Научная статья / Research article

# Региональное сотрудничество стран Центральной Азии в борьбе с кибертерроризмом

**А. Э. Галицына**

*Российский университет дружбы народов им. П. Лумумбы, Москва, Россия*
*E-mail: 1132223124@rudn.ru*

**О. В. Кембель**

*Российский университет дружбы народов им. П. Лумумбы, Москва, Россия*
*E-mail: 1132223122@rudn.ru*

**Д. Д. Потапова**

*Российский университет дружбы народов им. П. Лумумбы, Москва, Россия*
*E-mail: 1132223125@rudn.ru*

**Аннотация:** В статье коллектив авторов рассматривает актуальные инициативы и перспективы сотрудничества стран Центральной Азии по вопросам кибербезопасности и борьбы с кибертерроризмом. Регион стал свидетелем роста количества угроз, связанных с использованием информационных технологий в преступных целях. Подавляющее большинство совершаемых в киберпространстве атак приходится на финансовой сектор и носит частный характер, тем не менее, постепенная цифровизация важнейших отраслей экономики государств Центральной Азии и возрастающая роль всемирной информационной сети в координации действий как традиционных, так и нетрадиционных акторов, в перспективе могут привести к увеличению числа угроз и расширению «ассортимента» кибератак: от мошенничества и распространения экстремистских убеждений среди определённых слоев населения до нападений на промышленные объекты и их системы управления. В связи с этим правительства центральноазиатстких держав принимают меры для усиления контроля над каналами коммуникаций и защиты своей информационной инфраструктуры. Государства Центральной Азии активно развивают региональные инициативы по вопросам обеспечения кибербезопасности и пресечения террористической деятельности в киберсреде, однако данные форматы взаимодействия слабо институционализированы и преимущественно представлены дискуссионными площадками. На современном этапе страны региона отдают предпочтение совершенствованию государственного законодательства и организационных мероприятий по обеспечению информационной безопасности на национальном уровне, а также разработке соответствующих проектов в рамках более широкого региона – Евразии. Многостороннее сотрудничество в области противодействия киберугрозам на евразийском пространстве ведётся по линии СНГ и ШОС: механизмы, которые создаются и развиваются в стенах данных интеграционных объединений, дают импульс формированию системы региональной информационной безопасности.

**Ключевые слова:** терроризм, кибертерроризм, Центральная Азия, противодействие терроризму, СНГ, ШОС.

**Для цитирования:** Галицына А. Э., Кембель О. В., Потапова Д. Д. Региональное сотрудничество стран Центральной Азии в борьбе с кибертерроризмом // Постсоветские исследования. 2023;6(6):626-638.

# Regional Cooperation Between Central Asian Countries in Fight Against Cyberterrorism

**Arina E. Galitsyna**

*RUDN University named after P. Lumumba, Moscow, Russia*
*E-mail: 1132223124@rudn.ru*

**Olinda V. Kembel**

*RUDN University named after P. Lumumba, Moscow, Russia*
*E-mail: 1132223122@rudn.ru*

**Daria D. Potapova**

*RUDN University named after P. Lumumba, Moscow, Russia*
*E-mail: 1132223125@rudn.ru*

**Abstract:** In this article the authors study topical initiatives and prospects for cooperation between countries of Central Asia on cybersecurity and in the fight against cyberterrorism. The region has witnessed a rise in the number of threats related to information technologies and their use for criminal purposes. The vast majority of attacks in cyberspace belong to the financial industry and are of individual nature, nevertheless, gradual digitalization of the most important sectors of the Central Asian states' economy and increasing role of the global information network in coordination of actions of both traditional and non-traditional actors in the future can result in increased number of threats and expansion of the range of cyberattacks: from fraud and spread of extremist beliefs among certain parts of the population to attacks on industrial facilities and their management systems. In this regard, Central Asian countries' governments take measures to strengthen control over communication channels and to protect their information infrastructure. The states of Central Asia are actively developing regional initiatives on cybersecurity and suppression of terrorist activity in cybersphere, however, these formats of interaction are badly institutionalized and mainly represented by discussion platforms. At the current stage the countries of the region prefer improvement of state law and institutional arrangements for ensuring information security at national level, as well as developing projects within the wider region – Eurasia. Multilateral cooperation in the area of countering cyberthreats in the Eurasian space is under way through the CIS and SCO: mechanisms that are being established and developed within the walls of these integration associations give the impetus to the formation of a regional information security system.

**Key words:** terrorism, cyberterrorism, Central Asia, countering terrorism, CIS, SCO.

**For citation:** Arina E. Galitsyna, Olinda V. Kembel, Daria D. Potapova. Regional Cooperation Between Central Asian Countries in Fight Against Cyberterrorism // Post-Soviet Studies. 2023;6(6):626-638. (In Russ.).

В XXI в. киберпространство становится не только фундаментом для дальнейшего развития стратегических секторов экономики, транспортных систем и обороны той или иной страны, но и площадкой для взаимодействия многочисленных акторов мировой политики. Постепенный перенос конфликтов в глобальное информационное пространство также актуализирует проблему кибертерроризма как новой формы терроризма, появление которой стало возможным благодаря развитию гибких сетевых организационных структур и широкому доступу террористических формирований к коммуникационным технологиям и другим научно-техническим ресурсам.

Американский политолог В. Лакер отмечал, что в случае, если современный терроризм направит свою энергию на информационную войну, его разрушительная сила экспоненциально возрастёт и станет даже больше, чем могла бы быть при условии попадания в руки террористов биологического и химического оружия [Laqueur 1996: 35]. В свою очередь, сетевая война может охватывать широкий спектр различных видов деятельности: от информационных операций, целью которых является психологическое воздействие, до кибератак на системы связи и объекты критической инфраструктуры.

Центральная Азия является частью глобального информационного общества. В период с 2000 по 2022 гг. количество интернет-пользователей в странах региона выросло на 99,8%: с 113 тыс. до почти 42 млн

чел.[1] В контексте кибербезопасности данный показатель является одним из важнейших: всемирная сеть объединяет колоссальные объёмы информации и обеспечивает обмен данными как между людьми, так и в рамках единой системы серверов, компьютеров и других вычислительных приборов, однако именно здесь и кроется уязвимость, поскольку, по словам бывшего генерального директора ICANN Р. Бекстрома, всё оборудование, которое имеет доступ в Интернет, может быть взломано [Цаканян 2017: 340].

