил МИД. 2024. URL: https://ria.ru/20240626/interpol-1955644906.html (дата обращения: 28.06.2024).

Пискунова Е. В. Информационная преступность: уголовно-правовые и криминалистические аспекты // Государство и право в новой информационной реальности. 2018. № 1. С. 248-266. DOI:10.31249/pras/2018.01.12.

Президент РФ Владимир Путин: Ущерб от ИТ-преступлений за год превысил 156 млрд рублей. 2023. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9F%D0%BE%D1%82%D0%B5%D1%80%D0%B8_%D0%BE%D1%82_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D0%B8#.2A_.D0.9F.D1.80.D0.B5.D0.B7.D0.B8.D0.B4.D0.B5.D0.BD.D1.82_.D0.A0.D0.A4_.D0.92.D0.BB.D0.B0.D0.B4.D0.B8.D0.BC.D0.B8.D1.80_.D0.9F.D1.83.D1.82.D0.B8.D0.BD:_.D0.A3.D1.89.D0.B5.D1.80.D0.B1_.D0.BE.D1.82_.D0.98.D0.A2-.D0.BF.D1.80.D0.B5.D1.81.D1.82.D1.83.D0.BF.D0.BB.D0.B5.D0.BD.D0.B8.D0.B9_.D0.B7.D0.B0_.D0.B3.D0.BE.D0.B4_.D0.BF.D1.80.D0.B5.D0.B2.D1.8B.D1.81.D0.B8.D0.BB_156_.D0.BC.D0.BB.D1.80.D0.B4_.D1.80.D1.83.D0.B1.D0.BB.D0.B5.D0.B9 (дата обращения: 20.07.2024).

Резолюция, принятая Генеральной Ассамблеей 27 декабря 2019 года 74/247. Противодействие использованию информационно-коммуникационных технологий в преступных целях. 2019. URL: https://undocs.org/ru/A/Res/74/247 (дата обращения: 19.02.2022).

Резолюция, принятая Генеральной Ассамблеей 26 мая 2021 года 75/282. Противодействие использованию информационно-коммуникационных технологий в преступных целях. 2021. URL: https://undocs.org/ru/A/Res/74/247 (дата обращения: 19.02.2022).

СФ ратифицировал соглашение стран СНГ о сотрудничестве в сфере кибербезопасности. 2022. URL: https://vmeste-rf.tv/news/sf-ratifitsiroval-soglashenie-stran-sng-o-sotrudnichestve-v-sfere-kiberbezopasnosti (дата обращения: 23.02.2022).

Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». 2016. URL: http://kremlin.ru/acts/bank/41460 (дата обращения: 25.05.2020).

Указ Президента Российской Федерации от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы». 2017. URL: http://kremlin.ru/acts/bank/41919 (дата обращения: 25.05.2020).

Что стало с сотрудничеством России и Интерпола на фоне украинского конфликта. 2023. URL: https://www.mk.ru/politics/2023/07/29/chto-stalo-s-sotrudnichestvom-rossii-i-interpola-na-fone-ukrainskogo-konflikta.html?ysclid=lxxdm6m63083590987 (дата обращения: 20.06.2024).

Якимова Е. М., Нарутто С. В. Международное сотрудничество в борьбе с киберпреступностью // Всероссийский криминологический журнал. 2016. № 2. С. 369-378.

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. 2022. URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home (accessed: 19.02.2022).

CyberBRICS. About us. 2022. URL: https://cyberbrics.info/about-us/ (accessed: 20.02.2022).

Cyber Crime. 2022. URL: https://www.fbi.gov/investigate/cyber (accessed: 19.02.2022).

Cybercrime Collaboration Services. 2022. URL: https://www.interpol.int/Crimes/Cybercrime/Cybercrime-Collaboration-Services (accessed: 19.02.2022).

Demambro J. Digital Sovereignty In The BRICS: Structuring Self-Determination, Cybersecurity, And Control. 2024. URL: https://cyberbrics.info/digital-sovereignty-from-the-brics-structuring-self-determination-cybersecurity-and-control/ (accessed: 10.05.2024).

