УГОЛОВНО-ПРАВОВЫЕ НАУКИ

Научная статья
УДК 343
DOI: 10.18384/2949-513X-2025-1-74-82

О ВОЗМОЖНОСТЯХ И ПЕРСПЕКТИВАХ СОЗДАНИЯ МЕЖДУНАРОДНОЙ СИСТЕМЫ БОРЬБЫ С СОВРЕМЕННОЙ ПРОФЕССИОНАЛЬНОЙ КИБЕРПРЕСТУПНОСТЬЮ

Зарубина К. А.*, Чапчиков С. Ю.
[1]Юго-Западный государственный университет, г. Курск, Российская Федерация
**Корреспондирующий автор, e-mail: kris1996z@mail.ru; ORCID: 0000–0003–2725–6906*

Поступила в редакцию 28.12.2024
После доработки 20.01.2025
Принята к публикации 17.02.2025

Аннотация
Цель. Анализ современной международной системы противодействия профессиональной киберпреступности и разработка предложений по её модернизации с учётом угроз и вызовов современности.
Процедура и методы. В работе использовались сравнительно-правовой, исторический и системный методы, а также методы анализа, синтеза и обобщения.
Результаты. Определено, что профессиональная киберпреступность сегодня представляет реальную угрозу для безопасности государства и характеризуется трансграничностью, что обуславливает консолидацию усилий всего международного сообщества для противодействия этому опасному явлению. Установлены риски противодействия таким преступлениям, предложены меры по совершенствованию данной системы с учётом имеющегося опыта международного сотрудничества в этой сфере.
Теоретическая и/или практическая значимость. Сформулированы конкретные предложения по модернизации системы мер противодействия профессиональной киберпреступности. Обобщён новый теоретический материал по исследуемой теме.

Ключевые слова: киберпреступность, международная система, мировое сообщество, противодействие, профессиональная киберпреступность.

Благодарности. Исследование подготовлено в рамках выполнения госзадания «Правовые меры обеспечения стратегических приоритетов по противодействию угрозам национальной безопасности» (FENM-2025-0010). Регистрационный номер 1024031900131-7-5.5.1.

Для цитирования:
Зарубина К. А., Чапчиков С. Ю. О возможностях и перспективах создания международной системы борьбы с современной профессиональной киберпреступностью // Московский юридический журнал. 2025. № 1. С. 74–82. https://doi.org/10.18384/2949-513X-2025-1-74-82.

Original research article

ON THE POSSIBILITIES AND PROSPECTS OF CREATING AN INTERNATIONAL FRAMEWORK AGAINST MODERN PROFESSIONAL CYBERCRIME

K. Zarubina*, S. Chapchikov
South-West State University, Kursk, Russian Federation
**Corresponding author, e-mail: kris1996z@mail.ru; ORCID: 0000–0003–2725–6906*

Received by the editorial office 28.12.2024
Revised by the author 20.01.2025
Accepted for publication 17.02.2025

Abstract
Aim. To analyze both modern international framework against professional cybercrime and the development of proposals for its modernization, considering modern threats and challenges.
Methodology. Comparative, legal, historical, and systematic methods, analysis, synthesis, and generalization were used in the work.
Results. It is determined that professional cybercrime today poses a real threat to the interests of society and the state and is characterized by cross-border activity, which leads to the consolidation of efforts by the entire international community to counter this criminal phenomenon. Despite certain risks, measures have been proposed to counter such crimes, considering the existing experience of international cooperation in this area.
Research implications. Proposals have been formulated to modernize the framework against professional cybercrime. At the theoretical level, the new material on the topic under study has been summarized.

Keywords: cybercrime, international system, global community, counteraction, professional cybercrime

Acknowledgements. was prepared within the framework of the implementation of state assignment "Legal Measures to Ensure Strategic Priorities to Counter Threats to National Security" (FENM-2025-0010). Registration number 1024031900131-7-5.5.1.

For citation:
Zarubina, K .A. & Chapchikov, S. Yu. (2025). On The Possibilities and Prospects of Creating an International Framework Against Modern Professional Cybercrime. In*: Moscow Juridical Journal*, 1, C. 74–82. https://doi.org/10.18384/2949-513X-2025-1-74-82.