Информационное пространство стран региона весьма ограничено: только в Казахстане и Кыргызстане количество интернет-пользователей превышает 50% от общей численности населения и составляет 86% и 55%, соответственно (табл. 1). В Узбекистане глобальной сетью пользуются только 50,1% населения, в Таджикистане – 30,4%, а в Туркменистане – 25,3%, что определяется негативным воздействием таких факторов, как неравномерное распределение базовых станций, нехватка инвестиций в инфраструктуру, плохое качество сотового сигнала, низкая скорость Интернета, дороговизна мобильной и интернет-связи и т. д.[2]

Конъюнктура будет неизбежно меняться под воздействием внешних факторов (например, в силу заинтересованности освоения рынка телекоммуникационных услуг Центральной Азии российскими, китайскими и западными компаниями) и внутренней потребности в цифровизации экономики и других сфер. Тем не менее, вопрос распространения информационно-коммуникационных технологий становится предметом дискуссий не только ввиду недостаточного финансирования и научно-технологической базы, но и из-за особенностей политической культуры стран региона, которая выражается в попытках фильтрации и мониторинга контента [Schmitz, Wolters 2012: 28]: центральноазиатские режимы осознают важность внедрения современных цифровых технологий для обеспечения устойчивого экономического роста и одновременно с этим выражают обеспокоенность из-за возможной потери контроля над информационными потоками.

Эта озабоченность обусловлена тем, что с развитием киберпространства радикальные группировки получат больше возможностей для экспорта свой идеологии, вербовки и координации лиц для осуществления террористических актов, а также проведения кибератак на объекты энергосистемы и др. Данная проблема стала чрезвычайно актуальной после событий «арабской весны»: в августе 2011 г. в Астане прошёл неформальный саммит ОДКБ, одной из центральных тем которого стала роль социальных сетей и Интернета в политических процессах на Ближнем Востоке. В своей вступительной речи бывший лидер Казахстана Н. Назарбаев обозначил свободу информации в сети как угрозу региональной стабильности и безопасности [Schmitz, Wolters 2012: 28]. Тогда же главы государств договорились о выработке совместных мер противодействия угрозам в киберпространстве.

Согласно Глобальному индексу кибербезопасности (GCI), наиболее высоким уровнем защищённости обладает Казахстан: набрав 93,15 баллов из 100, Республика обеспечила себе второе место среди стран постсоветского пространства и вошла в ТОП-35 государств мира по данному показателю (табл. 2). Среди направлений, в которых Казахстан добился значительного успеха, были отмечены правовые меры и меры в отношении сотрудничества.

В качестве области дальнейшего роста были выделены меры для развития потенциала в сфере кибербезопасности, включающие государственную поддержку малых и средних предприятий в управлении киберрисками – необходимо отметить, что данная категория является слабым местом всех стран региона, кроме Казахстана и Узбекистана.

[1] Internet 2022 Usage in Asia // Internet World Stats. URL: https://www.internetworldstats.com/stats3.htm. (accessed: 15.04.2023).

[2] Karimova A. How is Mobile Communications and the Internet Developing in Central Asia? // CABAR. 25.10.2021. URL: https://cabar.asia/en/how-is-mobile-communications-and-the-internet-developing-in-central-asia. (accessed: 15.04.2023).

Особенно уязвимыми к киберугрозам оказались Таджикистан и Туркменистан, занявшие 138 и 144 места, соответственно. Основной проблемной областью этих стран выступает техническая составляющая, т. е. отсутствие или неэффективность служб реагирования на компьютерные инциденты на государственном уровне. Также в докладе GCI 2020 акцент делается на потребности в укреплении организационных мер: так, национальные стратегии и иные документы, затрагивающие кибербезопасность, подлежат регулярному обновлению. Помимо этого, подчёркивается приоритетность создания механизмов защиты детей в сети Интернет[3].

По состоянию на 2022 г. Центральная Азия находилась на третьем месте в общемировом рейтинге по проценту компьютеров автоматизированных систем управления, которые были атакованы вредоносными объектами (45,06%), основным источником угроз стала сеть Интернет (> 25%) [4]. «Лаборатория Касперского» не публикует отдельную статистику по странам региона с выделением отраслей, подвергшихся наибольшему количеству атак. Однако в одном из докладов в сравнении указаны данные по России, Беларуси и Казахстану: согласно представленному в аналитическом материале графику, большая часть кибератак на АСУ в Казахстане пришлась на автоматизацию зданий и нефтегазовую сферу[5].

Также в центральноазиатских странах отмечается большая активность финансовых «зловредов»: в ТОП-10 государств по доле атакованных банковскими троянами пользователей вошли Туркменистан (1 место, 6,7%), Таджикистан (3 место, 5,2%) и Узбекистан (5 место, 3,5%) [6]. Кроме того, Туркменистан, Казахстан и Таджикистан входят в десятку стран, в которых были зафиксированы попытки установки программ-майнеров для скрытой генерации криптовалют.

В основном данные кибератаки имеют целью получение материальной выгоды, тем не менее, это не говорит об отсутствии политически ангажированных взломов и иных видов киберпреступлений: например, в Узбекистане действует хакерская группа Clone-Security, которая совершает атаки на сайты администраций (хокимиятов) и официальные страницы других органов власти в знак несогласия с узбекской политикой.

## Региональные форматы взаимодействия

Центрально-Азиатский форум по управлению Интернетом (CA IGF) выступает крупнейшей региональной неформальной платформой для обсуждения вопросов цифрового развития. Он был учреждён в 2016 г. и является частью глобальной инициативы ООН. Уникальность этой площадки в том, что она привлекает к обсуждению государственной политики в отношении Интернета не только представителей органов власти стран региона, но и делегатов от бизнес-структур и неправительственных организаций [7]. Это способствует развитию государственно-частного партнёрства и в перспективе может уменьшить дисбаланс: как отметил бывший глава Центра анализа и расследования кибератак (ЦАРКА) А. Абдрасилов, в центральноазиатских странах сложилась ситуация, когда специалисты по кибербезопасности сконцентрированы преимущественно в частном секторе, но функции по выработке политики и принятию решений находятся в руках правительства[8].

