оригинальная статья / original paper
специальность: 5.1.5
EDN: DPHRBL

Взаимодействие Шанхайской организации сотрудничества с Интерполом в контексте борьбы с киберпреступностью

Сергевнин С. Л.*, Алексеев Г. В., Калкэй Е. И.
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Северо-Западный институт управления, Санкт-Петербург, Россия
* e-mail: sergevnin-sl@ranepa.ru
ORCID: 0000-0001-7397-4023

РЕФЕРАТ

Взаимодействие государств — членов Шанхайской организации сотрудничества с *Международной организацией уголовной полиции* (Интерполом) в деле борьбы с общеуголовной киберпреступностью предполагает формирование общей системы ценностей и гармонизацию национального уголовного права государств в Евразийском регионе. Анализ международно-правовых норм и правил взаимодействия Шанхайской организации сотрудничества и Интерпола демонстрирует широкие перспективы международного взаимодействия правоохранительных органов в деле борьбы с киберпреступностью на универсальном и региональном уровнях. **Цель.** Характеристика международно-правового принципа неделимости безопасности при взаимодействии государств — членов Шанхайской организации сотрудничества с Интерполом. Региональный евразийский дискурс по проблеме борьбы с киберпреступностью позволяет не только развить классификацию составов киберпреступлений, но и — при участии Интерпола в нем — способствует достижению всеобъемлющей и неделимой информационной безопасности в процессе цифровой трансформации мирового сообщества. **Методология.** Формально-юридическая, сравнительно-правовая и дискурсивная методики исследования демонстрируют интерес государств Евразии к проблеме борьбы с киберпреступностью и формируют теоретическую основу для гармонизации регионального и универсального правопорядков в киберпространстве. **Результаты.** Вовлечение международных организаций и институтов гражданского общества в практику противодействия киберпреступности на региональном и универсальном уровнях способствует легитимации норм международного уголовного права. Формирование международной системы справедливого и соразмерного тяжести преступлений уголовного преследования лиц, совершивших общественно опасные деяния в киберпространстве, отвечает интересам достижения целей устойчивого развития, Уставу Интерпола 1956 г. и положениям Шанхайской конвенции о борьбе с терроризмом, сепаратизмом и экстремизмом 2001 г. **Выводы**. Пропаганда экстремизма и оправдание терроризма в киберпространстве несут в себе значительную угрозу международной безопасности, и такие преступления не должны оставаться безнаказанными, особенно ввиду религиозного и политического разнообразия Евразийского региона. Участие институтов гражданского общества в формировании политики Шанхайской организации сотрудничества и Интерпола по противодействию киберпреступности будет способствовать росту доверия в Евразийском регионе, становлению прогрессивных форматов международного взаимодействия для борьбы с кибермошенничеством и пропагандой насильственного экстремизма в сети Интернет.

Ключевые слова: преступность, безопасность, искусственный интеллект, экстремизм, терроризм, мошенничество, робототехника

Для цитирования: Сергевнин С. Л., Алексеев Г. В., Калкэй Е. И. Взаимодействие Шанхайской организации сотрудничества с Интерполом в контексте борьбы с киберпреступностью // Евразийская интеграция: экономика, право, политика. 2025. Т. 19, № 3. С. 68–79. EDN: DPHRBL

Interaction between the Shanghai Cooperation Organization and Interpol in the Context of Combatting Cybercrime

Sergey L. Sergevnin*, George V. Alexeyev, Elina I. Kalkey
Russian Presidential Academy of National Economy and Public Administration, North-West Institute of Management, Saint Petersburg, Russia
* e-mail: sergevnin-sl@ranepa.ru
ORCID: 0000-0001-7397-4023

ABSTRACT
The interaction of the member States of the Shanghai Cooperation Organization with the International Criminal Police Organization (Interpol) in combating ordinary law cybercrime involves the formation of a common system of values and harmonization of national criminal law of States in the Eurasian region. An analysis of international legal norms and rules of interaction between the Shanghai Cooperation Organization and Interpol demonstrates broad prospects for international interaction between law enforcement agencies in combating cybercrime at the universal and regional levels. **Aim.** Characteristics of the international legal principle of indivisibility of security in the interaction of the member States of the Shanghai Cooperation Organization with Interpol. The regional Eurasian discourse on the problem of combating cybercrime allows not only to develop the classification of cybercrime, but also, with the participation of Interpol, contributes to the achievement of comprehensive and indivisible information security in the process of digital transformation of the world community. **Methods.** The formal-legal, comparative-legal and discursive research methodology shows both the interest of the Eurasian states in the problem of combating cybercrime and the theoretical basis for the harmonization of regional and universal legal order in cyberspace. **Results.** The involvement of international organizations and civil society institutions in the practice of combating cybercrime at the regional and universal levels contributes to the legitimization of the norms of international criminal law. The formation of an international system of fair and proportionate to the gravity of the crimes public prosecution of persons who have committed socially dangerous acts in cyberspace meets the interests of achieving the goals of sustainable development, the Interpol Constitution 1956 and the provisions of the Shanghai Convention on Combating Terrorism, Separatism and Extremism 2001. **Conclusions.** Propaganda of extremism and justification of terrorism in cyberspace pose a significant threat to international security, and such crimes should not go unpunished because of the religious and political diversity in the Eurasian region. The participation of civil society institutions in the formation of Interpol and the Shanghai Cooperation Organization policies on combating cybercrime will contribute to the growth of trust in the Eurasian region, the establishment of progressive formats of international cooperation to combat cyber fraud and propaganda of violent extremism on the Internet.

