DOI: 10.31857/S032150750019782-2 *Оригинальная статья / Original article*

Сотрудничество Китая и России в области кибербезопасности

© Хань Шиин[a], 2022

[a] Московский государственный университет им. М.В.Ломоносова, Москва, Россия
ORCID ID: 0000-0001-5799-7217; hanshiying@bfsu.edu.cn

Резюме. Развитие современных компьютерных технологий привело к увеличению угроз кибербезопасности как для Китая, так и для России. Несмотря на то, что обе страны уже обнародовали ряд законов и правил по укреплению кибербезопасности, из-за безграничности и открытости киберпространства решить все проблемы силами только одной страны весьма сложно. Необходимо сотрудничать и действовать сообща для достижения желаемого эффекта.

В настоящее время сотрудничество между Китаем и Россией осуществляется как в двустороннем формате, так и в рамках международных организаций и многосторонних структур. Многостороннее сотрудничество осуществляется в рамках ШОС и стран БРИКС. ШОС более склонна к сотрудничеству в борьбе с кибертерроризмом, а страны БРИКС больше интересуются сотрудничеством в области обеспечения информационной безопасности. Двустороннее сотрудничество началось относительно поздно, но две страны уже установили обмены и каналы связи.

В целом, механизмы для китайско-российского сотрудничества в области кибербезопасности уже созданы. Однако существуют определенные ограничения в сотрудничестве, и следует повышать степень взаимного доверия между двумя странами. Тем не менее, по сравнению с отношениями США со своими союзниками, Китай и Россия уделяют больше внимания равенству и взаимному уважению. Таким образом, сотрудничество между двумя сторонами представляет собой долгосрочную или устойчивую тенденцию.

Ключевые слова: Китай, Россия кибербезопасность, кибертерроризм, БРИКС, ШОС

Для цитирования: Хань Шиин (КНР). Сотрудничество Китая и России в области кибербезопасности. *Азия и Африка сегодня*. 2022. № 8. С. 66-72. DOI: 10.31857/S032150750019782-2

Sino-Russian cyber security cooperation

© Han Shiying[a], 2022

[a] Lomonosov Moscow State University, Moscow, Russia
ORCID ID: 0000-0001-5799-7217; hanshiying@bfsu.edu.cn

Abstract. With mounting cyber conflicts, cyber crimes and other security threats in the wake of technological advancement, Russia and China have suffered from malicious cyber attacks, data insecurity, cyberterrorism, among others. Despite domestic efforts in regulation and releasing a series of laws on cyber security, both nations still find it difficult to solve all cyber security issues, because the cyber space itself is highly open, extends beyond borders and has no boundaries. As such, mutual cooperation is needed to yield the expected results.

So far China and Russia have mainly conducted multilateral and bilateral cooperation. The former is done under the SCO and BRICS frameworks, of which SCO emphasizes on cooperation to prevent cyberterrorism, and BRICS leans towards cooperation on data security. Though bilateral cooperation has witnessed a later start, it has achieved some results, mainly in establishing a communication channel to mutually respond to international information safety threats. Experts from both countries believe that as a whole, the Sino-Russian cyber safety cooperation mechanism is quite comprehensive, and has made substantial progress at the technical and infrastructure building level. That being said, there are still some limitations. For instance, both countries still lack substantial safety cooperation, and there is still room for improvement on cyber mutual trust.

Nonetheless, when compared with the relation between the US and its allies, the cooperation between China and Russia pays greater attention to equality and mutual respect, and therefore has shown more trends of sustainability.

Keywords: China, Russia, cybersecurity, cyberterrorism, BRICS, SCO

For citation: Han Shiying (China). Sino-Russian Cyber Security Cooperation. *Asia and Africa today*. 2022. № 8. Pp. 66-72 (In Russ.). DOI: 10.31857/S032150750019782-2

ВВЕДЕНИЕ

Кибербезопасность - это совокупность методов и практик защиты компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных от атак злоумышленников. В настоящее время исследования в области кибербезопасности выполняются в трех направлениях: безопасность информации и данных,

безопасность системы передачи информации и безопасность последствий распространения информации. По мере развития современных технологий и общества кибербезопасность становится все более важным элементом национальной безопасности.