[3] Global Cybersecurity Index 2020 // ITU Publications. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf. (accessed: 24.04.2023).

[4] Статистика // Kaspersky ICS CERT. URL: https://ics-cert.kaspersky.ru/statistics/. (accessed: 28.04.2023).

[5] Ландшафт угроз для систем промышленной автоматизации. Второе полугодие 2022 // Kaspersky ICS CERT. 06.03.2023. URL: https://ics-cert.kaspersky.ru/publications/reports/2023/03/06/threat-landscape-for-industrial-automation-systems-statistics-for-h2-2022/. (accessed: 28.04.2023).

[6] Kaspersky Security Bulletin 2022 // Kaspersky. URL: https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2022_ru_final.pdf. (accessed: 28.04.2023).

[7] О форуме – CAIGF – Central Asia Internet Governance Forum // CAIGF. URL: https://caigf.org/ru/o-forume/. (дата обращения: 30.04.2023).

[8] Нурмаков А. Эксперты Центральной Азии: кто должен отвечать за кибербезопасность? // Информационно-аналитический портал Digital.Report. 29.07.2016. URL: https://digital.report/ekspertyi-

В марте 2022 г. в Узбекистане прошла международная конференция высокого уровня, посвящённая региональному сотрудничеству в рамках Совместного плана действий по осуществлению Глобальной контртеррористической стратегии ООН. В своём обращении к участникам мероприятия президент страны Ш.М. Мирзиёев выдвинул идею формирования Единой электронной сети по кибертерроризму в Центральной Азии, а также призвал международное сообщество к разработке единых правовых механизмов для противодействия терроризму в информационном пространстве[9].

Эта инициатива может стать первой формальной региональной структурой по борьбе с киберугрозами. Однако на современном этапе государства Центральной Азии больше предпочитают участвовать в проектах с широким кругом членов – в частности, речь идёт о многосторонних форматах сотрудничества в рамках СНГ и ШОС.

Рост числа радикальных организаций, использование ИКТ для вербовки молодёжи, а также повышение уровня опасности в связи с расширением потенциала возникновения террористических демаршей в регионе закрепляют необходимость в эффективных мерах по противодействию радикализации, а Интернет, хотя и делает коммуникации, а также образовательные и досуговые активности доступнее, стал основным средством пропаганды, вербовки и подготовки «новой» террористической элиты – так считает М.С. Мирвайсов, заведующий международным отделом Академии Наук Республики Таджикистан, выступивший с данным тезисом на Международном круглом столе «Кибербезопасность и противодействие кибертерроризму и экстремизму в странах Центральной Азии на современном этапе: результаты, проблемы и перспективы» в феврале 2019 г. в столице Республики Узбекистан[10].

Это мероприятие – одна из редких инициатив, участие в которой приняли непосредственно региональные игроки, а именно Казахстан, Кыргызстан, Таджикистан и Узбекистан при содействии Российской Федерации. Уже в 2019 г. центральноазиатские державы были озабочены тем, что международные террористические организации претерпевают трансформацию своей деятельности в киберпространстве, и выделяли в качестве одной из основных задач объединение усилий для анализа способов и каналов влияния террористических группировок в сети Интернет. Это обсуждение стало своего рода «предтечей» событий 2020 г.: пандемия COVID-19 напрямую повлияла на «перенос» деятельности террористических группировок в онлайн-пространство в связи с закрытием границ и затруднением транспортных перевозок любого толка, обострив проблему кибербезопасности [Солодухина, Тарасов 2022: 129] и в определённой степени подтвердив слова эксперта Академии МВД Республики Узбекистан Н.А. Тургунова о том, что существует два основных вида кибертерроризма: проявляющийся «в чистом виде», т. е. предполагающий совершение противоправных действий при помощи компьютерной техники, и «организационный», при котором группировки используют интернет-пространство с целью наладить коммуникацию[11].

Стоит отметить, что Узбекистан активно выдвигает собственные инициативы по борьбе с киберпреступностью на локальном и

tsentralnoy-azii-kto-dolzhen-otvechat-za-kiberbezopasnost/. (дата обращения: 30.04.2023).

[9] Обращение Президента Узбекистана Ш. Мирзиёева к участникам Международной конференции высокого уровня по глобальной контртеррористической стратегии ООН // Исполнительный комитет СНГ. 04.03.2022. URL: https://cis.minsk.by/news/22628/obraschenie_prezidenta_uzbekistan_sh.mirzijoeva_k_uchastnikam_mezhdunarodnoj_konferencii_vysokogo_urovnja_po_globalnoj_kontrterrori kontrterro_strategii_oon. (дата обращения: 10.05.2023).

[10] Кибербезопасность и противодействие кибертерроризму и экстремизму в странах Центральной Азии // Каспийский Вестник. 04.03.2019. URL: http://casp-geo.ru/kiberbezopasnost-i-protivodejstvie-kiberterrorizmu-i-ekstremizmu-v-stranah-tsentralnoj-azii/?fbclid=IwAR2lB_Q1Is5NztnjoT57M8ttwBkQ8RYqGv9tkDq_3n_zhHiwyRFcwN8Zzhw. (дата обращения: 28.05.2023).

[11] Там же // Каспийский Вестник. 04.03.2019. URL: http://casp-geo.ru/kiberbezopasnost-i-protivodejstvie-kiberterrorizmu-i-ekstremizmu-v-stranah-tsentralnoj-azii/?fbclid=IwAR2lB_Q1Is5NztnjoT57M8ttwBkQ8RYqGv9tkDq_3n_zhHiwyRFcwN8Zzhw. (дата обращения: 28.05.2023).