Keywords: crime, security, artificial intelligence, extremism, terrorism, fraud, robotics
For citation: Sergevnin S. L., Alexeyev G. V., Kalkey E. I. Interaction between the Shanghai Cooperation Organization and Interpol in the Context of Combatting Cybercrime // Eurasian Integration: Economics, Law, Politics. 2025. Vol. 19, No. 3. P. 68–79 (In Rus.). EDN: DPHRBL

Введение

Генеральный секретарь Интерпола Вальдеси Уркиса (Valdecy Urquiza) по итогам операции HAECHI V отметил, что «последствия киберпреступности могут быть разрушительными — жизни перевернуты, бизнес разрушен, а доверие к цифровым системам подорвано… Объединившись, мы можем сделать как реальный, так и цифровой мир безопаснее»[1]. Глобальная операция Интерпола HAECHI V (июль — ноябрь

[1] Interpol financial crime operation makes record 5,500 arrests, seizures worth over USD 400 million [Электронный ресурс]. URL: https://www.interpol.int/News-and-Events/News/2024/INTERPOL-financial-crime-operation-makes-record-5-500-arrests-seizures-worth-over-USD-400-million (дата обращения: 05.06.2025).

2024 г.) была направлена на борьбу с различными типами кибермошенничества, онлайн-шантажом и незаконной организацией азартных игр в сети Интернет (online gambling); завершилась операция арестом более 5500 подозреваемых в финансовых преступлениях с изъятием более 400 млн долл. США в виртуальных активах. Интерпол координировал взаимодействие правоохранительных органов около 40 государств, среди которых Китайская Народная Республика, Республика Индия, Кыргызская Республика и Исламская Республика Пакистан — члены Шанхайской организации сотрудничества (ШОС).

Глобальный характер операций Интерпола и региональное взаимодействие государств под эгидой ШОС демонстрируют заинтересованность государств и международных организаций в снижении уровня киберпреступности. Профессионализм секретариата Интерпола и аппарата ШОС позволяет трансформировать современную геополитическую неопределенность в последовательную политику противодействия опасным проявлениям киберпреступности, таким как фишинг [20], другое компьютерное мошенничество, распространение вредоносных программ и кибертерроризм [6].

Материалы и методы

Сравнительный анализ отражает становление институтов международного сотрудничества в деле борьбы с правонарушениями в киберпространстве и демонстрирует то, как компетенция Интерпола и ШОС реализуется в сфере противодействия киберпреступности.

В Уставе Интерпола 1956 г. и Шанхайской конвенции о борьбе с терроризмом, сепаратизмом и экстремизмом 2001 г. международная безопасность получает различную интерпретацию. В соответствии со второй целью Устава Интерпола организация призвана «создавать и развивать институты, которые могут эффективно способствовать предотвращению и пресечению общеуголовных преступлений»[1]. После основания Интерпола в 1923 г. актуализировались попытки использовать международную уголовную полицию в политических целях, что привело к использованию структур Интерпола нацистами в годы Второй мировой войны для борьбы с антифашистским движением [26], и после реформирования в 1956 г. Уставом «организации категорически запрещается осуществлять какое-либо вмешательство или деятельность политического, военного, религиозного или расового характера» (ст. 3).

Борьба с терроризмом, сепаратизмом и экстремизмом в формате ШОС, напротив, имеет как политическое, так и идеологическое содержание. ШОС предполагает региональное сотрудничество в обеспечении безопасности киберпространства при реализации суверенных прав государств. Соглашение о сотрудничестве между правительствами государств — членов ШОС в борьбе с преступностью 2010 г.[2] определяет преступления в сфере информационных технологий как одно из направлений регионального взаимодействия правоохранительных органов (п. 1 ст. 1). Астанинская декларация Совета глав государств — членов ШОС от 4 июля 2024 г.[3] призывает к разработке документа ШОС о сотрудничестве в борьбе с преступлениями в сфере информационных технологий.

В своей работе Интерпол руководствуется Конвенцией о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.)[4], в то время как государства — члены ШОС выступают за широкое признание Конвенции ООН против киберпреступности от 24 декабря 2024 г.[5], которая предполагает защиту государственного суверенитета в киберпространстве (ст. 5) и правовую помощь государств на принципах взаимности (ст. 40). Конвенция ООН против киберпреступности 2024 г. нацелена на

---

1 The Constitution of the International Criminal Police Organization (ICPO) — Interpol [Электронный ресурс]. URL: https://www.interpol.int/Who-we-are/Legal-framework/Legal-documents (дата обращения: 15.05.2025).

2 Бюллетень международных договоров, февраль 2013. № 2. С. 17–22.

3 Шанхайская организация сотрудничества [Электронный ресурс]. URL: https://rus.sectsco.org/20240704/1420683.html (дата обращения: 15.05.2025).

4 Council of Europe — Convention on Cybercrime (ETS No. 185) [Электронный ресурс]. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/documents (дата обращения: 15.05.2025).

5 Конвенция ООН против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям. Резолюция 79/243 Генеральной Ассамблеи ООН от 24 декабря 2024 г. [Электронный ресурс]. URL: https://www.un.org/ru/documents/treaty/A-RES-79-243 (дата обращения: 15.05.2025).

противодействие киберугрозам посредством реализации государствами юрисдикции в киберпространстве, а Будапештская конвенция 2001 г. направлена на гармонизацию национального законодательства в сфере противодействия киберпреступности.

Согласно Будапештской конвенции 2001 г. международная помощь по вопросам противодействия киберпреступности осуществляется через Интерпол (пп. b п. 9 ст. 27). Поскольку исключительной юрисдикцией Интерпол Уставом не наделен, постольку основные направления деятельности организации включают координацию международных расследований преступлений, выходящих за пределы национальных юрисдикций, а также содействие предотвращению или раскрытию киберпреступлений. Для реализации этих задач Интерпол обеспечивает взаимодействие между своими структурными подразделениями, а также Национальными центральными бюро (НЦБ) в странах-участницах, что позволяет эффективно организовать обмен оперативной информацией и оказывать поддержку в проведении расследований.

Правовое взаимодействие Интерпола и ШОС характеризуется как правовая коммуникация, в которой публичные и частные акторы международной системы осуществляют противодействие преступности и содействие в правоохранительной деятельности [10]. Содействие ШОС и Интерпола осуществляется в соответствии с Всеобщей декларацией прав человека 1948 г. и другими принципами международного права. Правовое взаимодействие государств в рамках Интерпола, ШОС и других организаций, заинтересованных в обеспечении кибербезопасности, формирует транснациональный цифровой правопорядок.