СТИМУЛЫ К РАСШИРЕНИЮ СОТРУДНИЧЕСТВА МЕЖДУ КИТАЕМ И РОССИЕЙ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

Китай и Россию можно назвать интернет-державами. По данным международного исследования *Global Digital*, к 2021 г. число пользователей интернета в России достигло 124 млн человек. Это 85% населения страны[1]. Согласно статистике Китайского информационного центра сети Интернет (*China Internet Network Information Center - CNNIC*), количество китайских интернет-пользователей по состоянию на конец 2020 г. достигло 986 млн, а уровень охвата интернета в КНР составлял 70,4%[2]. В обеих странах чрезвычайно большие сообщества пользователей интернета, перед которыми стоит проблема защиты от киберугроз, таких как киберконфликты.

Текущие проблемы кибербезопасности в двух странах касаются, в основном, следующих аспектов:

1. Информационные инфраструктуры обеих стран постоянно подвергаются кибератакам из-за рубежа. Многие крупные сайты и правительственные сайты в Китае подвергаются атакам хакеров. В январе 2010 г. на сайте главной китайской поисковой системы Байду возникла проблема - не удавалось получить доступ к сайту. Согласно расследованию, проведенному Китайским государственным центром реагирования на чрезвычайные ситуации в интернете, информация о доменном имени Байду (*Baidu*) была незаконно подделана. В результате пользователи по всему миру не могли зайти на сайт.

В январе 2013 г. онлайн-сайт газеты «Жэньминь жибао» подвергся атаке типа «отказ в обслуживании» (*Distributed Denial of Service - DDoS*) из-за рубежа[3]. После эпидемии коронавируса масштабы облачных атак и нарушений, направленных против Китая, продолжают расти. В последние годы наблюдается растущая тенденция к увеличению компьютерных атак на сайты правительственных органов, школ и предприятий энергетики в Китае[4,5].

Россия также - страна с высоким уровнем киберриска. Многие сайты в России подвергаются атакам из-за рубежа. Так, в частности, 4 декабря 2011 г., в день выборов в Госдуму, из-за масштабной атаки типа *DDoS* были недоступны для пользователей сайты многих СМИ в России («Эхо Москвы», «Коммерсанта» и т.д.). После смены власти на Украине в феврале 2014 г. хакеры взломали сайт телеканала «Россия сегодня» (*RT*) и добавили слово «*Nazi*» (нацист, нацистский) к заголовкам всех англоязычных материалов[6]. По данным исследования «Лаборатории Касперского», с момента начала специальной военной операции на Украине в феврале 2022 г. количество атак типа *DDoS* на интернет-ресурсы России резко увеличилось, оно в 3 раза превысило показатель за аналогичный период прошлого года. Многие сайты государственных учреждений круглосуточно подвергаются *DDoS*-атакам [9].

2. Информацию легко украсть и подделать. Интернет появился в относительно закрытых, надежных системах безопасности и научных исследований. Отсутствуют необходимые гарантии безопасности при передаче и управлении информацией и данными. Они легко могут быть украдены и подделаны. Данные о звонках, почтовые сообщения и записи сообщений абонентов систематически отслеживаются и даже собираются. Это часто происходит с каждым пользователем интернета.

Кроме того, родина и ведущая страна в развитии интернета - США - на протяжении десятилетий удерживает господство в интернете. На территории США находится большинство из 16 корневых серверов, контролирующих мировой интернет, в этой стране также находится Корпорация по управлению доменны-

---

[1] Число пользователей интернета в России достигло 124 млн 19.10.2021. https://tass.ru/obschestvo/12698757utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (accessed 16.04.2022)

[2] CNNIC released the 47th “Statistical Report on Internet Development in China” (In Chin.). Cyberspace Administration of China, 03.02.2021. http://www.cac.gov.cn/2021-02/03/c_1613923422728645.htm (accessed 18.04.2022)