Введение

Современная виртуальная среда развивается чрезвычайно высокими темпами. В киберпространство в настоящее время переместилась большая часть денежных транзакций, наличные денежные средства постепенно выходят из оборота, а безналичные, напротив, всё активнее используются как юридическими, так и физическими лицами. Цифровая среда сегодня позволяет удалённо оплатить товары и услуги, перевести денежные средства на счёт другого пользователя практически любого онлайн-сервиса, заказать доставку продуктов питания, получить заработную плату и мн. др. Согласно последним статистическим данным, представленным Центральным банком РФ, доля безналичных платежей в розничном обороте в России по итогам 2024 г. составила 85,8%, а на 1 апреля 2025 г. в системе быстрых платежей было совершено 28,7 мдрд операций на 143,3 трлн рублей[1]. Как видим, большая часть населения страны ввиду удобства предпочитает использовать именно без-

[1] Национальная платёжная система обеспечивает безналичные расчёты и платежи граждан и юридических лиц // Банк России: [сайт]. URL: https://www.cbr.ru/PSystem (дата обращения: 10.10.2024).

наличные денежные средства, ставшие неотъемлемой частью современной национальной платёжной системы.

Профессиональная киберпреступность сегодня

Однако перемещение платёжных операций в «виртуальное» пространство создаёт определённые риски для граждан ввиду недостаточно высокой степени защищённости экономических отношений в киберсреде, в то время как преступники (особенно преступники-профессионалы, имеющие необходимые криминальные умения и навыки, а также цель «заработка» на совершении преступлений) получают дополнительные возможности для ведения преступной деятельности в киберпространстве или с использованием кибертехнологий. На высокую степень опасности современной корыстной профессиональной киберпреступности как разновидности преступной деятельности, осуществляемой в киберпространстве и характеризующейся наличием у преступников соответствующих криминальных знаний, умений, навыков, специализации и восприятия ими совершения преступлений как средства для получения постоянного дохода, указывает множество обстоятельств, что находит своё непосредственное отражение в отечественных документах стратегического планирования.

В Доктрине информационной безопасности РФ[1] устанавливается, что к современным информационным угрозам России относится использование трансграничного оборота информации для достижения криминальных целей в ущерб стратегической стабильности. В п. 14 данного нормативного правового акта определяется, что в настоящее время в Российском государстве возрастают масштабы компьютерной преступности, в первую очередь в кредитно-финансовой сфере, а методы и средства совершения таких преступных посягательств становятся всё изощрённее[2].

Стратегия национальной безопасности РФ[3] также определяет, что «быстрое развитие информационно-коммуникационных технологий сопровождается повышением вероятности возникновения угроз безопасности граждан, общества и государства», уточняя, что совершение преступлений с использованием таких технологий характеризуется в современности высокой анонимностью, что создаёт дополнительные угрозы национальной безопасности страны, а также благосостоянию её граждан, в т. ч. в сфере цифровой экономики (п. 57).

Развитие современного отечественного законодательства в сфере противодействия киберпреступности, всё чаще характеризующейся криминальным профессионализмом, также указывает на высокие темпы развития данного криминального явления и значительную опасность такой преступной деятельности для граждан, общества и государства. В качестве примера укажем на принятие Федерального закона № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации»[4], в котором устанавливаются организацион-

[1] Указ Президента РФ от 05.12.2016 № 646 // Президент России: [сайт]. URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 10.10.2024).

[2] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Президент России: [сайт]. URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 10.10.2024).

[3] Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // Президент России: [сайт]. URL: http://www.kremlin.ru/acts/bank/47046 (дата обращения: 10.04.2024).

[4] Федеральный закон 01.04.2025 № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» от [Электронный документ]. URL: http://www.kremlin.ru/acts/bank/51783 (дата обращения: 10.10.2024).

но-правовые механизмы противодействия правонарушениям с использованием интернет-технологий, в т. ч. преступным посягательствам интернет-мошенников, чья деятельность в настоящее время характеризуется исходя из специфики их криминального поведения именно как профессиональная преступная.

Как видим, и документы стратегического планирования, и законодательные новеллы в сопряжении с материалами современной судебной практики[1] указывают на особую распространённость в настоящее время не просто киберпреступности, а «промысла» профессиональных преступников, «орудующих» в киберпространстве или с использованием кибертехнологий [7, с. 53–56]. Однако указанная разновидность преступности является сложным криминальным явлением, отличающимся не только динамичностью развития, постоянным совершенствованием форм и методов преступной деятельности, её высокой интеллектуальностью, технологичностью, анонимностью и латентностью, но и трансграничностью [2, с. 56–64].