международном уровнях. Ранее в тексте статьи упоминалось создание Единой электронной сети по кибертерроризму в Центральной Азии; на одном из саммитов ШОС главы государств Республики Узбекистан и Республики Кыргызстан выдвинули инициативу о проведении совещания руководителей профильных министерств и возобновлении встреч министров внутренних дел и общественной безопасности для борьбы с кибертерроризмом [Черняева, Журавлёва 2022: 540–541]. Более того, Узбекистан выходит за рамки центральноазиатского сотрудничества: в 2017 г. представители правоохранительных органов республики обсуждали перспективы взаимодействия в области преступлений, связанных с использованием ИКТ, с делегатами соответствующих ведомств Южной Кореи[12]. Что касается внутренней политики, в 2022 г. в стране был принят Закон о кибербезопасности [13], регулирующий отношения в этой сфере, а ранее, в 2005 г. и 2013 г. соответственно, были созданы Группа реагирования на чрезвычайные компьютерные ситуации и Центр информационной безопасности в рамках Государственного комитета по коммуникациям, развитию информационной системы и технологиям телекоммуникаций.

Законодательная база Таджикистана в этом вопросе менее обширна: на территории государства действуют Концепция информационной безопасности Республики Таджикистан (2003 г.) [14] и Концепция государственной информационной политики (2008 г.) [15] (не считая отдельных ведомственных законов, связанных с противодействием киберпреступности и насильственному экстремизму онлайн и оффлайн).

Важно отдавать отчёт, что вся информация, имеющая государственную важность, может быть использована как средство политического давления при попадании в преступные руки. Об этом напоминает Д.Г. Орлов, директор киргизского аналитического центра «Стратегия Восток-Запад» [16]. В последние годы Кыргызстан достаточно активно обновляет свою политику в области цифрового обеспечения и кибербезопасности, о чём свидетельствует, в частности, тот факт, что 2020 г. в Республике прошёл под эгидой «развития регионов, цифровизации страны и поддержки детей» [17] : акцент на приоритетность информационных технологий был сделан и ранее, ещё в 2019 г., впоследствии тенденция закрепилась.

Основным документом, регулирующим связанную с ИКТ деятельность, является Концепция информационной безопасности Кыргызской Республики на 2019–2023 гг.[18], принятая, соответственно, в 2019 г., и План мероприятий по её реализации. Разработка и

[12] Узбекистан и Южная Корея намерены сотрудничать в противодействии киберпреступлениям // UZ DAILY. 18.12.2017. URL: https://uzdaily.uz/index.php/ru/post/35387. (дата обращения: 28.05.2023).

[13] Закон Республики Узбекистан от 15 апреля 2022 г. «О кибербезопасности». // Buxgalter.uz. URL: https://buxgalter.uz/doc?id=689744_zakon_respubliki_uzbekistan_ot_15_04_2022_g_n_zru-764_o_kiberbezopasnosti_(prinyat_zakonodatelnoy_palatoy_25_02_2022_g_odobren_senatom_17_03_2022_g_)&prodid=1_zakonodatelstvo_ruz&ysclid=liaidjb345678037513#. (дата обращения: 28.05.2023).

[14] Концепция информационной безопасности Республики Таджикистан от 7 ноября 2003 г. // ЦБПИ «Адлия». URL: http://adlia.tj/show_doc.fwx?Rgn=5104. (дата обращения: 28.05.2023).

[15] Концепция государственной информационной политики Республики Таджикистан от 30 апреля 2008 г. // ЦБПИ «Адлия». URL: http://adlia.tj/show_doc.fwx?rgn=12904. (дата обращения: 28.05.2023).

[16] Кибербезопасность и противодействие кибертерроризму и экстремизму в странах Центральной Азии // Каспийский Вестник. 04.03.2019. URL: http://casp-geo.ru/kiberbezopasnost-i-protivodejstvie-kiberterrorizmu-i-ekstremizmu-v-stranah-tsentralnoj-azii/?fbclid=IwAR2lB_Q1Is5NztnjoT57M8ttwBkQ8RYqGv9tkDq_3n_zhHiwyRFcwN8Zzhw. (дата обращения: 28.05.2023).

[17] От цифровизации до волонтерства: каким будет 2020 год в странах Центральной Азии // News-Asia. 03.01.2020. URL: news-asia.ru/view/kz/. (дата обращения: 28.05.2023).

politics/13202 (дата обращения: 28.05.2023)

[18] Концепция информационной безопасности Кыргызской Республики на 2019–2023 гг. от 3 мая 2019 г. // Министерство Юстиции Кыргызской Республики. URL: http://cbd.minjust.gov.kg/act/view/ru-

принятие проекта осуществлялись с целью сформулировать методы обеспечения кибербезопасности, оценить и спрогнозировать вероятные угрозы. Безусловно, это не первая из внутригосударственных инициатив, направленная на достижение указанных задач. Так, например, в 2009 г. для анализа деятельности экстремистских организаций в сети Интернет (главным образом, группировки «Хизб ут-Тахрир» [19] ) была создана подведомственная МВД Республики Кыргызстан группа специалистов по вопросам киберугроз. Важно отметить, что отличительной чертой киргизской политики в области обеспечения информационной безопасности является прямое государственное вмешательство: все связанные с повесткой вопросы находятся в ведении Государственного комитета национальной безопасности[20] – это закрытая структура, конфиденциальность которой не позволяет исчерпывающе оценить эффективность вводимых практик.

Нельзя не упомянуть ситуацию, складывающуюся в Казахстане. По словам Ш.У. Сабирова, выступавшего от лица Института по вопросам безопасности и сотрудничества в Центральной Азии [21] , государство и гражданское общество Республики должны объединить усилия, т. к. только координированные действия сторон могут дать практический результат. Несомненно, ключевой внутренней инициативой можно считать Национальную концепцию кибербезопасности Казахстана, или «Киберщит» (2017 г.) [22], – программу, которая создавалась с целью решить проблему распространения влияния киберпреступников и выявить закономерности и возможную логику действий кибертеррористов локального и международного уровней [Лагуткина, Мадалимбеков, Омарова 2022: 855]. По состоянию на второе полугодие 2022 г. велась работа над обновлением стратегии – Национальной политики «Киберщит 2.0», которая, как планировалось, должна стать более практико-ориентированной. Ранее (2014 г.) были внесены изменения в Уголовный кодекс Республики Казахстан, которые выразились в указании на составы уголовных правонарушений, касающихся информатизации и связи[23].