[3] China has been increasingly attacked by overseas hackers, more than half of computer malware attacks in China from overseas entities originated in the US (In Chin.). Ministry of Foreign Affairs of the PRC, 10.03.2013. https://www.mfa.gov.cn/ce/cefr//chn/zgyw/t1020320.htm (accessed 12.04.2022)

[4] China's Internet network security monitoring data analysis report in the first half of 2021. From CNCERT (In Chin.). CNCERT, 01.07.2021. https://www.cert.org.cn/publish/main/upload/File/first-half%20%20year%20cyberseurity%20report%202021.pdf (accessed 16.04.2022)

[5] Foreign Ministry Spokesperson Zhao Lijian’s Regular Press Conference on March 14, 2022 (In Chin.). Ministry of Foreign Affairs of the PRC, 15.03.2022. https://www.fmprc.gov.cn/web/wjb_673085/zzjg_673183/jks_674633/jksxwlb_674635/202203/t20220315_10651922.shtml (accessed 20.04.2022)

[6] Хакерские атаки на сайты российских СМИ в 2010-2015 гг. Хронология. 01.06.2014. https://tass.ru/info/1028467?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (accessed 19.04.2022)

ми именами и *IP*-адресами в интернете (*Internet Corporation for Assigned Names and Numbers, ICANN*), присваивающая интернет-адреса. Поэтому США часто неограниченно расширяет рамки наблюдения за интернетом «во имя безопасности».

Типичный пример - проект «Призма» (*Prism*). В июне 2013 г. бывший сотрудник ЦРУ Сноуден передал газетам секретную информацию Агентства национальной безопасности США (АНБ), касающуюся массовой слежки американских спецслужб за своими гражданами. По его словам, правительство США использует программные продукты крупных *IT*-компаний для мониторинга и управления телекоммуникационными сетями всех стран. Контрольный список АНБ содержал не только имена лиц из враждебных стран, но и из стран-союзников (например, Ангела Меркель).

АНБ по договоренности с интернет-компаниями собирает данные, передаваемые по оптоволоконным каналам, в том числе подводным. АНБ также сотрудничает с разведывательными сообществами союзников и осуществляет перехват информации в более чем 200 оптоволоконных кабельных система [10]. Такое поведение спецслужбы США вызвало глобальный резонанс. После этого многие страны начали исследовать вопрос обеспечения суверенитета своего сегмента интернета и принимать соответствующие меры по защите собственного киберпространства.

3. Утечка информации может легко произойти вследствие случайного обнародования данных, или же если злоумышленник специально пытается разведать чужую информацию, скрытую от посторонних лиц. В начале октября 2019 г. информацию пытался похитить руководитель сектора в одном из бизнес-подразделений Сбербанка России. Это привело к утечке данных более 60 млн кредитных карт[7].

В Китае сотрудник китайского телекоммуникационного провайдера «Чайна Телеком» (*China Telecom*) продал несколькими траншами одной из преступных групп в теневом интернете более 200 млн учетных записей мобильных телефонов[8]. В 2020 г. злоумышленники посредством раскрытия информации о профилактике и борьбе с эпидемиями центральной больницы Циндао, передаваемой посредством крупнейшего мобильного приложения для обмена сообщениями в Китае Вичат (*Wechat*), скомпрометировали личную информацию более 6000 человек[9].

4. Террористы используют глобальное информационное пространство для своей деятельности. Благодаря развитию интернета пользователи могут легко получать различную информацию в системах мгновенного обмена сообщениями и на сайтах социальных сетей. Террористы используют эти новые интернет-СМИ для взаимодействия, преследуя свои преступные цели. Они пытаются распространять экстремистские, террористические и сепаратистские идеи, оказывают информационное и психологическое влияние на целевую аудиторию. Используя информацию, распространяемую террористами, злоумышленники могут обучаться проведению террористических актов. Поскольку эти люди раньше не участвовали в террористических организациях, они не находились под наблюдением спецслужб, что затрудняло их обнаружение и предотвращение подготавливаемых ими террористических актов. Заместитель секретаря Совета безопасности России Ю.Коков отметил, что террористы используют методы брачного мошенничества в интернете. При этом молодые женщины, польстившиеся на обещания обеспеченной и счастливой семейной жизни в одной из зарубежных стран, оказываются в террористических формированиях и впоследствии используются террористами, в т.ч. в качестве смертниц [11].