И Интерпол, и ШОС реализуют собственную независимую политику по борьбе с киберпреступностью, однако преследуют общие цели в области кибербезопасности. Если Интерпол фокусируется на создании инновационных методик расследований, оперативном обмене информацией между странами-участницами и разработке стандартов работы с цифровыми доказательствами [2], то для ШОС проявления экстремизма и терроризма в киберпространстве являются основной критической угрозой. Дополнительный протокол к Конвенции о киберпреступности, касающийся криминализации деяний расистского и ксенофобского характера, совершаемых с помощью компьютерных систем (2003 г.[1]) показывает, что все международные механизмы борьбы с киберпреступностью дополняют друг друга, формируя принципиальную основу международного реагирования на вызовы цифровой эпохи, однако результаты исследования отражают ряд институциональных отличий в работе Интерпола и ШОС.

Результаты

Проявления киберпреступности характеризуются как комплекс преступлений международного характера, где политическая преступность, общеуголовное мошенничество и компьютерные преступления используются как организованными преступными сообществами, так и одиночными субъектами для достижения противоправных экономических и политических целей. Борьба с киберпреступностью и противодействие терроризму в условиях цифровой трансформации как со стороны Интерпола, так и в форматах ШОС, требуют международной вовлеченности в правоохранительную деятельность не только государств, но и структур гражданского общества.

Совместная разработка и реализация академических проектов — перспективная форма сотрудничества Интерпола и государств — членов ШОС. Интерпол регулярно проводит конференции, круглые столы и семинары для сотрудников правоохранительных органов, осуществляющих мероприятия по борьбе с киберпреступностью [4; 16].

Повышение квалификации полицейских — перспективное направление международного сотрудничества в деле борьбы с преступностью вообще [9] и киберпреступностью в частности [24]. Подготовку полицейских кадров по международным стандартам осуществляет совместный учебный центр в Ташкенте, созданный в 2023 г. Центр проводит сертифицированные курсы по расследованию криптовалютных схем и противодействию кибератакам, объединяя методологии Интерпола и специфику противодействия киберугрозам в Евразийском регионе. Ежегодные киберучения в Центре (проводятся с 2019 г.) стали

[1] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. 2003. (ETS № 189).

примером эффективного сотрудничества, так, например, в 2024 г. на учениях моделировались атаки на финансовые системы с участием 120 экспертов, что позволило отработать механизмы экстренного взаимодействия правоохранительных органов.

Противодействие киберпреступности предполагает скоординированные усилия на международной арене, где значимую роль играют полицейские организации различного уровня авторитета и компетенции. Глобальные структуры, такие как Интерпол, обеспечивают и соответствующий универсальный охват, координируя действия правоохранительных органов разных государств и способствуя оперативному обмену информацией об актуальных киберугрозах. Региональные объединения государств, такие как ШОС, сосредоточиваются на специфических вызовах в своих географических рамках, разрабатывая специализированные подходы к кибербезопасности с учетом социально-культурных особенностей региона. На универсальном уровне Организация Объединенных Наций (ООН) задает стратегические направления международной политики в цифровой сфере, способствуя выработке единых стандартов и правовых норм всеми акторами международной системы.

Совместными усилиями ООН, Интерпол и ШОС ведут работу по нескольким направлениям: повышение киберграмотности, укрепление межгосударственного взаимодействия правоохранительных структур, сближение национальных законодательных систем в области противодействия компьютерной преступности, мошенничеству и распространению запрещенной информации через сеть Интернет, что в совокупности формирует многоуровневую систему противодействия цифровой преступности. Такое мультилатеральное сотрудничество становится необходимым в условиях, когда киберугрозы приобретают все более широкий трансграничный характер.

Перспективы дальнейшего развития партнерства Интерпола и ШОС связаны с углублением институциональных связей, включая создание совместных рабочих групп по конкретным видам киберпреступлений, а также гармонизацию правовых норм в области расследований правонарушений в киберпространстве.

Консенсус в определении кибертерроризма между Интерполом и ШОС может способствовать обеспечению всеобъемлющей информационной безопасности. Термин «кибертерроризм» впервые появился в 1980 г. и был введен специалистом Института безопасности и разведки в Калифорнии Барри Коллином (Barry Collin) для характеристики активности террористов в Сети [22]. Данным термином теперь обозначаются провокации террористических атак через киберпространство и дезорганизация работы государственных сетевых ресурсов [30]. Между тем мировое сообщество до сих пор не выработало единообразного и общепризнанного определения термина «кибертерроризм», что обусловлено политическими и религиозными разногласиями в национальных элитах.

Интерпол обоснованно рассматривает терроризм как общеуголовное преступление и координирует борьбу с проявлениями политизированного насилия [29]. Вместе с тем многие типичные правонарушения экстремистского характера редко квалифицируются Интерполом как тяжкие или общеуголовные деликты, несмотря на то, что они приводят к проявлениям международного терроризма [7] и преступлениям, связанным с ненавистью [19].

Стратегическим направлением в обеспечении всеобъемлющей кибербезопасности и борьбе с политической киберпреступностью стала кибердипломатия, особенно в свете инициатив ШОС по формированию альтернативных моделей управления интернетом, которые, с одной стороны, могут противоречить западным подходам, но с другой — открывают новые возможности для выстраивания многосторонних механизмов противодействия киберпреступности и поддержания необходимой свободы в сети. Форматы кибервзаимодействия, учитывающие интересы всех заинтересованных сторон (stakeholders), продвигаются через специальные учреждения ООН и призваны способствовать поддержанию доверия к открытым сетевым технологиям. Сотрудничество Интерпола и ШОС может стать элементом глобальной архитектуры кибербезопасности, показывая пример того, как региональные и международные организации могут дополнять друг друга в деле борьбы с общими угрозами цифровой эпохи.