MEPs ask to exclude Russia from Interpol. 2023. URL: https://ecrgroup.eu/article/meps_ask_to_exclude_russia_from_interpol (accessed: 10.06.2024).

Pitchkites M. Cyber Security Statistics, Facts & Trends in 2022. 2022. URL: https://www.cloudwards.net/cyber-security-statistics/ (accessed: 19.02.2022).

Ransomware Task Force. 2022. URL: https://securityandtechnology.org/ransomwaretaskforce/ (accessed: 20.02.2022).

Reiner P. J. Greater Harm Is Not Inevitable: How Global Collaboration Can Reduce Ransomware Threat. Digital Debates, 2021. № 8. Pp. 8-15.

Russia Wrongly Escapes Suspension From Interpol. 2022. URL: https://www.heritage.org/global-politics/commentary/russia-wrongly-escapes-suspension-interpol (accessed: 19.06.2024).

The Code of Conduct for the Protection of Children from Sexual Exploitation in Travel and Tourism. 2022. URL: https://thecode.org/ourmembers/ (accessed: 19.02.2022).

The International Criminal Police Organization. 2022. URL: https://www.interpol.int/ (accessed: 19.02.2022).

Ukraine: INTERPOL General Secretariat statement. 2022. URL: https://www.interpol.int/News-and-Events/News/2022/Ukraine-INTERPOL-General-Secretariat-statement (accessed: 28.06.2024).

XIV BRICS Summit Beijing Declaration. 2022. URL: http://brics2022.mfa.gov.cn/eng/dtxw/202206/t20220624_10709295.html (accessed: 15.07.2024).

国际刑警组织打击电诈犯罪全球行动 “曙光行动 2024”线下总结会在津成功举办 [The International Interpol Organization to fight the global action of electrical fraud "Dawn

Action 2024" offline summary meeting was successfully held in Jinjin]. 2024. URL: https://www.thepaper.cn/newsDetail_forward_27882775 (accessed: 28.07.2024).
全球瞩目！“天网 2024”行动正式开启，跨国犯罪将无处遁形 [Global attention! The "Skynet 2024" operation is officially opened, and multinational crimes will have nowhere to hide]. 2024. URL: https://baijiahao.baidu.com/s?id=1793967147369027642&wfr=spider&for=pc (accessed: 28.07.2024).

References

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. (2022). URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home (accessed: 19.02.2022).

CyberBRICS. About us. (2022). URL: https://cyberbrics.info/about-us/ (accessed: 20.02.2022).

Cyber Crime. (2022). URL: https://www.fbi.gov/investigate/cyber (accessed: 19.02.2022).

Cybercrime Collaboration Services. (2022). URL: https://www.interpol.int/Crimes/Cybercrime/Cybercrime-Collaboration-Services (accessed: 19.02.2022).

Decree of the President of the Russian Federation dated December 5, 2016 No. 646 “On approval of the Information Security Doctrine of the Russian Federation.” (2016). URL: http://kremlin.ru/acts/bank/41460 (accessed: 25.05.2020). (In Russian).

Decree of the President of the Russian Federation dated May 9, 2017 No. 203 “On the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030.” (2017). URL: http://kremlin.ru/acts/bank/41919 (accessed: 25.05.2020). (In Russian).

Demambro, J. Digital Sovereignty In The BRICS: Structuring Self-Determination, Cybersecurity, And Control. 2024. URL: https://cyberbrics.info/digital-sovereignty-from-the-brics-structuring-self-determination-cybersecurity-and-control/ (accessed: 10.05.2024).

Dushanbe Declaration of the twentieth anniversary of the SCO of September 17, 2021. (2021). URL: http://rus.sectsco.org/load/779610/ (accessed: 20.02.2022). (In Russian).

International Day against Violence at School and the Internet and the VK project to combat cyberbullying. (2022). URL: https://iite.unesco.org/ru/news/den-protiv-nasiliya-kiberbulling-unesco-vk/ (accessed: 19.02.2022. (In Russian).