Главной особенностью цифрового пространства, в котором «промышляют» такие преступники, как раз и является отсутствие государственных границ, зачастую, сковывающих деятельность «традиционных» правонарушителей. Киберпространство существует вне территорий государств и позволяет совершать преступления, находясь на значительном удалении от жертвы преступления – в другом регионе, стране или даже континенте. Как справедливо отмечают К. Н. Евдокимов и К. В. Хобонкова, «киберпреступники, являясь частью технического "андеграунда" мирового сообщества, не разделяют себя по национальному признаку» и распространяют свою криминальную «активность» на разные регионы [3, с. 90–95], что также повышает степень опасности преступной деятельности такого рода.

В качестве примера укажем на деятельность так называемых мошеннических телефонных колл-центров, «атакующих» россиян звонками, сообщениями и вирусными программами с территории Украины. По утверждению депутата Государственной Думы РФ А. И. Немкина, за день из каждого такого колл-центра совершается до 10 тыс. звонков, что подвергает российских граждан и их сбережения реальной опасности[2]. Однако трансграничность подобного рода преступной деятельности, имеющей все признаки проявления криминального профессионализма (от наличия преступной специализации до извлечения постоянного дохода от совершения данных посягательств), значительно осложняет процесс противодействия такого рода преступной деятельности и обуславливает необходимость разработки мер пресечения совершения таких преступлений не только на уровне отдельно взятого государства, но и на наднациональном уровне.

Правовая регламентация потиводействия профессиональной киберпреступности на международном уровне

Усилиями отдельных государств, по верному утверждению современных исследователей, уже неоднократно предпринимались попытки разработки и принятия универсального нормативно-правового акта, положения которого позволяли бы организовывать противодействие как профессиональной, так и «традиционной» киберпреступности, в т. ч. за счёт международного сотрудничества [4, с. 305–310]. Так, Конвенцией о преступности в сфере компьютерной информации ETS № 185[3]

[1] *См.*: Приговор № 1-352/2014 от 08.08.2014 (Самарская область) [Электронный ресурс]. URL: https://sudact.ru/regular/doc/tiO9I4eFimQW (дата обращения: 27.07.2024); Приговор № 1-617/2023 от 05.09.2023 по делу № 1-617/2023, С. городской суд (Республика Коми) [Электронный ресурс]. URL: https://sudact.ru/regular/doc/e82eh3iuUxbK (дата обращения: 27.09.2024).

[2] В ГД рассказали о мошеннических украинских колл-центрах, атакующих россиян // РИА Новости: [сайт]. URL: https://ria.ru/20240706/ukraina-1957808640.html (дата обращения: 10.10.2024).

[3] Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября

(Будапешт), ратифицированной государствами-членами Совета Европы и некоторыми иными странами, предусматривается, к примеру, выполнение каждой стороной обязательства о принятии законодательных и иных мер, необходимых для того, чтобы квалифицировать в качестве преступления, согласно её внутригосударственному праву, любое вмешательство в функционирование компьютерной системы с мошенническим или бесчестным намерением неправомерного извлечения экономической выгоды для себя или для иного лица (ст. 8).

Особо в сфере организационно-правового противодействия киберпреступности на наднациональном уровне выделяется Соглашение о сотрудничестве в области обеспечения международной информационной безопасности[1], в котором унифицировано понятие *information crime* (информационное преступление), а в качестве основных направлений сотрудничества государств определены противодействие информационной преступности, совершенствование международно-правовой базы и практических механизмов взаимодействия сторон в обеспечении международной информационной безопасности, создание условий для взаимодействия национальных компетентных органов в целях реализации данного соглашения и др. Указанное соглашение Российской Федерацией не ратифицировано.

Среди международных нормативных правовых актов также выделим Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий[2]. Данным нормативным правовым актом стороны признают в соответствии с национальным законодательством в качестве уголовно наказуемых такие деяния, как «хищение имущества путём изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путём введения в компьютерную систему ложной информации, либо сопряжённое с несанкционированным доступом к охраняемой законом компьютерной информации». Среди форм международного сотрудничества определены: обмен информацией, исполнение соответствующих запросов по предупреждению, выявлению, пресечению, раскрытию и расследованию таких преступлений, планирование и проведение скоординированных мероприятий и операций по предупреждению, выявлению, пресечению, раскрытию и расследованию преступлений в сфере информационных технологий и другие формы.