Национальные стратегии противодействия киберпреступности и кибертерроризму требуют гармонизации уголовного и транснационального цифрового права, а также оперативного полицейского

сотрудничества. Одной из заметных инициатив сотрудничества ШОС с Интерполом стал оперативный проект Cyber SCO-Interpol, запущенный в 2021 г. Цифровая платформа объединяет ресурсы стран — членов ШОС для мониторинга DDoS-атак на критическую инфраструктуру, и с 2023 г. она интегрирована с глобальной системой обмена данными Интерпола I-24/7, что значительно ускоряет реагирование на транснациональные инциденты [32].

Принцип оперативности противодействия кибератакам реализуется при обмене информацией между странами — участницами Интерпола через защищенную глобальную полицейскую сеть, которая позволяет правоохранительным органам получать доступ к информации о мошенниках и террористах.

Взаимодействие Интерпола и экспертных групп, созданных при международных организациях для противодействия киберпреступности, представляет собой комплексный и динамично развивающийся процесс, сочетающий в себе элементы формального сотрудничества и неформальных партнерских инициатив. Опыт сотрудничества Интерпола с экспертным сообществом может быть полезен для взаимодействия государств в форматах ШОС и СНГ.

Интерпол является межправительственной организацией, чья деятельность строго регламентирована учредительными документами и ограничена национальными юрисдикциями, чем принципиально отличается от экспертных групп по обеспечению кибербезопасности, которые непосредственно участвуют в разработке универсальных технических решений, необходимых для обеспечения законности в киберпространстве.

Одним из ключевых направлений полицейского взаимодействия является обмен информацией и согласование методик экспертиз. Интерпол, обладая глобальной сетью правоохранительных агентств, предоставляет широкому спектру организаций доступ к данным о новых видах киберпреступлений, тенденциях в области цифровой преступности и методах расследования, в то время как экспертные группы специализируются на технических аспектах кибербезопасности, защите цифровых прав от уязвимостей программного обеспечения и разработке правил кибербезопасности [27]. Например, в рамках Организации гражданской авиации (ICAO) функционирует целая система экспертных групп программистов для обеспечения кибербезопасности авиации[1], такие группы по мере необходимости задействуются в операциях по противодействию киберпреступности.

Компетенция Интерпола определяется его Уставом и положениями национального административного права, которые нацелены на вовлечение гражданского общества в борьбу с международной преступностью. В частности, Положение о Национальном центральном бюро Интерпола Министерства внутренних дел Российской Федерации (НЦБ Интерпола МВД России)[2] в качестве одной из основных функций определяет «выявление и обобщение положительного опыта взаимодействия с международными правоохранительными организациями» (п. 10.27), среди которых множество профсоюзных и добровольческих объединений полицейских.

Эффективность борьбы с киберпреступностью зависит от международного взаимодействия гражданского общества с правоохранительными органами в силу глобального характера и технической природы цифровых коммуникаций. Стратегия государственно-частного партнерства позволяет Интерполу реализовывать проекты в области криптографии и робототехники для экспертного анализа потенциальных угроз и уязвимостей в сети Интернет.

Совместные операции Интерпола и экспертных групп при международных организациях, как правило, соответствуют национальным интересам государств — членов ШОС. Так, например, при нейтрализации ботнета Retadup в 2019 г. исследователи из гражданского сектора помогли выявить инфраструктуру преступников; другой пример — операция HAECHI IV (2023 г.) против финансового кибермошенничества в Азии с участием экспертов по блокчейн-аналитике[3].

---

[1] Aviation Cybersecurity. ICAO Expert Groups [Электронный ресурс]. URL: https://www.icao.int/aviationcybersecurity/Pages/ICAO-Expert-Groups.aspx (дата обращения: 15.05.2025).

[2] Утверждено приказом МВД России от 31 марта 2012 г. № 305 «Об утверждении положения о Национальном центральном бюро Интерпола Министерства внутренних дел Российской Федерации» [Электронный ресурс]. URL: https://мвд.рф/mvd/structure1/Upravlenija/Nacionalnoe_centralnoe_bjuro_Interpola (дата обращения: 15.05.2025).

[3] Interpol. International cooperation dismantles Retadup malware network. 2019.

Особого внимания заслуживает операция Silent Network 2022 г., в ходе которой были нейтрализованы бот-сети, использовавшие серверы в Казахстане и Китае для масштабного банковского мошенничества. Успех операции стал возможен благодаря координации через Национальные центральные бюро Интерпола и использованию аналитических институтов ШОС. Такая практика подтверждает конструктивность инициатив по подключению региональных инициатив ШОС к глобальной сети Интерпола.

Обсуждение

Работы профессора Ю. А. Тихомирова демонстрируют то, как юридические коллизии [17] приводят к нарушению правопорядка и кризисным явлениям вплоть до распада мироустройства [18]. Несомненно, «влияние национальных нормативных правовых актов на международные акты ощущается по линии межгосударственных интеграционных объединений» [5], которые формируют региональный правопорядок. Партнерство Интерпола и ШОС может способствовать «включенности национальных правовых систем в метасистему мирового правопорядка в их соотношении и взаимодействии с наднациональными юридическими инструментами и механизмами» [15, с. 17], что приведет к разрешению многих коллизий цифрового права и сформирует универсальный и безопасный цифровой правопорядок.

К коллизиям международного и национального цифрового правопорядка приводит принципиальное расхождение в подходах к безопасности. В частности, международные правозащитные организации последовательно критикуют практики массового сбора информации правоохранительными органами, рассматривая их как угрозу фундаментальным правам человека. Юридические барьеры также осложняют транснациональное взаимодействие — например, в Европейском союзе (ЕС) жесткие требования директивы GDPR[1] создают сложности для оперативного международного обмена информацией. С одной стороны, государственные институты и правозащитные организации формируют систему региональной кибербезопасности в ЕС [25], с другой стороны, опыт ЕС в деле борьбы с нарушением авторских прав показывает то, как ограничения цифровой свободы способствуют формированию цифрового разрыва.

Сочетание научных исследований, технического прогресса и активной гражданской позиции позволяет интернет-сообществу содействовать государствам в борьбе с киберпреступностью. Эксперты не только расследуют киберделикты (например, атаки на журналистов с помощью шпионской программы Pegasus), но и разрабатывают технические инструменты защиты, такие как детекторы вредоносного кода [28].