Интересно также отметить, что Казахстан инвестирует в подготовку кадров: предполагается, что специализированные школы, занимающиеся повышением квалификации специалистов в области программирования, будут вовлечены в развитие компетенций учащихся для обучения реагированию на киберугрозы [24] . Важность такой инициативы разделяют Узбекистан и Казахстан, которые независимо друг от друга создали специальные учебные программы в национальных университетах с целью подготовки специалистов в области кибербезопасности.

Таким образом, обозначенные выше страны Центральной Азии активно развивают проекты, направленные на борьбу с кибертерроризмом, однако эти инициативы

ru/13652?ysclid=liai3m7vi5472708875. (дата обращения: 29.05.2023).

[19] Запрещена на территории Российской Федерации.

[20] Экспертная встреча: Кибербезопасность в странах Центральной Азии. Что делается для ее улучшения? // Central Asian Bureau for Analytical Reporting. 29.06.2022. URL: https://cabar.asia/ru/ekspertnaya-vstrecha-kiberbezopasnost-v-stranah-tsentralnoj-azii-chto-delaetsya-dlya-ee-uluchsheniya. (дата обращения: 29.05.2023).

[21] Кибербезопасность и противодействие кибертерроризму и экстремизму в странах Центральной Азии // Каспийский Вестник. 04.03.2019. URL: http://casp-geo.ru/kiberbezopasnost-i-protivodejstvie-kiberterrorizmu-i-ekstremizmu-v-stranah-tsentralnoj-azii/?fbclid=IwAR2lB_Q1Is5NztnjoT57M8ttwBkQ8RYqGv9tkDq_3n_zhHiwyRFcwN8Zzhw. (дата обращения: 29.05.2023).

[22] Об утверждении Концепции кибербезопасности («Киберщит Казахстана») от 30 июня 2017 г. // Информационно-правовая система нормативных правовых актов РК. URL: https://adilet.zan.kz/rus/docs/P1700000407. (дата обращения: 29.05.2023).

[23] Обзор законодательства Республики Казахстан: Борьба с киберпреступностью // Digital Report. 29.07.2016. URL: https://digital.report/zakonodatelstvo-kazahstana-borba-s-kiberprestupnostju/. (дата обращения: 29.05.2023).

[24] Экспертная встреча: Кибербезопасность в странах Центральной Азии. Что делается для ее улучшения? // Central Asian Bureau for Analytical Reporting. 29.06.2022. URL: https://cabar.asia/ru/ekspertnaya-vstrecha-kiberbezopasnost-v-stranah-tsentralnoj-azii-chto-delaetsya-dlya-ee-uluchsheniya. (дата обращения: 29.05.2023).

по большей части односторонние, ставящие целью укрепление национальной безопасности. Тем не менее, стоит отметить, что, помимо отраженных в тексте статьи международных соглашений, существуют дополнительные: так, например, Казахстан, Узбекистан и Кыргызстан присоединились к глобальной сети компьютерных групп реагирования на чрезвычайные ситуации (Computer Emergency Response Teams, или CERT: CERT-KZ, UZ-CERT, CERT.KG соответственно).

Нельзя не обратить внимание на соглашения, касающиеся вопросов кибербезопасности и предполагающие сотрудничество стран центральноазиатского региона в рамках СНГ. Первым шагом к формированию единого пространства для диалога по теме угроз, которые могут нести информационные технологии, стало Соглашение о сотрудничестве в борьбе с преступлениями в сфере компьютерной информации [25] (2001 г.). В этой концепции впервые были зафиксированы основные термины и описания, а также основания для привлечения к уголовно-правовой ответственности за нарушения в обозначенной сфере. Документ стал альтернативой Будапештской конвенции Совета Европы о компьютерных преступлениях 2001 г., которую страны Центральной Азии, а также РФ, отказались подписывать в связи с угрозой нарушения государственного суверенитета действиями иностранных служб: предполагалось, что они получали право беспрепятственного доступа к коммуникационным сетям стран-участниц договора [Аляутдинова, Валиахметова 2020: 43].

Годом ранее, 21 июня 2000 г., был создан Антитеррористический центр государств-участников СНГ. АТЦ продолжает свою деятельность и в настоящее время, выступая связующим звеном между инициативами, реализуемыми СНГ, и международными организациями, в частности ООН (фактически с момента создания), ОБСЕ, Интерполом (с 2008 г.)[26].

Значительно позже, в 2013 г., были выдвинуты две новые инициативы, а именно: Концепция сотрудничества по борьбе с преступлениями, совершаемыми с использованием ИКТ [27], и Соглашение о сотрудничестве в области обеспечения информационной безопасности[28]. Некоторые специалисты сходятся во мнении, что документы, принятые в тот год, не сыграли ключевой роли в процессе работы над развитием системы кибербезопасности стран Содружества[29].

Один из последних, наиболее актуальных на данный момент проектов, – Соглашение о сотрудничестве в борьбе с преступлениями в сфере информационных технологий[30].

В настоящее время соглашения, подписанные в рамках многостороннего сотрудничества стран СНГ, не отмечены крупными реализуемыми на практике инициативами. В данном случае страны Центральной Азии обращаются, скорее, «вовнутрь», работая над проектами национальной безопасности.

---

[25] Соглашения о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации от 6 июня 2001 г. // МИД РФ. URL: https://www.mid.ru/ru/foreign_policy/integracionnye-struktury-prostranstva-sng/sng/1682423/. (дата обращения: 29.05.2023).

[26] Международное сотрудничество // АТЦ СНГ. URL: https://www.cisatc.org/1289/9141. (дата обращения: 29.05.2023).

[27] Концепция сотрудничества по борьбе с преступлениями, совершаемыми с использованием ИКТ от 25 октября 2013 г. // АТЦ СНГ. URL: https://www.cisatc.org/9030. (дата обращения: 29.05.2023).

[28] Соглашение о сотрудничестве государств-участников СНГ в области обеспечения информационной безопасности от 20 ноября 2013 г. // КонтурНорматив. URL: https://normativ.kontur.ru/document?moduleId=1&documentId=253328&ysclid=liaogcullb464396956. (дата обращения: 29.05.2023).