Схожие проблемы существуют и в Китае. Социально маргинализированные люди легко поддаются идеологической обработке со стороны экстремистских группировок. Совершившие теракт в Куньмине в 2014 г. признали, что их экстремистская организация занималась «промывкой мозгов» с помощью интернет-трансляций лекций и радиопередач, видео джихада. Они планировали теракты в людных местах, например, на вокзалах[10].

Таким образом, необходимо принять всесторонние эффективные меры для предотвращения более серьезных проблем кибербезопасности. В связи с этим Китай и Россия обнародовали ряд законов и нормативных актов с целью управления кибербезопасностью.

Однако мировой и транснациональный характер киберпространства не позволяет заключить его в национальные географические границы. Трудно решить проблемы в этой области, полагаясь на силы лишь

---

[7] Сбербанк подтвердил утечку данных 5 тыс. клиентов. *Коммерсантъ*. 07.10.2019. https://www.kommersant.ru/doc/4118056 (accessed 10.04.2022)

[8] Over 200 million pieces of user information from China Telecom were sold for as low as 0.01 yuan per piece (In Chin.). *Sina Tech.* 03.01.2020. https://tech.sina.com.cn/t/2020-01-03/doc-iihnzhfz9993505.shtml (accessed 05.04.2022)

[9] The three are suspected of revealing epidemic prevention and control information from Qingdao Jiaozhou Central Hospital, compromising more than 6000 people's private information (In Chin.). *Xinhua News Agency.* 19.04.2020. http://www.xinhuanet.com/legal/2020-04/19/c_1125877355.htm (accessed 21.04.2022)

[10] No country is immune from this cyberterrorism (In Chin.). *CPCNews*, 04.07.2014. http://cpc.people.com.cn/n/2014/0704/c83083-25239165.html (accessed 16.04.2022)

одной страны. Существует настоятельная необходимость работать совместно с другими странами для создания международной системы управления в области кибербезопасности, которая соответствовала бы целям национальной безопасности и экономическим и социальным интересам государства.

Позиции России и Китая по проблеме кибербезопасности близки: обе страны подчеркнули необходимость рассмотрения вопроса об информационном суверенитете и поддерживают установление многостороннего и демократического режима глобального управления интернетом. На принципах универсальности, равенства, конструктивного диалога и сотрудничества все страны вместе могли бы разработать условия, правила и руководящие принципы для решения проблем кибербезопасности.

Подводя итоги, сотрудничество между Китаем и Россией в области кибербезопасности обусловлено не только насущными потребностями в обеспечении безопасности, но и законами геополитики. Поэтому необходимо и целесообразно поддерживать и углублять сотрудничество в области обеспечения информационной безопасности.

НЫНЕШНЕЕ СОСТОЯНИЕ СОТРУДНИЧЕСТВА ДВУХ СТРАН

Сотрудничество в области кибербезопасности между Китаем и Россией началось в рамках V саммита глав государств-членов ШОС в июле 2005 г. в Астане. На саммите ШОС в Шанхае в июне 2006 г. Китай и Россия подписали «Заявление глав государств-членов ШОС по международной информационной безопасности», ставшее первым специальным документом о сотрудничестве в области информационной безопасности в рамках ШОС. В заявлении отмечается, что неправомерное использование информационно-коммуникационных технологий может приводить к мировым катастрофам, сопоставимым по своим разрушительным последствиям с результатами применения оружия массового уничтожения. Только путем принятия скоординированных и взаимодополняющих мер государства смогут дать адекватный ответ современным вызовам и угрозам безопасности в информационной сфере.