Экспертные группы необходимы в деле обеспечения кибербезопасности. Показателен пример того, как коллаборация экспертов Quad9 и Интерпола позволила заблокировать тысячи фишинговых доменов, нацеленных на больницы во время пандемии COVID-19 в 2020 г.[2] Экспертные группы систематически участвуют в нейтрализации угроз глобальной кибербезопасности под эгидой Интерпола [21], и этот опыт международного сотрудничества, безусловно, полезен.

Международные неправительственные организации и экспертные группы формируют систему институтов вокруг Инженерного совета Интернета (IETF)[3]. Эксперты IETF компетентны в сфере обнаружения уязвимостей в сети Интернет, они документируют кибератаки и разрабатывают инструменты для отслеживания криптовалютных транзакций [12].

Усилия экспертных групп дополняют возможности Интерпола, так как кибербезопасность — общий интерес государств, транснациональных корпораций и гражданского общества [31]. Вместе с тем в развитых государствах сохраняется настороженное отношение к неправительственным организациям, чью деятельность обоснованно воспринимают как потенциальный инструмент деструктивного иностранного вмешательства в работу правоохранительных органов [3]. Политизация международного правосудия создает препятствия для полноценного международного полицейского сотрудничества.

---

1 Directive 95/46/EC (General Data Protection Regulation) [Электронный ресурс]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:310401_2&from=EN (дата обращения: 15.05.2025).

2 Quad9 & Interpol (2020). Cybercrime Directorate Disrupts COVID-19 Phishing Campaigns [Электронный ресурс]. URL: https://www.interpol.int/News-and-Events/News/2020/Cybercrime-Directorate-disrupts-COVID-19-phishing-campaigns (дата обращения: 15.05.2025).

3 Internet Engineering Task Force [Электронный ресурс]. URL: https://www.ietf.org (дата обращения: 15.05.2025).

Взаимодействие Интерпола с экспертными группами по кибербезопасности и его сотрудничество с государствами — членами ШОС в сфере противодействия киберпреступности развиваются в принципиально разных форматах, отражающих особенности содействия при обеспечении кибербезопасности. В то время как в России и странах ШОС господствует государственный подход к обеспечению кибербезопасности [14], западный опыт показывает преимущества и недостатки международного содействия с привлечением широкого круга интересантов (multi-stakeholder) в соответствии с Глобальным цифровым договором 2024 г.[1]

Интерпол, обладая универсальным мандатом и глобальным охватом, выступает для ШОС центральным партнером в вопросах оперативного обмена информацией и координации расследований. В свою очередь, ШОС, фокусирующаяся на региональной безопасности в Центральной Азии и сопредельных регионах, предлагает Интерполу доступ к критическим данным о киберугрозах, включая деятельность хакерских групп, связанных с организованной преступностью и терроризмом.

Заключение

Усилия Международной организации уголовной полиции (Интерпола) в деле противодействия киберпреступности совпадают с целями и задачами Шанхайской организации сотрудничества по этой злободневной для обеспечения всеобъемлющей международной безопасности тематике. Вместе с тем далеко не все государства — члены ШОС принимают активное участие в операциях Интерпола по противодействию киберпреступности по ряду причин политического и правового характера.

Во-первых, любые операции Интерпола носят информационно-аналитический характер, который в своей проевропейской политизированной юридической оценке состояния угроз киберпреступности не может разделяться всеми государствами — членами ШОС. Поскольку Интерпол ориентирован только на борьбу с преступлениями международного характера по обычному уголовному праву (ordinary law crimes), постольку в условиях цифровой трансформации политизация дискурса вокруг киберпреступности приводит к правовым коллизиям в вопросах квалификации пропаганды терроризма и проявлений экстремизма в киберпространстве. Например, между исламскими республиками (Ираном и Пакистаном) и Китайской Народной Республикой существуют как много общего в деле понимания необходимости пресечения мошенничества и наркоторговли в Сети, так и принципиальные противоречия в вопросах реагирования на речевые правонарушения против официальной идеологии. Международное сотрудничество под эгидой Интерпола наглядно демонстрирует преимущество гармонизации уголовного законодательства. Международное уголовное право, характеризуя проявления политической преступности, призвано — в соответствии с Уставом ООН — опираться на позицию Совета Безопасности.

Во-вторых, развитие цифровых технологий приводит к появлению новых форм преступности, которые в ближайшее время потребуют инновационных методов работы как Интерпола, так и правоохранительных органов государств — членов ШОС. Успешная борьба с киберпреступностью предполагает способность международных организаций гибко и адаптивно реагировать на новые возможности искусственного интеллекта и робототехники. Технологическое лидерство государств — членов ШОС необходимо для успеха в борьбе с киберпреступностью, и работа по укреплению сотрудничества с Интерполом может способствовать юридическому признанию мировым сообществом не только аксиологической основы международного права, но и правил рационального использования цифровых инноваций и робототехники, что приведет к созданию более безопасного киберпространства.

В-третьих, партнерство Интерпола с региональными организациями и неправительственными структурами возможно только при условии их светского и профессионального характера. Участие профсоюзов полицейских, творческих ассоциаций и общественных движений в совершенствовании дефиниции кибертерроризма может способствовать широкому международному консенсусу в понимании границ допустимого поведения в виртуальном мире.

[1] Global Digital Compact 2024 [Электронный ресурс]. URL: https://www.un.org/digital-emerging-technologies/global-digital-compact (дата обращения: 15.05.2025).

Гармонизация национального законодательства о противодействии киберпреступности с принципами международного права и преодоление политических разногласий в Евразийском регионе позволят создать основанную на доверии и защищенную нормами международного уголовного права цифровую экосистему, где региональное лидерство ШОС дополняется глобальным охватом Интерпола и технологическими инновациями.