[29] Эксперты Центральной Азии: кто должен отвечать за кибербезопасность // Digital Report. 29.07.2016. URL: https://digital.report/ekspertyi-tsentralnoy-azii-kto-dolzhen-otvechat-za-kiberbezopasnost/. (дата обращения: 29.05.2023).

[30] Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере информационных технологий от 1 июля 2021 г. // Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/351210645?ysclid=li7gxxadpt51895898. (дата обращения: 29.05.2023).

**Взаимодействие стран-членов ШОС в борьбе с кибертерроризмом**

История деятельности межправительственной региональной организации начинается в 2001 г.[31] У истоков создания Шанхайской организации сотрудничества наряду с Россией и Китаем стояли такие государства Центральной Азии, как Казахстан, Таджикистан, Узбекистан и Кыргызстан, приоритетом деятельности которых в рамках Организации является поддержание стабильности и безопасности в регионе на постоянной основе.

Нельзя отрицать тот факт, что кибератаки на информационные системы стран стали неотъемлемым инструментом борьбы в каждом современном военном конфликте, политическом противостоянии или международном кризисе. Признавая кибертерроризм «глобальным вызовом XXI в.», государства ШОС тесно сотрудничают для противостояния угрозам, которые возникают в информационном пространстве.

Утверждением в 2007 г. Долгосрочного плана действий по обеспечению и поддержанию безопасности в информационном пространстве [32] было положено начало борьбы с кибертерроризмом в евразийском регионе. Основные положения данного документа закрепляли меры и механизмы, которые были направлены на предотвращение использование инструментов ИКТ террористическими группировками с целью навязывания радикальных экстремистских идеологий.

В 2009 г. ШОС продолжила выработку совместных защитных мер: подписав межправительственное Соглашение, направленное на поддержание тесного сотрудничества стран Организации по обеспечению безопасности международного информационного пространства [33] (действующее до сих пор), страны-члены Организации определили общие принципы и основные направления взаимодействия, среди которых можно отметить:

– создание систем мониторинга и совместного реагирования на возникающие угрозы;

– борьбу с преступностью с использованием инструментов ИКТ;

– противодействие информационному терроризму;

– противостояние информационной войне и использованию информационного оружия;

– борьбу с передачей данных, которая может нанести ущерб не только экономической инфраструктуре, но и духовным и социальным ценностям населения.

В том же году в рамках Международного круглого стола «ШОС: климат доверия и информационная безопасность», собравшего в том числе и представителей ведущих СМИ стран-участниц Организации, были представлены на обсуждение такие темы, как особенности информационного пространства евразийского региона, возможности и компетенции средств массовой информации в сфере обеспечения безопасности, а также вопрос необходимости противодействия использованию инструментов информационно-коммуникационных технологий в кибератаках.

ШОС определяет СМИ одним из субъектов международной информационной безопасности и подчёркивает, что в настоящее время крайне важно выбрать верный и наиболее лояльный способ донесения информации через телевидение, радио и прессу, и для достижения данной цели Организация намерена создать межправительственные СМИ, чтобы обеспечить безопасность и стабильность общего информационного пространства.

[31] Декларация о создании Шанхайской организации сотрудничества // Президент России. 14.06.2001. URL: http://kremlin.ru/supplement/3406. (дата обращения: 20.05.2023).

[32] Документы, принятые на заседании Совета глав государств-членов Шанхайской организации сотрудничества (ШОС), Бишкек, 16–17 августа 2007 года // МИД РФ. URL: https://www.mid.ru/ru/foreign_policy/rso/1679469/. (дата обращения: 20.05.2023).

[33] Соглашение между правительствами государств-членов Шанхайской организации сотрудничества в области обеспечения международной информационной безопасности (Екатеринбург, 16 июня 2009 г.) // ГАРАНТ. URL: https://base.garant.ru/2571379/. (дата обращения: 20.05.2023).

В рамках заседания Совета глав государств ШОС в июне 2011 г. бывший глава Казахстана Н. Назарбаев выступил с идеей создания на территории государств ШОС киберполиции в целях выявления и пресечения преступлений. Данную инициативу поддержали также Россия и Таджикистан. Впоследствии Казахстан разработал проект по созданию подобного специального подразделения, он до сих пор не был реализован[34].

В декабре 2015 г. в ходе 14-го заседания Совета глав правительств было заключено соглашение «О выделении целевых денежных средств на создание защищённой информационно-телекоммуникационной системы связи между компетентными органами государств-членов ШОС» [35]. Данный проект осуществлялся поэтапно с 2016 по 2018 гг., на его реализацию было выделено более 4 млн долл. США [Булва 2019: 100].

Следует подчеркнуть, что реализация положений всех соглашений, принимаемых с 2007 г., по обеспечению международной информационной безопасности осуществляется на проводимых ежегодно встречах руководителей силовых министерств государств и специальных ведомств Организации, где особое внимание уделяется вопросам выявления, предупреждения и борьбы с киберпреступностью [Евдокимов, Хобонкова 2022: 92].

Стоит также отметить, что в настоящее время обсуждается проект по созданию специализированной системы фильтрации Интернета стран ШОС, механизмы деятельности которой будут направлены на выявление актов вербовки новых сторонников и распространения радикальных идеологий среди населения. Прототипом такой новации стала разработанная в 2003 г. IT-специалистами Китая система «Золотой щит» с целью выявления и предупреждения новых киберпреступлений [Юе 2021: 3701].

С 2007 по 2015 гг. было предпринято множество попыток оградить страны-участниц ШОС и их население от кибератак и снизить количество актов нарушения информационного пространства, тем не менее, кибертерроризм всё ещё остаётся одной из главных проблем международной безопасности.

В Стратегии развития ШОС до 2025 г.[36], принятой в 2015 г., особое внимание уделяется необходимости создания универсального механизма обеспечения международной информационной безопасности, который смог бы не только выявлять и пресекать военные и политические угрозы, но и противостоять бесконтрольному доступу террористических группировок к личным данным пользователей.

Стоит также отметить, что, начиная с 2015 г., каждые два года ШОС проводит учения по борьбе с кибертерроризмом. В рамках данных мероприятий искусственно создаются условия неизвестной кибератаки на системы безопасности стран, согласно которым международная террористическая группировка пытается завербовать новых сторонников и распространяет информацию экстремистского характера. Благодаря таким учениям спецслужбы ШОС проверяют свою готовность и способность выявлять и предотвращать случаи кибертерроризма.