Кроме того, главы государств единогласно приняли решение о создании группы экспертов государств-членов ШОС по Международной информационной безопасности (МИБ) с участием представителей Секретариата Организации и Исполкома региональной антитеррористической структуры для выработки плана действий по обеспечению международной информационной безопасности. Эта группа является одним из постоянно действующих административных органов ШОС. Она отвечает в основном за оказание помощи в разработке законодательства и технологий в области кибербезопасности [1].

В 2011 г. Китай, Россия, Таджикистан и Узбекистан предложили ООН «Правила поведения в области обеспечения международной информационной безопасности», в соответствии с которыми страны должны были принять на себя обязательство не использовать кибероружие различных типов. Это первый комплексный и систематизированный документ, в котором содержатся четкие международные правила, касающиеся кибербезопасности. Однако документ не получил широкого отклика во многих западных странах во главе с США.

Государства-члены ШОС внесли на рассмотрение Генеральной Ассамблеи ООН новую редакцию «Правил поведения в области обеспечения международной информационной безопасности», в которой формулировка «использование кибероружия» была заменена на «использование ИКТ в целях, способных нанести серьезный ущерб безопасности человека, общества и государства в нарушение основополагающих принципов равноправия и взаимного уважения» и включен расширенный раздел о правах человека. На этот раз пересмотренный проект правил был поддержан различными странами и в конечном итоге стал официальным документом ООН. Вместе с Таллиннским руководством «Правила поведения в области обеспечения международной информационной безопасности» он представляет собой руководящий документ о международных правилах кибербезопасности [1].

В апреле 2015 г. в г. Сямэнь на востоке Китая компетентные органы стран-членов ШОС провели антитеррористические учения в Сети «Сямэнь-2015». Это первые совместные учения по борьбе с террористической деятельностью в интернете, которые проводил ШОС. Основной целью учений является повышение эффективности взаимодействия компетентных органов государств-членов ШОС по предупреждению, выявлению, пресечению и расследованию фактов терроризма, сепаратизма и экстремизма в интернете. Государства-члены обменялись с участниками информацией по правовой процедуре, организационно-техническим возможностям и конкретным мерам в целях противодействия террористической деятельности в интернете[11]. Учения получили высокую оценку со стороны присутствующих представителей государств. После этого учения в Сямэне проводились в 2017 г. и 2019 г.

[11] SCO's first cyber anti-terrorism exercise was successfully held in Xiamen. 14.10.2015. (In Chin.). http://www.gov.cn/xinwen/2015-10/14/content_2946854.htm (accessed 16.04.2022)

В 2019 г. утверждена «Концепция сотрудничества государств-членов ШОС в сфере цифровизации и информационно-коммуникационных технологий». В 2020 г. подписано «Заявление Совета глав государств-членов ШОС о сотрудничестве в области цифровой экономики». И утверждена «Концепция сотрудничества государств-членов ШОС по развитию удаленных и сельских территорий в цифровую эпоху». Документ помогает облегчить проблему цифрового разрыва, вызванного неравномерностью развития информационно-коммуникационных технологий в разных регионах, и уменьшить вероятность возникновения проблем кибербезопасности[12].

Сотрудничество в рамках БРИКС разделено на два этапа - усилия на начальном этапе были сосредоточены на кибертерроризме. В 2011 г. страны БРИКС достигли консенсуса по вопросам поддержки кибербезопасности и борьбы с киберпреступностью [12]. В январе 2013 г. на встрече советников по вопросам безопасности было сделано заявление о намерении создать новые глобальные механизмы для предотвращения пропаганды терроризма и распространения дезинформации в киберпространстве[13]. В апреле того же года 5 стран впервые представили в ООН проект резолюции об укреплении международного сотрудничества в борьбе с киберпреступностью от имени БРИКС, в котором содержится призыв к ООН продолжать содействовать проведению исследований и реагированию на киберпреступность. Это - первый случай, когда страны БРИКС выступили с совместной инициативой по кибербезопасности.