Список литературы

1. *Алескеров В. И., Баранов В. В.* Телекоммуникация и киберпространство как средство преступления экстремистской и террористической направленности // Труды Академии управления МВД России. 2020. № 1 (53). С. 104–113. EDN: MZGXHY.
2. *Алиева М. Н., Аримова С. А.* Деятельность Интерпола по раскрытию преступлений в компьютерной сфере // Закон и право. 2021. № 11. С. 194–196. EDN: MKHZPC. DOI: 10.24412/2073-3313-2021-11-194-196.
3. *Гончаров В. В.* Общественный контроль за филиалами и представительствами международных неправительственных организаций на территории России // Общество: политика, экономика, право. 2023. № 7 (120). С. 94–99. EDN: EKKZAR. DOI: 10.24158/pep.2023.7.11.
4. *Евдокимов К. Н., Хобонкова К. В.* К проблеме совершенствования международного сотрудничества в сфере противодействия киберпреступности // Сибирский юридический вестник. 2022. № 3 (98). С. 90–95. EDN: BEPXHH. DOI: 10.26516/2071-8136.2022.3.90.
5. *Каширкина А. А., Морозов А. Н.* Международно-правовое регулирование борьбы с коррупцией: уровни взаимодействия и потенциал развития // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2018. № 2 (42). С. 148–154. EDN: UUCSTA. DOI: 10.24411/2078-5356-2018-1002.
6. *Кириленко В. П., Алексеев Г. В.* Киберпреступность и цифровая трансформация // Теоретическая и прикладная юриспруденция. 2021. № 1. С. 39–53. EDN: UDZCMU. DOI: 10.22394/2686-7834-2021-1-39-53.
7. *Кириленко В. П., Хлутков А. Д., Алексеев Г. В.* Методология борьбы с экстремизмом в киберпространстве: опыт Шанхайской организации сотрудничества // Евразийская интеграция: экономика, право, политика. 2023. Т. 17, № 4. С. 29–42. EDN: SXNLED. DOI: 10.22394/2073-2929-2023-04-29-42.
8. *Мороз Н. О.* Деятельность Интерпола по координации сотрудничества в борьбе с преступностью в сфере высоких технологий // Вестник Полоцкого гос. ун-та. Сер. D. Экономич. и юрид. науки. 2011. № 14. С. 147–148. EDN: ULXVQD.
9. *Нижник Н. С., Лясович Т. Г.* Полицейская деятельность и профессиональная подготовка сотрудников органов внутренних дел как предмет правовых исследований // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. 2024. Т. 10 (76), № 1. С. 410–426. EDN: TYBDBP.
10. *Панченко В. Ю.* Правовое взаимодействие как вид социального взаимодействия. М. : Проспект, 2015. 232 с. ISBN: 978-5-392-18871-0. EDN: WOIQJU.
11. *Пузырева Ю. В., Мысина А. И.* Международное полицейское сотрудничество по вопросам раскрытия и расследования преступлений в сфере информационных технологий. М. : Инфра-М, 2020. 92 с. EDN: LEVJZF.
12. *Репецкая А. Л., Миронов А. О.* Криптовалюта как объект уголовно-правового и криминологического исследования // Вестник Восточно-Сибирского института МВД России. 2022. № 3 (102). С. 109–120. EDN: XLTNYQ. DOI: 10.55001/2312-3184.2022.78.15.010.
13. *Рыжов В. Б.* Участие Интерпола в борьбе с терроризмом // Международное право. 2020. № 2. С. 56–69. EDN: BHEFSS. DOI: 10.25136/2644-5514.2020.2.29854.
14. *Северин В. А.* Правовые аспекты обеспечения информационной безопасности цифровой экономики // Пробелы в российском законодательстве. 2023. Т. 16, № 8. С. 46–51. EDN: QIHBEF.
15. *Сергевнин С. Л.* К вопросу о факторах эффективности позитивного права // Теоретическая и прикладная юриспруденция. 2021. № 1. С. 7–17. EDN: VOYHYV. DOI: 10.22394/2686-7834-2021-1-7-17.
16. *Ситков А. С.* Международное сотрудничество полиции в рамках Интерпола по противодействию киберпреступности и обеспечению кибербезопасности // Вестник Московского университета МВД России. 2022. № 5. С. 238–242. EDN: TMBVAP. DOI: 10.24412/2073-0454-2022-5-238-242.
17. *Тихомиров Ю. А.* Юридическая коллизия, власть и правопорядок // Государство и право. 1994. № 1. С. 3–11. EDN: QYUJJL.
18. *Тихомиров Ю. А.* Мироустройство: устойчивость и распад // Журнал российского права. 2025. Т. 29, № 2. С. 5–16. EDN: RXKDYS. DOI: 10.61205/S160565900032645-3.