Кроме того, укажем на одну из последних законодательных новелл, регулирующих отношения в данной сфере, – Конвенцию Организации Объединённых Наций против киберпреступности[3] (Конвенция ООН), разработанную по инициативе России [5, с. 65–69] и принятую резолюцией 79/243 Генеральной Ассамблеей (церемония подписания Конвенции ООН была проведена в Социалистической Республике Вьетнам в 2025 г.). Конвенция нацелена на борьбу с киберхищениями, кибермошенничествами, отмыванием доходов от противоправных деяний в «виртуальном пространстве». В документе также содержатся положения о закреплении

2001 г.) // Гарант: [сайт]. URL: https://base.garant.ru/4089723 (дата обращения: 10.10.2024).

[1] Соглашение о сотрудничестве в области обеспечения международной информационной безопасности от 16.06.2009 (Шанхай) [Электронный ресурс]. URL: https://cis-legislation.com/document.fwx?rgn=28340 (дата обращения: 10.10.2024).

[2] Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 28.09.2018 (ратифицировано Федеральным законом от 01.07.2021 № 237-ФЗ) [Электронный ресурс]. URL: https://docs.cntd.ru/document/351210645?marker=7DS0KD (дата обращения: 10.10.2024).

[3] Конвенция Организации Объединённых Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определёнными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьёзным преступлениям [Электронный ресурс]. URL: https://www.un.org/ru/documents/treaty/A-RES-79-243 (дата обращения: 10.10.2024).

цифрового суверенитета государств над своим информационным пространством, определены направления международного взаимодействия между компетентными ведомствами в данной области.

Безусловно, рассмотренные выше и иные попытки правовой регламентации системы отношений по противодействию киберпреступности, предпринимаемые усилиями международного сообщества, направлены на борьбу с её разными проявлениями (от кибертерроризма до профессиональных киберхищений). Однако комплексно проблема борьбы с профессиональными киберпреступниками по-прежнему не решена. Указанные международные соглашения, во-первых, ратифицированы не всеми государствами, во-вторых, охватывают не все аспекты противодействия именно профессиональной киберпреступности как одному из наиболее опасных видов преступной деятельности такого рода. И, в-третьих, данные организационно-правовые механизмы не в полной мере отвечают высокотехнологичному «оснащению» профессионального мира киберпреступников, зачастую, опережающего темпы научно-технического прогресса в цифровой сфере. Вместе с этим, считаем, что решение данной проблемы должно быть предложено и разработано именно на международном уровне, поскольку профессиональная киберпреступность является современной криминальной угрозой для всего мирового сообщества.

Полагаем, что помимо ратификации большей частью государств Конвенции ООН против киберпреступности, направленной на противодействие киберпреступности в целом и профессиональной киберпреступности в частности, на международном уровне для решения обозначенной проблемы также необходимо разработать следующие вопросы:

– обязать поставщиков серверов и услуг своевременно и в полном объёме уведомлять соответствующие национальные органы государственной власти и их структуры обо всех уязвимых местах киберпространства, а также принимать эффективные меры по их устранению, собирать и хранить до востребования в целях обеспечения международной кибербезопасности персональные данные о пользователях с их предварительным обязательным уведомлением;

– запретить передачу персональных данных пользователей третьим лицам, их раскрытие, изменение или удаление, за исключением предоставления необходимой информации уполномоченным органам государственной власти, которые занимаются охраной кибербезопасности страны;

– установить обязательную верификацию пользователей для доступа к сети Интернет;

– ускорить работу по согласованию национально-правовых систем в вопросе выработки единых международных стандартов криминализации профессиональных киберпреступлений;

– регламентировать процедурные аспекты борьбы с профессиональной киберпреступностью, в частности, уточнить вопросы территориальной подсудности при проведении расследований таких преступлений, осуществления следственных действий в отношении иностранных граждан, являющихся потерпевшими, свидетелями, обвиняемыми по таким составам преступлений, проведения соответствующих криминалистических экспертиз и т. п.;

– создать в рамках международного сотрудничества единую базу обмена информацией между интернет-провайдерами, операторами сотовой связи и соответствующими правоохранительными органами государств в целях оперативного фиксирования «цифровых следов» преступлений, обнаружения и идентификации профессиональных киберпреступников и пресечения их общественно опасной деятельности в условиях трансграничности указанного вида преступности.