В более поздний период центром внимания в области сотрудничества стала безопасность данных. Переломным моментом был 2013 г. В Дурбане (ЮАР) 27 марта 2013 г. проходил Пятый саммит БРИКС, на котором участники достигли консенсуса по реализации проекта «Кабель “независимого Интернета БРИКС”». План Кабеля «независимого Интернета БРИКС» поможет странам БРИКС избавиться от зависимости от европейской и американской информационной инфраструктуры, сократить расходы на связь, обеспечить информационную безопасность стран БРИКС, может способствовать обмену современными информационными технологиями и содействовать развитию финансовой торговли. Это планируемая подводная волоконно-оптическая кабельная система связи, при помощи которой осуществляется телекоммуникация между странами БРИКС. Кабель пройдет по маршруту: Владивосток (Россия) - Шаньтоу (Китай) - Ченнаи (Индия) - Кейптаун (ЮАР) - Форталеза (Бразилия). Её общая протяженность составит примерно 34 000 км[14].

На Шестом саммите БРИКС (Форталеза, Бразилия) в 2014 г. страны БРИКС опубликовали Форталезскую Декларацию. Помимо акцента на усилении защиты кибербезопасности и борьбы с киберпреступностью, в декларации также высказывается мысль о том, что нужно решительно осуждать акты массовой электронной слежки и сбора данных о частных лицах по всему миру, а также нарушение суверенитета государств и прав человека, включая права на неприкосновенность частной жизни. Некоторые китайские эксперты считают, что подобного рода заявления - это выражение недовольства, вызванного американским проектом «Призма» (*Prism*) [2].

В июле 2015 г. на Седьмом саммите БРИКС в Уфе обсуждался вопрос о сотрудничестве в области обеспечения безопасности самих информационно-коммуникационных технологий и их использования. Также было принято решение о создании рабочей группы БРИКС по сотрудничеству в области информационно-коммуникационных технологий. Тогда же обсуждалось создание системы, позволяющей обеспечить конфиденциальность и защиту персональной информации пользователей на основе принципа многосторонности, демократии, прозрачности и взаимного доверия. Будут сформулированы соответствующие общепризнанные руководящие принципы, касающиеся киберпространства.

В сентябре 2017 г. на Девятом саммите БРИКС (Сямэнь, Китай) страны-члены рассмотрели возможность создания Института БРИКС по изучению сетей будущего в целях дальнейшего продвижения сотрудничества в сфере информационно-коммуникационных технологий. После этого на четвертой встрече министров коммуникаций стран БРИКС в сентябре 2018 г. было официально принято решение о создании Института БРИКС по изучению сетей будущего, его китайский филиал открылся в Шэньчжэне в августе 2019 г. [3].

Двустороннее сотрудничество между Китаем и Россией началось гораздо позже многостороннего сотрудничества. 8 мая 2015 г. министры иностранных дел двух стран подписали «Соглашение между Правительством РФ и Правительством КНР о сотрудничестве в области обеспечения международной информационной безопасности». В документе обозначены основные направления сотрудничества между Китаем и Россией в области обеспечения международной информационной безопасности, в т.ч. организация техно-

[12] The First Meeting of the SCO ICT leaders takes place SCO, 25.11.2021 (In Chin.). http://chn.sectsco.org/news/20211125/802626.html (accessed 25.04.2022)

[13] Terrorism, cyber security issues dominate BRICS security meet. 10.01.2013. https://www.dnaindia.com/india/report-terrorism-cyber-security-issues-dominate-brics-security-meet-1787706 (accessed 19.04.2022)

[14] BRICS Announce Joint Cybersecurity Group. 07.12.2013. http://www.thebricspost.com/brics-announce-joint-cyber-group/#.Yp3-sqhBzzB (accessed 29.04.2022)

логического канала связи для противодействия угрозам международной информационной безопасности, продвижение сотрудничества в сферах борьбы с кибертерроризмом и киберпреступностью, подготовка кадров и проведение научных исследований, усиление мер реагирования на кибер-чрезвычайные ситуации, укрепление сотрудничества в рамках ООН, МСЭ, ШОС, БРИКС и АСЕАН[15].