19. *Уткин Н. И., Ермолович Г. П., Воробейчикова А. А.* Американская система профилактики преступлений, связанных с ненавистью (Hate Crimes) // Вестник Санкт-Петербургского университета МВД России. 2001. № 2 (10). С. 153–158. EDN: GFNNVP.
20. *Юсупов М. Ю., Путилов А. О.* Фишинг как угроза конфиденциальности в сети // E-Scio. 2021. № 10 (61). С. 223–232. EDN: BSZNZY.
21. *Bartoli L.,* Cybersecurity and the Fight against Cybercrime: Partners or Competitors? // European Journal of Risk Regulation. 2025. Vol. 16, Iss. 2. P. 498–513. DOI: 10.1017/err.2025.31.
22. *Collin B. C.* The Future of Cyber Terrorism // Crime & Justice International. 1997. Vol. 13, No. 2. P. 15–18.
23. *Emmert F.* Cryptocurrencies: The Impossible Domestic Law Regime? // The American Journal of Comparative Law. 2022. Vol. 70, Iss. Supp_1. P. i185–i219. DOI: 10.1093/ajcl/avac022.
24. *Hadlington L, Chivers S.* Segmentation Analysis of Susceptibility to Cybercrime: Exploring Individual Differences in Information Security Awareness and Personality Factors // Policing: A Journal of Policy and Practice 2020. Vol. 14, Iss. 2. P. 479–492. DOI: 10.1093/police/pay027.
25. *Hustinx P.* Data Protection and International Organizations: A Dialogue between EU Law and International Law // International Data Privacy Law. 2021. Vol. 11, Iss. 2. P. 77–80. DOI: 10.1093/idpl/ipab015.
26. *Ling C. W.* Mapping Interpol's Evolution: Functional Expansion and the Move to Legalization // Policing: A Journal of Policy and Practice 2010. Vol. 4, Iss. 1. P. 28–37. DOI: 10.1093/police/pap060.
27. *Mačák K.* From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers // Leiden Journal of International Law. 2017. Vol. 30, Iss. 4. P. 877–899. DOI: 10.1017/S0922156517000358.
28. *Olivas Osuna, J. J.* The Pegasus Spyware Scandal: A Critical Review of Citizen Lab's "CatalanGate" report 2023. DOI: 10.13140/RG.2.2.17511.93603.
29. *Sandler T., Arce D. G., Enders W.* An Evaluation of Interpol's Cooperative-Based Counterterrorism Linkages // The Journal of Law & Economics. 2011. Vol. 54, Iss. 1. P. 79–110. DOI: 10.1086/652422.
30. *Shandler R., Gross M. L., Backhaus S., Canetti D.* Cyber Terrorism and Public Support for Retaliation — A Multi-Country Survey Experiment // British Journal of Political Science. 2022. Vol. 52, Iss. 2. P. 850–868. DOI: 10.1017/S0007123420000812.
31. *Wang X.* Global (re-)Framing of Cybercrime: An Emerging Common Interest in Flux of Competing Normative Powers? // Leiden Journal of International Law. 2024. P. 1–27. DOI: 10.1017/S0922156524000402.
32. *Zheng Z., Lin H.* SCO's Cyber Counterterrorism Law Enforcement Cooperation: Current Status, Challenges, and Countermeasures // Advances in Social Behavior Research. 2024. No. 9. P. 16–19. DOI: 10.54254/2753-7102/9/2024077.

Об авторах:

Сергевнин Сергей Львович, доктор юридических наук, заслуженный юрист Российской Федерации, профессор, декан юридического факультета, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Северо-Западный институт управления (Санкт-Петербург, Россия);
e-mail: sergevnin-sl@ranepa.ru; ORCID: 0000-0001-7397-4023

Алексеев Георгий Валерьевич, кандидат юридических наук, доцент, заведующий кафедрой международного и гуманитарного права, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Северо-Западный институт управления (Санкт-Петербург, Россия);
e-mail: alekseev-gv@ranepa.ru; ORCID: 0000-0003-3720-0105

Калкэй Елина Игоревна, преподаватель кафедры международного и гуманитарного права, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Северо-Западный институт управления (Санкт-Петербург, Россия);
e-mail: kalkey-ei@ranepa.ru ORCID: 0009-0009-1327-3722

References

1. Aleskerov, V. I., Baranov, V. V. Telecommunications and Cyberspace as Means of Extremist and Terrorist Crimes // Proceedings of Management Academy of the Ministry of the Interior of Russia. 2020. No. 1 (53). P. 104–113 (In Rus.). EDN: MZGXHY.

2. Alieva, M. N., Arimova, S. A. The Activities of Interpol in Solving Crimes in the Computer Sphere // Law and Legislation. 2021. No. 11. P. 194–196 (In Rus.). EDN: MKHZPC. DOI: 10.24412/2073-3313-2021-11-194-196.
3. Goncharov, V. V. Public Control over Branches and Representative Offices of International Non-Governmental Organizations in Russia // Society: Politics, Economics, Law. 2023. No. 7 (120). P. 94–99 (In Rus.). EDN: EKKZAR. DOI: 10.24158/pep.2023.7.11.
4. Evdokimov, K. N., Hobonkova, K. V. On the Problem of Improving International Cooperation in Countering Cybercrime // Siberian Law Review, 2022. No. 3 (98). P. 90–95 (In Rus.). EDN: BEPXHH. DOI: 10.26516/2071-8136.2022.3.90.
5. Kashirkina, A. A., Morozov, A. N. International Legal Regulation of Combating Corruption: The Level of Interaction and Potential for Development // Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia. 2018. No. 2 (42). P. 148–154 (In Rus.). EDN: UUCSTA. DOI: 10.24411/2078-5356-2018-1002.
6. Kirilenko, V. P., Alekseev, G. V. Cybercrime and Digital Transformation // Theoretical and Applied Law. 2021. No. 1. P. 39–53 (In Rus.). EDN: UDZCMU. DOI: 10.22394/2686-7834-2021-1-39-53.
7. Kirilenko, V. P., Khlutkov, A. D., Alekseev, G. V. Methodology for Combating Extremism in Cyberspace: Experience of the Shanghai Cooperation Organization // Eurasian Integration: Economic, Law, Politics. 2023. Vol. 17, No. 4. P. 29–42 (In Rus.). EDN: SXNLED. DOI: 10.22394/2073-2929-2023-04-29-42.
8. Moroz, N. O. Interpol Activity on Cooperation Coordination in Struggle against Criminality in the Sphere of High Technologies // Bulletin of Polotsk State University. Series D. Economic and Legal Sciences. 2011. No. 14. P. 147–148 (In Rus.). EDN: ULXVQD.
9. Nizhnik, N. S., Lyasovich, T. G. Policing and Professional Activities Training of Employees of the Internal Affairs Bodies as a Subject of Legal Research // Scientific notes of V. I. Vernadsky Crimean Federal University. Juridical science. 2024. Vol. 10 (76), No. 1. P. 410–426 (In Rus.). EDN: TYBDBP.
10. Panchenko, V. Yu. Legal Interaction as a Type of Social Interaction. Moscow : Prospect Publishing House, 2015. 232 p. ISBN: 978-5-392-18871-0 (In Rus.). EDN: WOIQJU.
11. Puzyreva, Yu. V., Mysina, A. I. International Police Cooperation in Investigating and Solving IT Crimes : monograph. Moscow : Infra-M, 2020. 92 p. (In Rus.). EDN: LEVJZF.
12. Repetskaya, A. L., Mironov, A. O. Cryptocurrency as an object of criminal law and criminological research // Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2022. No. 3 (102). P. 109–120 (In Rus.). EDN: XLTNYQ. DOI: 10.55001/2312-3184.2022.78.15.010.
13. Ryzhov, V. B. Interpol's Participation in the Fight against Terrorism // International Law. 2020. No. 2. P. 56–69 (In Rus.). EDN: BHEFSS. DOI: 10.25136/2644-5514.2020.2.29854.
14. Severin, V. A. Legal Aspects of Ensuring Information Security of the Digital Economy // Gaps in Russian Legislation. 2023. Vol. 16, No. 8. P. 46–51 (In Rus.). EDN: QIHBEF.
15. Sergevnin, S. L. On the Efficiency Factors of Positive Law // Theoretical and Applied Law. 2021. No. 1. P. 7–17 (In Rus.). EDN: VOYHYV. DOI: 10.22394/2686-7834-2021-1-7-17.
16. Sitkov, A. S. International Police Cooperation within the Framework of Interpol on Combating Cybercrime and Ensuring Cybersecurity // Bulletin of Moscow University of the Ministry of Internal Affairs of Russia. 2022. No. 5. P. 238–242 (In Rus.). EDN: TMBVAP. DOI: 10.24412/2073-0454-2022-5-238-242.
17. Tikhomirov, Yu. A. Legal Collision, Power and Law and Order // State and Law. 1994. No. 1. P. 3–11 (In Rus.). EDN: QYUJJL.
18. Tikhomirov, Yu. A. World Order: Stability and Disintegration // Journal of Russian Law. 2025. Vol. 29, No. 2. P. 5–16 (In Rus.). EDN: RXKDYS. DOI: 10.61205/S160565900032645-3.
19. Utkin, N. I., Ermolovich, G. P., Vorobeychikova, A. A. American System of Prevention of Crimes Related to Hatred // Vestnik of the St. Petersburg University of the Ministry of Internal Affairs of Russia. 2001. No. 2 (10). P. 153–158 (In Rus.). EDN: GFNNVP.
20. Yusupov, M. Yu., Putilov, A. O. Phishing as a Threat to Online Privacy // E-Scio. 2021. No. 10 (61). P. 223–232 (In Rus.). EDN: BSZNZY.
21. Bartoli, L. Cybersecurity and the Fight against Cybercrime: Partners or Competitors? // European Journal of Risk Regulation. 2025. Vol. 16, Iss. 2. P. 498–513. DOI: 10.1017/err.2025.31.
22. Collin, B. C. The Future of Cyber Terrorism // Crime & Justice International. 1997. Vol. 13, No. 2. P. 15–18.
23. Emmert, F. Cryptocurrencies: The Impossible Domestic Law Regime? // The American Journal of Comparative Law. 2022. Vol. 70, Iss. Supp_1. P. i185–i219. DOI: 10.1093/ajcl/avac022.