Krutskikh, A., Khamidullin, A. (2021). *The world community has become one step closer to a “vaccine” against cybercrime.* URL: https://interaffairs.ru/news/show/31003 (accessed: 19.07.2024). (In Russian).

Manoilo, A. (2018). *Cooperation between the SCO and BRICS countries in the information sphere can contribute to the growth of trust in relations between Russia and the West*. URL: http://infobrics.org/post/27324 (accessed: 27.05.2020). (In Russian).

MEPs ask to exclude Russia from Interpol. (2023). URL: https://ecrgroup.eu/article/meps_ask_to_exclude_russia_from_interpol (accessed: 10.06.2024).

On the activities of the CIS Anti-Terrorism Center to coordinate the interaction of national security agencies and special services. (2022). URL: https://e-cis.info/news/566/96729/?sphrase_id=32834 (accessed: 19.02.2022). (In Russian).

Ordinary people will suffer from the exclusion of Russia from Interpol, the Foreign Ministry said. (2024). URL: https://ria.ru/20240626/interpol-1955644906.html (accessed: 28.06.2024). (In Russian).

Piskunova, E. V. (2018). Information crime: criminal law and forensic aspects // State and law in the new information reality. № 1. Pp. 248-266. DOI:10.31249/pras/2018.01.12. (In Russian).

Pitchkites M. (2022). Cyber Security Statistics, Facts & Trends in 2022. URL: https://www.cloudwards.net/cyber-security-statistics/ (accessed: 19.02.2022).

Ransomware Task Force. (2022). URL: https://securityandtechnology.org/ransomwaretaskforce/ (accessed: 20.02.2022).

Reiner P. J. (2021). Greater Harm Is Not Inevitable: How Global Collaboration Can Reduce Ransomware Threat. *Digital Debates*, 2021. № 8. Pp. 8-15.

Resolution adopted by the General Assembly on December 27, 2019 74/247. Countering the use of information and communication technologies for criminal purposes. (2019). URL: https://undocs.org/ru/A/Res/74/247 (accessed: 19.02.2022). (In Russian).

Resolution adopted by the General Assembly on May 26, 2021 75/282. Countering the use of information and communication technologies for criminal purposes. (2021). URL: https://undocs.org/ru/A/Res/74/247 (accessed: 19.02.2022). (In Russian).

Russian President Vladimir Putin: Damage from IT crimes for the year exceeded 156 billion rubles. (2023). URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9F%D0%BE%D1%82%D0%B5%D1%80%D0%B8_%D0%BE%D1%82_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D0%B8#.2A_.D0.9F.D1.80.D0.B5.D0.B7.D0.B8.D0.B4.D0.B5.D0.BD.D1.82_.D0.A0.D0.A4_.D0.92.D0.BB.D0.B0.D0.B4.D0.B8.D0.BC.D0.B8.D1.80_.D0.9F.D1.83.D1.82.D0.B8.D0.BD:_.D0.A3.D1.89.D0.B5.D1.80.D0.B1_.D0.BE.D1.82_.D0.98.D0.A2-.D0.BF.D1.80.D0.B5.D1.81.D1.82.D1.83.D0.BF.D0.BB.D0.B5.D0.BD.D0.B8.D0.B9_.D0.B7.D0.B0_.D0.B3.D0.BE.D0.B4_.D0.BF.D1.80.D0.B5.D0.B2.D1.8B.D1.81.D0.B8.D0.BB_156_.D0.BC.D0.BB.D1.80.D0.B4_.D1.80.D1.83.D0.B1.D0.BB.D0.B5.D0.B9 (accessed: 20.07.2024). (In Russian).

Russia Wrongly Escapes Suspension From Interpol. (2022). URL: https://www.heritage.org/global-politics/commentary/russia-wrongly-escapes-suspension-interpol (accessed: 19.06.2024).

The Code of Conduct for the Protection of Children from Sexual Exploitation in Travel and Tourism. (2022). URL: https://thecode.org/ourmembers/ (accessed: 19.02.2022).