В 2022 г., по результатам исследований, ШОС была выделена в качестве одной из организаций, которые внесли большой вклад в развитие системы международной информационной безопасности [Евдокимов, Хобонкова 2022: 91].

Проанализировав основные механизмы и направления взаимодействия стран-членов ШОС, можно сделать вывод, что, благодаря реализации множества проектов и инициатив, эффективному управлению ресурсами и

[34] В рамках ШОС будет создана киберполиция // Информационная Россия. 25.04.2012. URL: http://inforos.ru/ru/?module=news&action=view&id=30049. (дата обращения: 23.05.2023).

[35] Решение Совета глав правительств (премьер-министров) Шанхайской организации сотрудничества (15 декабря 2015 год) // Законодательство стран СНГ. URL: https://base.spinform.ru/show_doc.fwx?rgn=84271. (дата обращения: 27.05.2023).

[36] Стратегия развития Шанхайской организации сотрудничества до 2025 года // Президент России. URL:http://static.kremlin.ru/media/events/files/ru/a3YPpGqLvQI4uaMX43lMkrMbFNewBneO.pdf. (дата обращения: 27.05.2023).

тесному сотрудничеству в борьбе за международную информационную безопасность, Организация выступает влиятельным актором мировой политики, способным наращивать собственный технологический потенциал в сфере информационно-коммуникационных технологий.

Методы и формы сотрудничества подтверждают, что страны-члены ШОС обладают большим потенциалом для кооперации и сотрудничества в рамках Организации и за её пределами. Все государства выражают заинтересованность и готовность в урегулировании конфликтов и укреплении взаимодействия по обеспечению и поддержанию безопасности глобального киберпространства.

**Заключение**

В последние годы Центральная Азия стала свидетелем роста угроз кибербезопасности. Кибертерроризм – относительно новое явление, его разрушительный потенциал очень велик. Преступники, совершающие противоправные действия в информационном пространстве, активно используют технологии для своих целей, что создает угрозы в т. ч. для ключевой инфраструктуры, а также для государств-партнёров: Центральная Азия – важный с точки зрения транспортной и нефтегазовой системы регион. Он располагает значительными запасами ископаемого топлива, нефти и газа, и, находясь в центре евразийского континента, связывает Восток и Запад. Учитывая это, руководителям центральноазиатских государств важно выдвигать инициативы, направленные на предотвращение возможных кибератак. В рамках региональных организаций принимаются декларации, создаются международные группы экспертов, проводятся совместные мероприятия, направленные на повышение уровня кибербезопасности в регионе.

## ИЛЛЮСТРАЦИИ

*Таблица 1*

**Использование сети Интернет в странах Центральной Азии (2000–2022 гг.)[37]**

| *Государство* | *Количество интернет-пользователей* | | *% от численности населения (2022 г.)* |
|---|---|---|---|
| | *2000 г.* | *2022 г.* | |
| Казахстан | 70 000 | 16 465 777 | 86% |
| Кыргызстан | 51 600 | 3 683 700 | 55% |
| Таджикистан | 2 000 | 3 013 256 | 30,4% |
| Туркменистан | 2 000 | 1 562 794 | 25,3% |
| Узбекистан | 7 500 | 17 161 534 | 50,1% |

*Таблица 2*

**Глобальный индекс кибербезопасности 2020 г.: Центральная Азия**

| *Государство* | *Количество баллов (max 100)* | *Место в общемировом рейтинге* |
|---|---|---|
| Казахстан | 93,15 | 31 |
| Кыргызстан | 49,64 | 92 |
| Таджикистан | 17,1 | 138 |
| Туркменистан | 14,48 | 144 |
| Узбекистан | 71,11 | 70 |

Источник: Global Cybersecurity Index 2020 // ITU Publications.

[37] Internet 2022 Usage in Asia // Internet World Stats.

## СПИСОК ЛИТЕРАТУРЫ

*Аляутдинова К.Ш., Валиахметова Г.Н.* Особенности формирования системы национальной кибербезопасности Киргизской Республики // Вестник МГЛУ. Общественные науки. 2020. № 3 (840). С. 36–49.

*Барсегян А.А., Кернер Е.А.* Проблема цифровизации терроризма на пространстве СНГ // Постсоветские исследования. 2020. Т. 3. № 4. С. 315–322.

*Булва В.И.* Проблемы информационной безопасности на евразийском пространстве: пути их преодоления в рамках ШОС // Международный журнал конституционного и государственного права. 2019. № 2. С. 98–102.

*Евдокимов К.Н., Хобонкова К.В.* К проблеме совершенствования международного сотрудничества в сфере противодействия киберпреступности // Сибирский юридический вестник. 2022. №. 3 (98). С. 90–95.

*Курылев К.П., Мартыненко Е.В.* Российско-китайское экономическое сотрудничество в контексте проекта "один пояс, один путь". Фактор ЕАЭС и ШОС // Вопросы национальных и федеративных отношений. 2019. Т. 9. № 11 (56). С. 1937-1948.

*Лагуткина Ю. Н., Мадалимбеков Ж. И., Омарова Д. К.* Противодействие стран Российской Федерации и Республики Казахстан информационному терроризму // Постсоветские исследования. 2022. Т.5. № 8. С. 847–860.

*Рахимов К.Х.* Правовое регулирование противодействия терроризму и экстремизму в государствах Шанхайской организации сотрудничества // Евразийский юридический журнал. 2019. № 2 (129). С. 67–70.

*Ревин В.П.* Актуальные проблемы сотрудничества государств-участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий // Международное сотрудничество евразийских государств: политика, экономика, право. 2017. № 1. С. 83–92.

*Солодухина Е.А., Тарасов Д.С.* Противодействие государств-участников СНГ терроризму и экстремизму в сфере информационных технологий // Постсоветские исследования. 2022. Т. 5. № 1. С. 124–130.

*Сосновская Ю.Н., Маркина Э.В.* К вопросу о международном сотрудничестве в сфере противодействия кибертерроризму // Вестник Московского университета МВД России. 2022. № 3. С. 253–256.