Указанный перечень мер может быть расширен и более детально разработан с учётом меняющихся цифровых вызовов современности и новых угроз, создаваемых криминальным сообществом

киберпрофессионалов. Однако при всём положительном эффекте создания коллективной системы противодействия профессиональной киберпреступности к разработке подобного рода международных организационно-правовых механизмов стоит подходить осторожно, поскольку в данном случае, по верному утверждению отдельных исследователей, в угоду защиты кибербезопасности мирового сообщества могут быть нарушены принципы обеспечения национальной безопасности и суверенности отдельно взятых государств [6, с. 28–41]. В качестве примера укажем на п. «b» ст. 32 Конвенции о преступности в сфере компьютерной информации ETS № 185 (Будапешт), в котором, по справедливому утверждению О. И. Лепёшкиной, создаётся правовая возможность для нарушения суверенитета государств-участников посредством закрепления положения о возможности трансграничного доступа к компьютерным данным, хранящимся в другом государстве, без его согласия [7, с. 82–91]. Ввиду этого Российская Федерация, подписав данный НПА, была вынуждена отозвать подпись в связи с имеющимися разногласиями относительно указанных условий [8, с. 60–71; 9, с. 83–89]. Кроме того, определённые опасения вызывает современная международная политическая риторика, препятствующая «нормальному» диалогу государств в решении общих для мирового сообщества проблем, в числе которых и противостояние трансграничным криминальным угрозам, таким как профессиональная киберпреступность.

Однако, соглашаясь с мнением А. А. Цримова, отметим, что для формирования действительно эффективной системы противодействия киберпреступности в целом и её разновидности профессиональной киберпреступности в частности необходимо реализовать соответствующие меры борьбы с данным криминальным явлением по нескольким направлениям: совершенствование правовой базы, технических мер, организационной работы уполномоченных структур, а также в общем международного сотрудничества в рассматриваемой сфере [10, с. 146–150]. При этом гармонизация национально-правовых систем в области борьбы с киберпреступностью (в т. ч. ипрофессиональной) является необходимым условием противодействия таким преступлениям [11, с. 317–322].

Заключение

Таким образом, процесс сдерживания профессиональной киберпреступности имеет сложный и дискретный характер, как ввиду специфики криминальной деятельности такого рода, так и вследствие влияния общей международной обстановки и новых для обеспечения национальной безопасности государств вызовов, создающих дополнительные риски. Между тем трансграничность профессиональной киберпреступности как важнейшая характеристика указанного вида преступной деятельности в условиях современности обуславливает разработку и принятие на международном уровне программных, стратегических актов правового регулирования соответствующего круга отношений.

Несмотря на то, что ООН в данном вопросе (посредством разработки и рассмотрения в декабре 2024 г. Конвенции по борьбе с киберпреступностью) возьмёт на себя координирующую роль, проблема противодействия именно профессиональной криминальной деятельности киберпреступников по-прежнему актуальна. Вследствие этого полагаем, что для решения обозначенной проблемы необходимы не только ратификация Конвенции ООН большинством современных государств, но и дальнейшее международное сотрудничество в данной отрасли.

С целью решения указанной проблемы предложено:

1) усилить взаимодействие между поставщиками серверов и услуг и уполномоченными национальными органами государственной власти (в т. ч. создать в рамках международного сотрудничества единую базу обмена информацией между интернет-провайдерами, операторами со-

товой связи и соответствующими уполномоченными правоохранительными органами); запретить передачу персональных данных пользователей третьим лицам, их раскрытие, изменение или удаление;

2) установить обязательную верификацию пользователей для доступа к сети Интернет;

3) ускорить работу по согласованию национально-правовых систем в вопросе выработки единых международных стандартов криминализации профессиональных киберпреступлений;

4) уточнить вопросы территориальной подсудности при проведении расследований профессиональных киберпреступлений, имеющих признаки трансграничности, осуществлении соответствующих следственных действий и криминалистических экспертиз.