В июне того же года группа правительственных экспертов двух стран приняла участие в Международной конференции ООН по информационной безопасности. В декабре 2015 г. китайская компания по информационным технологиям в сфере кибербезопасности - *China Electronic Technology Cyber Security Co., Ltd.* (*CETC-CS*) подписала соглашение о стратегическом партнерстве с компанией «Лаборатория Касперского». Обе стороны будут углублять сотрудничество в области защиты домашнего компьютера от вирусных угроз, защиты APT, обмена информацией об угрозах, безопасности облачных вычислений, безопасности промышленных систем управления и обучения кадров [4].

В апреле 2016 г. в Москве прошел первый российско-китайский форум по безопасности в сети, организованный Ассоциацией безопасности киберпространства Китая и Альянсом интернет-безопасности. Представители правительства, бизнеса и эксперты обеих сторон обсудили кибербезопасность стран на всех уровнях. На форуме подчеркивалось, что двум странам нужно выстраивать свой цифровой суверенитет самостоятельно. У Китая одна из самых совершенных систем контроля интернета. Россия очень заинтересована в этой системе. Обе стороны выразили надежду на укрепление сотрудничества в этой области[16].

ЗАКЛЮЧЕНИЕ

Очевидно - китайско-российское сотрудничество в области кибербезопасности достигло определенных результатов. Конечно, для этого сотрудничества характерны определенные ограничения. Например, соглашение 2015 г. между двумя странами было оценено российскими экспертами просто как рамочное соглашение, основанное на согласованных общих ценностях и ожиданиях [5]. Китайские эксперты подвергли критике то, что многие планы сотрудничества остаются на уровне деклараций ежегодных саммитов и различных документов общего характера, принимаемых на встречах. Подписанные документы не были реализованы [1]. Эксперты обеих стран едины в том, что одна сторона имеет желание, а другая, похоже, психологически не готова [5; 6; 7].

Кроме того, российские эксперты отмечали, что появляются регулярные атаки на российские ресурсы с китайских *IP*-адресов [8]. А китайская сторона объясняла это тем, что зарубежные группы атаковали китайских пользователей, взяв под контроль компьютеры в стране, чтобы осуществить кибератаки на Россию. На самом деле, большинство адресов для этих атак изначально находились в Соединенных Штатах[17]. Такой кризис усугубил чувство незащищенности и недоверия между двумя сторонами. Более того, внутренняя политика двух стран в отношении суверенитета в интернете стала причиной того, что в обеих странах занимаются локализацией приложений[18]. Поэтому в некоторых аспектах сотрудничество в области кибербезопасности не может быть углублено.

Тем не менее, в целом, сотрудничество в области кибербезопасности между двумя странами вышло за рамки общего уровня. В отличие от неравноправного сотрудничества между Соединенными Штатами и их союзниками, Китай и Россия уделяют большое внимание равенству и взаимному уважению в процессе сотрудничества в области кибербезопасности. Их сотрудничество характеризуется устойчивым развитием.

ЛИТЕРАТУРА / REFERENCES

1. Zhang Wenwei. 2016. Information Security Cooperation in the Shanghai Cooperation Organization: The Necessity, Status Quo and Prospect. *Russia, East Europe and Central Asia Studies*. Issue 3. Beijing. Pp. 94-106, 157-158. (In Chin.)
2. Gao Wanglai. 2017. Advances in Cybersecurity Cooperation of BRICS Countries and the Way Forward. *China International Studies*. Issue 5. Beijing. Pp. 63-74. (In Chin.)