*Цаканян В.Т.* Роль кибербезопасности в мировой политике // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2017. Т. 17. № 2. С. 339–348.

*Чжэн И.* Сотрудничество РФ и КНР в борьбе с кибертерроризмом // Вестник Московского государственного областного университета. 2018. № 2. С. 204–213.

*Юе Г.* Противодействие кибертерроризму в рамках ШОС // Вопросы политологии. 2021. № 12 (76). С. 3700–3704.

*Arquilla J.* Ethics and Information Warfare // Strategic Appraisal: The Changing Role of Information in Warfare / Khalilzad Z. et al. RAND Corporation, 1999. P. 379–402.

*Laqueur W.* Postmodern Terrorism // Foreign Affairs. 1996. Vol. 75. № 5. P. 24–35.

*Schmitz A., Wolters A.* Politischer Protest in Zentralasien: Potentiale und Dynamiken // SWP-Studie. 2012. № 4. 30 p.

## REFERENCES

*Alyautdinova K.Sh., Valiakhmetova G.N.* Osobennosti formirovaniya sisnemy nacional’noj kiberbezopasnosti Kirgizskoj Respubliki // Vestnik MGLU. Obshestvennye nauki. 2020. № 3 (840). S. 36–49.

*Arquilla J.* Ethics and Information Warfare // Strategic Appraisal: The Changing Role of Information in Warfare / Khalilzad Z. et al. RAND Corporation, 1999. P. 379–402.

*Barsegian A.A., Kerner E.A.* Problema cifrovizacii terrorizma na prostranstve SNG // Postsovetskie issledovaniya. 2020. T. 3. № 4. S. 315–322.

*Bulva V.I*. Problemy informacionnoj bezopasnosti na evrazijskom prostranstve: puti ih preodoleniya v ramkah ShOS // Mezhdunarodnyj zhurnal konstitucionnogo i gosudarstvennogo prava. 2019. № 2. S. 98–102.

*Evdokimov K.N., Hobonkova K.V*. K probleme sovershenstvovaniya mezhdunarodnogo sotrudnichestva v sfere protivodejstviya kiberprestupnosti // Sibirskij yuridicheskij vestnik. 2022. № 3 (98). S. 90–95.

*Kurylev K.P., Martynenko E.V.* Rossijsko-kitajskoe ekonomicheskoe sotrudnichestvo v kontekste proekta "odin poyas, odin put'". Faktor EAES i SHOS // Voprosy nacional'nyh i federativnyh otnoshenij. 2019. T. 9. № 11 (56). S. 1937-1948.

*Lagutkina Y.N., Madalimbekov Zh.I., Omarova D.K.* Protivodejstvie stran Rossijskoj Federacii i Respubliki Kazahstan informacionnomu terrorizmu // Postsovetskie issledovaniya. 2022. T. 5. № 8. S. 847–860.

*Laqueur W.* Postmodern Terrorism // Foreign Affairs. 1996. Vol. 75. № 5. P. 24–35.

*Rakhimov K.Kh.* Pravovoe regulirovanie protivodejstviya terrorizmu i ekstremizmu v gosudarstvah Shanhajskoj organizacii sotrudnichestva // Evrazijskij yuridicheskij zhurnal. 2019. № 2 (129). S. 67–70.

*Revin V.P.* Aktualnye problemy sotrudnichestva gosudarstv-uchastnikov Sodruzhestva Nezavisimyh Gosudarstv v bor'be s prestupleniyami, sovershaemymi s ispol'zovaniem informacionnyh tehnologij // Mezhdunarodnoe sotrudnichestvo evrazijskih gosudarstv: politika, ekonomika, pravo. 2017. № 1. S. 83–92.

*Schmitz A., Wolters A.* Politischer Protest in Zentralasien: Potentiale und Dynamiken // SWP-Studie. 2012. № 4. 30 p.

*Solodukhina E.A., Tarasov D.S.* Protivodejstvie gosudarstv-uchastnikov SNG terrorizmu i ekstremizmu v sfere informacionnyh tehnologij // Postsovetskie issledovaniya. 2022. T. 5. № 1. S. 124–130.

*Sosnovskaya Y.N., Markina E.V*. K voprosu o mezhdunarodnom sotrudnichestve v sfere protivodejstviya kiberterrorizmu // Vestnik Moskovskogo universiteta MVD Rossii. 2022. № 3. S. 253–256.

*Tsakanyan V.T*. Rol' kiberbezopasnosti v mirovoj politike // Vestnik Rossijskogo universiteta druzhby narodov. Seriya: Mezhdunarodnye otnosheniya. 2017. T. 17. № 2. S. 339–348.

*Youe G*. Protivodejstvie kiberterrorizmu v ramkah ShOS // Voprosy politologii. 2021. № 12 (76). S. 3700–3704.

*Zheng Yi*. Sotrudnichestvo RF i KNR v bor'be s kiberterrorizmom // Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. 2018. № 2. S. 204–213.

## ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

**Галицына Арина Эдуардовна,** студент 1 курса магистратуры, направление «Международные отношения», РУДН им. П. Лумумбы, Москва, Россия. (E-mail: 1132223124@rudn.ru)

**Кембель Олинда Викторовна,** студент 1 курса магистратуры, направление «Международные отношения», РУДН им. П. Лумумбы, Москва, Россия. (E-mail: 1132223122@rudn.ru)

**Потапова Дарья Дмитриевна,** студент 1 курса магистратуры, направление «Международные отношения», РУДН им. П. Лумумбы, Москва, Россия. (E-mail: 1132223125@rudn.ru)

**Arina E. Galitsyna,** 1st year student of the master's program "International Relations", RUDN University named after P. Lumumba, Moscow, Russia. (E-mail: 1132223124@rudn.ru)

**Olinda V. Kembel,** 1st year student of the master's program "International Relations", RUDN University named after P. Lumumba, Moscow, Russia. (E-mail: 1132223122@rudn.ru)

**Daria D. Potapova,** 1st year student of the master's program "International Relations", RUDN University named after P. Lumumba, Moscow, Russia. (E-mail: 1132223125@rudn.ru).