The concept of foreign policy of the Russian Federation (approved by the President of the Russian Federation V.V. Putin on November 30, 2016. (2016). URL: https://www.mid.ru/foreign_policy/official_documents//asset_publisher/CptICkB6BZ29/content/id/2542248 (accessed: 18.05.2020). (In Russian).

The Federation Council ratified the agreement of the CIS countries on cooperation in the field of cybersecurity. (2022). URL: https://vmeste-rf.tv/news/sf-ratifitsiroval-soglashenie-stran-sng-o-sotrudnichestve-v-sfere-kiberbezopasnosti (accessed: 23.02.2022). (In Russian).

The International Criminal Police Organization. (2022). URL: https://www.interpol.int/ (accessed: 19.02.2022).

The Ministry of Internal Affairs announced the "backstage debate" about the exclusion of Russia from Interpol. (2023). URL: https://www.rbc.ru/politics/07/09/2023/64f91d6a9a7947d6241c4bbb (accessed: 18.06.2024). (In Russian).

Ukraine: INTERPOL General Secretariat statement. 2022. URL: https://www.interpol.int/News-and-Events/News/2022/Ukraine-INTERPOL-General-Secretariat-statement (accessed: 28.06.2024).

What happened to the cooperation of Russia and Interpol against the backdrop of the Ukrainian conflict. (2023). URL: https://www.mk.ru/politics/2023/07/29/chto-stalo-s-sotrudnichestvom-rossii-i-interpola-na-fone-ukrainskogo-konflikta.html?ysclid=lxxdm6m63083590987 (accessed: 20.06.2024). (In Russian).

Yakimova, E. M., Narutto, S. V. (2016). International cooperation in the fight against cybercrime // *All-Russian Criminological Journal.* № 2. Pp. 369-378. (In Russian).

XIV BRICS Summit Beijing Declaration. (2022). URL: http://brics2022.mfa.gov.cn/eng/dtxw/202206/t20220624_10709295.html (accessed: 15.07.2024).

国际刑警组织打击电诈犯罪全球行动 “曙光行动 2024”线下总结会在津成功举办 [The International Interpol Organization to fight the global action of electrical fraud "Dawn

Action 2024" offline summary meeting was successfully held in Jinjin]. 2024. URL: https://www.thepaper.cn/newsDetail_forward_27882775 (accessed: 28.07.2024). (In Chinese).

全球瞩目！“天网 2024”行动正式开启，跨国犯罪将无处遁形 [Global attention! The "Skynet 2024" operation is officially opened, and multinational crimes will have nowhere to hide]. (2024). URL: https://baijiahao.baidu.com/s?id=1793967147369027642&wfr=spider&for=pc (accessed: 28.07.2024). (In Chinese).

Сведения об авторах:

Пашенцев Евгений Николаевич – д.и.н., профессор, ведущий научный сотрудник Института актуальных международных проблем Дипломатической академии Министерства иностранных дел Российской Федерации; профессор факультета международных отношений Санкт-Петербургского государственного университета; Россия, 191060, г. Санкт-Петербург, ул. Смольного 1/3, подъезд 8; icspsc@mail.ru; ORCID: 0000-0001-5487-4457. *Личный номер телефона +79164582101 (не для публикации!)*

Базаркина Дарья Юрьевна – д.полит.н., ведущий научный сотрудник Отдела исследований европейской интеграции Института Европы Российской академии наук и факультета международных отношений Санкт-Петербургского государственного университета; Россия, 191060, г. Санкт-Петербург, ул. Смольного 1/3, подъезд 8; bazarkina-icspsc@yandex.ru; ORCID: 0000-0002-8421-5396. *Личный номер телефона +79151561508 (не для публикации!)*

Михалевич Екатерина Андреевна – главный специалист Управления организационного развития ПАО «Газпром нефть»; инженер-исследователь факультета международных отношений Санкт-Петербургского государственного университета; Россия, 191060, г. Санкт-Петербург, ул. Смольного 1/3, подъезд 8; ekaterina_mikhalevich@mail.ru; ORCID: 0000-0003-0703-4134. *Личный номер телефона +79245810074 (не для публикации!)*