[15] Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development (In Chin.). 04.02.2022. http://www.scio.gov.cn/m/tt/xjp/Document/1719826/1719826.htm (accessed 16.04.2022)

[16] The first Russia-China Information and Communication Technologies Development and Security Forum held in Moscow in April 2016 (In Chin.). Xinhua News Agency, 28.04.2016. http://www.xinhuanet.com/world/2016-04/28/c_1118756226.htm (accessed 07.04.2022)

[17] Chinese internet suffers from overseas cyberattacks (In Chin.). Cyberspace Administration of China, 11.03.2022. http://www.cac.gov.cn/2022-03/11/c_1648615063553513.htm (accessed 127.04.2022)

[18] Domestic operating systems have to pass the procurement and adoption threshold (In Chin.). CCGP, 22.12.2014. http://www.ccgp.gov.cn/specialtopic/2015yd/dzz/201412/t20141222_4866410.htm (accessed 15.04.2022)

3. Chi Cheng. 2021. Analysis of BRICS Network Security Governance. *Network Security Technology & Application*. Issue 4. Beijing. Pp. 166-168. (In Chin.)
4. Lang Ping. 2020. Greatly Changing International Structure and the Major Power Relationship in the Governance of Cyberspace. *Global Media Journal.* Vol. 7. Issue 1. Beijing. Pp. 70-85. (In Chin.)
5. Куликова А. Киберпакт Китая и России: есть ли повод для беспокойства. *Индекс Безопасности.* 2015. Вып. 4. С. 113-126.
Kulikova A. 2015. CyberPact of China and Russia: Is there a reason for concern. *Security Index.* Issue 4. Moscow. Pp. 113-126. (In Russ.)
6. Shan Xiaoying. 2017. An analysis of the foundation and approach of Sino Russian cooperation in cyberspace governance. *Chinese Journal of Journalism & Communication.* Vol. 39, Issue 9. Beijing. Pp. 40-53. (In Chin.)
7. Sun Wei. 2015. Preliminary study of Sino-Russian Network Arms Control Cooperation. *Science and technology.* Issue 21. Yinchuan. Pp. 218-221. (In Chin.)
8. Исаев А.С. Российско-китайское взаимодействие по вопросам обеспечения информационной безопасности. *Китай в мировой и региональной политике. История и современность.* 2018. Вып. 23. С. 223-237.
Isaev A.S. 2018. Russian-Chinese Cooperation on Ensuring Information Security. *China in World and Regional Politics. History and Modernity.* Issue 23. Moscow. Pp. 223-237. (In Russ.)
9. Степанова Ю. Бойцы невидимого мошенничества. 28.02.2022. https://www.kommersant.ru/doc/5238079 (accessed 16.04.2022)
Stepanova Yu. Fighters of the invisible fraud (In Russ.). https://www.kommersant.ru/doc/5238079 (accessed 16.04.2022)
10. Khazan O. The Creepy, Long-Standing Practice of Undersea Cable Tapping. 16.07.2013. https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/ (accessed 16.04.2022)
11. Егоров И. Опасные клики - В Совбезе РФ прогнозируют серьезную активизацию террористов. 20.10.2020. https://rg.ru/2020/10/20/v-sovbeze-rf-prognoziruiut-sereznuiu-aktivizaciiu-terroristov.html (accessed 16.04.2022)
Egorov I. Dangerous cliques - The Security Council of the Russian Federation predicts a serious activation of terrorists (In Russ.). https://rg.ru/2020/10/20/v-sovbeze-rf-prognoziruiut-sereznuiu-aktivizaciiu-terroristov.html (accessed 28.04.2022)
12. Zhu Yingku. BRIC countries will work together to fight cybercrime (In Chin.). *Huanqiu*, 16.04.2010. https://world.huanqiu.com/article/9CaKrnJnhiq (accessed 20.04.2022)

ИНФОРМАЦИЯ ОБ АВТОРЕ / INFORMATION ABOUT THE AUTHOR

Хань Шиин (КНР), аспирантка кафедры международной безопасности, факультет мировой политики, Московский государственный университет им. М.В.Ломоносова, Москва, Россия.

Han Shiying (China), Post-graduate student, Department of International Security, Faculty of World Politics, Lomonosov Moscow State University, Moscow, Russia.

Поступила в редакцию (Received) 18.04.2022
Доработана после рецензирования (Revised) 26.05.2022
Принята к публикации (Accepted) 02.07.2022