24. Hadlington, L, Chivers, S. Segmentation Analysis of Susceptibility to Cybercrime: Exploring Individual Differences in Information Security Awareness and Personality Factors // Policing: A Journal of Policy and Practice 2020. Vol. 14, Iss. 2. P. 479–492. DOI: 10.1093/police/pay027.
25. Hustinx, P. Data Protection and International Organizations: A Dialogue between EU Law and International Law // International Data Privacy Law. 2021. Vol. 11, Iss. 2. P. 77–80. DOI: 10.1093/idpl/ipab015.
26. Ling, C. W. Mapping Interpol's Evolution: Functional Expansion and the Move to Legalization // Policing: A Journal of Policy and Practice 2010. Vol. 4, Iss. 1. P. 28–37. DOI: 10.1093/police/pap060.
27. Mačák, K. From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers // Leiden Journal of International Law. 2017. Vol. 30, Iss. 4. P. 877–899. DOI: 10.1017/S0922156517000358.
28. Olivas Osuna, J. J. The Pegasus Spyware Scandal: A Critical Review of Citizen Lab's "CatalanGate" report 2023. DOI: 10.13140/RG.2.2.17511.93603.
29. Sandler, T., Arce, D. G., Enders, W. An Evaluation of Interpol's Cooperative-Based Counterterrorism Linkages // The Journal of Law & Economics. 2011. Vol. 54, Iss. 1. P. 79–110. DOI: 10.1086/652422.
30. Shandler, R., Gross, M. L., Backhaus, S., Canetti, D. Cyber Terrorism and Public Support for Retaliation — A Multi-Country Survey Experiment // British Journal of Political Science. 2022. Vol. 52, Iss. 2. P. 850–868. DOI: 10.1017/S0007123420000812.
31. Wang, X. Global (re-)Framing of Cybercrime: An Emerging Common Interest in Flux of Competing Normative Powers? // Leiden Journal of International Law. 2024. P. 1–27. DOI: 10.1017/S0922156524000402.
32. Zheng, Z., Lin, H. SCO's Cyber Counterterrorism Law Enforcement Cooperation: Current Status, Challenges, and Countermeasures // Advances in Social Behavior Research. 2024. No. 9. P. 16–19. DOI: 10.54254/2753-7102/9/2024077.

About the authors:

Sergey L. Sergevnin, Doctor of Science (Jurisprudence), Professor, Honored Lawyer of the Russian Federation, Dean of the Faculty of Law, Russian Presidential Academy of National Economy and Public Administration, North-West Institute of Management (Saint Petersburg, Russia);
e-mail: sergevnin-sl@ranepa.ru; ORCID: 0000-0001-7397-4023

George V. Alexeyev, PhD in Jurisprudence, Associate Professor, Head of the Department of International and Humanitarian Law, Russian Presidential Academy of National Economy and Public Administration, North-West Institute of Management (Saint Petersburg, Russia);
e-mail: alekseev-gv@ranepa.ru; ORCID: 0000-0003-3720-0105

Elina I. Kalkey, Lecturer Russian Presidential Academy of National Economy and Public Administration, North-West Institute of Management (Saint Petersburg, Russia);
e-mail: kalkey-ei@ranepa.ru; ORCID: 0009-0009-1327-3722