ЛИТЕРАТУРА

1. Аккаева Х. А. Киберпреступления: криминологический анализ // Право и управление. 2025. № 1. С. 317–322.
2. Астахова Е. А. Перспективы противодействия использованию информационно-коммуникационных технологий в преступных целях // Правовая политика и правовая жизнь. 2025. № 1. С. 56–64.
3. Горелик И. Б. Роль международных организаций в процессе противодействия киберпреступности // Международное право. 2022. № 3. С. 28–41.
4. Горелик И. Б. Формирование международно-правовой системы противодействия киберпреступности: от терминологии до проекта универсальной конвенции // Международное право. 2022. № 4. С. 60–71.
5. Евдокимов К. Н., Хобонкова К. В. К проблеме совершенствования международного сотрудничества в сфере противодействия киберпреступности // Сибирский юридический вестник. 2022. № 3. С. 90–95.
6. Кобец П. Н. Совершенствование межгосударственного сотрудничества в сфере информационной безопасности: основа противодействия международной киберпреступности // Вестник Белгородского юридического института МВД России имени И. Д. Путилина. 2023. № 1. С. 83–89.
7. Лакомов А. С. Киберпреступность: современные тенденции // Академическая мысль. 2019. № 2. С. 53–56.
8. Лепешкина О. И. Киберпреступность как угроза национальной безопасности // Теоретическая и прикладная юриспруденция. 2022. № 2. С. 65–69.
9. Лепешкина О. И. Международное сотрудничество государств СНГ по противодействию киберпреступности // Евразийская интеграция: экономика, право, политика. 2023. Т. 17. № 4. С. 82–91.
10. Цримов А. А. Отражение киберпреступлений в российском и международном правовом поле // Право и управление. 2023. № 2. С. 146–150.
11. Шестак В. А., Чеботарь А. С. Будапештская конвенция как основополагающий механизм противодействия киберпреступности: новации и перспективы международно-правового регулирования // Образование и право. 2023. № 8. С. 305–310.

REFERENCES

1. Akkaeva, H. A. (2025). Cybercrime: Criminological Analysis. In: *Law and Management*, 1, 317–322 (in Russ.).
2. Astakhova, E. A. (2025). Prospects to Counteract the Use of Information and Communication Technologies for Criminal Purposes. In: *Legal Policy and Legal Life*, 1, 56–64 (in Russ.).
3. Gorelik, I. B. (2022). The Role of International Organizations in Counteraction to Cybercrime. In: *International Law*, 3, 28–41 (in Russ.).
4. Gorelik, I. B. (2022). Formation of the International Legal System for Combating Cybercrime: From Terminology to a Universal Convention Draft. In: *International Law*, 4, 60–71 (in Russ.).
5. Evdokimov, K. N. & Khobonkova, K. V. (2022). On the Problem of Improving International Cooperation in Combating Cybercrime. In: *Siberian Law Herald*, 3, 90–95 (in Russ.).
6. Kobets, P. N. (2023). Improving Interstate Cooperation in Information Security: Basis to Combat International Cybercrime. In: *Vestnik of Putilin Belgorod Law Institute of Ministry of the Interior of Russia*, 1, 83–89 (in Russ.).

7. Lakomov, A. S. (2019). Cybercrime: Modern Trends. In: *Academic Thought*, 2, 53–56 (in Russ.).
8. Lepeshkina, O. I. (2022). Cybercrime as a Threat to National Security. In: *Theoretical and Applied Law*, 2, 65–69 (in Russ.).
9. Lepeshkina, O. I. (2023). International Cooperation of the CIS States in Combating Cybercrime. In: *Eurasian Integration: Economics, Law, Politics*, 17-4, 82–91 (in Russ.).
10. Tsrimov, A. A. (2023). Cybercrime Reflections in the Russian and International Legal Field. In: *Law and Management*, 2, 146–150 (in Russ.).
11. Shestak, V. A. & Chebotar, A. S. (2023). The Budapest Convention as a Fundamental Mechanism to Combat Cybercrime: Innovations and Prospects for International Legal Regulation. In: *Education and Law*, 8, 305–310 (in Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Зарубина Кристина Александровна (г. Курск) – кандидат исторических наук, старший преподаватель кафедры теории и истории государства и права Юго-Западного государственного университета;
e-mail: kris1996z@mail.ru; ORCID: 0000–0003–2725–6906;
Чапчиков Сергей Юрьевич (г. Курск) – доктор юридических наук, профессор, профессор кафедры теории и истории государства и права Юго-Западного государственного университета;
e-mail: tgpKSTU@yandex.ru; ORCID: 0009-0008-1785-1019

INFORMATION ABOUT THE AUTHORS

Kristina A. Zarubina (Kursk) – Cand. Sci. (History), Senior Lecturer, Department of Theory and History of State and Law, South-West State University;
e-mail: kris1996z@mail.ru; ORCID: 0000–0003–2725–6906
Sergey Yu. Chapchikov (Kursk) – Dr. Sci. (Law), Prof., Department of Theory and History of State and Law, South-West State University;
e-mail: tgpKSTU@yandex.ru; ORCID: 0009-0008-1785-1019