Научная статья
УДК 343

Совершенствование противодействия киберпреступности на пространстве Содружества Независимых Государств

Т. В. Прокофьева

Московский государственный лингвистический университет, Москва, Россия
prokofftv@list.ru

Аннотация. В статье рассматривается состояние преступности в сфере информационных технологий на территории государств – участников СНГ; анализируется действующая в рамках СНГ межгосударственная правовая база по борьбе с киберпреступностью, в том числе модельное законодательство СНГ, а также уголовное законодательство стран Содружества в указанной сфере. Определены актуальные направления совершенствования противодействия киберпреступности на пространстве СНГ.

Ключевые слова: киберпреступность, преступность в сфере информационных технологий, правовое регулирование, модельный закон, противодействие киберпреступности, Содружество Независимых Государств

Для цитирования: Прокофьева Т. В. Совершенствование противодействия киберпреступности на пространстве Содружества Независимых Государств // Вестник Московского государственного лингвистического университета. Образование и педагогические науки. 2023. Вып. 4 (849). С. 108–114.

Original Article

Improving Counteraction to Cybercrime in the Commonwealth of Independent States

Tatyana V. Prokofieva

Moscow State Linguistic University, Moscow, Russia
prokofftv@list.ru

Abstract. The article examines the state of crime in the area of information technology on the territory of the CIS member states; analyzes the current interstate legal framework aimed at combating cybercrime within the CIS, including the model legislation of the CIS, as well as the criminal legislation of the Commonwealth countries in this area, identifies imperative directions for improving cybercrime counteraction in the CIS.

Keywords: cybercrime, information technology crime, legal regulation, model law, countering cybercrime, Commonwealth of Independent States

For citation: Prokofieva, T. V. (2023). Improving counteraction to cybercrime in the Commonwealth of Independent States. Vestnik of Moscow State Linguistic University. Education and Teaching, 4(849), 108–114.

ВВЕДЕНИЕ

Интеграция информационного пространства вполне закономерно повлияла на то, что практически все сферы жизнедеятельности оказались погруженными в цифровую среду. Динамичное развитие информационных отношений отразилось на социально-негативной деятельности, что повлекло за собой и рост преступлений, совершенных с использованием информационно-коммуникационных технологий (ИКТ), или киберпреступлений. Распространяя свое влияние на территории целого ряда государств, легко нарушая границы, киберпреступность стала глобальной угрозой мирового масштаба, что требует объединения усилий компетентных органов зарубежных стран. Особую значимость вопросы консолидации приобретают для государств – участников СНГ, поскольку помимо тесной геополитической связи есть сходство как в построении правоохранительной системы, так и в национальном законодательстве.

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ НА ПРОСТРАНСТВЕ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

На сегодняшний день согласно Концепции дальнейшего развития Содружества Независимых Государств к числу приоритетных направлений деятельности СНГ относится сотрудничество в сфере противодействия трансграничной преступности в любых ее формах и проявлениях, а также в области обеспечения международной информационной безопасности и противодействия преступлениям в сфере ИКТ[1].

Однако практика показывает, что существующий механизм международного сотрудничества не смог быстро адаптироваться к стремительной кибертрансформации преступности.

Согласно статистическим данным за последние несколько лет отмечается существенный рост регистрируемой преступности в сфере информационных технологий. В 2022 году общее число таких преступлений, совершенных на территории государств – участников СНГ, по сравнению с 2019 годом увеличилось почти в 2,7 раза (2019 год – 196556; 2022 год – 538438 преступлений)[2].

Характеризуя структуру киберпреступности, следует отметить, что «наибольшее количество преступлений (порядка 82 %), совершенных с применением ИКТ, составляют разного рода хищения (мошенничество, кража), далее в процентном соотношении следуют преступления, связанные со сбытом наркотических средств и психотропных веществ (около 8–9 %), условное третье место (порядка 6–7 %) занимают противоправные деяния, связанные с экстремистской деятельностью и вовлечением несовершеннолетних в различные деструктивные группы суицидальной направленности (синий кит), на другие виды преступлений, относимых к рассматриваемой категории, приходится до 4 %» [Волков, 2022, с. 13].

Если говорить о преобладающих в структуре киберпреступности хищениях, совершенных с применением ИКТ, то в 85 % случаев это хищение денежных средств с расчетных счетов граждан (так называемые интернет-мошенничества).

Еще раз следует отметить, что особую сложность при раскрытии представляют трансграничные преступления, которые совершаются с территории зарубежных стран.

В связи с этим ключевое место в вопросах борьбы с преступлениями в сфере информационно-коммуникационных технологий, а также по линии обеспечения международной информационной безопасности занимает формирование международно-правовой базы сотрудничества стран в указанной области деятельности.

На разных международных площадках ведется активная работа по формированию международно-правовой базы противодействия преступности в информационном пространстве. Несмотря на это, единого общего (универсального) и приемлемого для всех документа (соглашения), расширяющего область международного взаимодействия в вопросах борьбы с киберпреступностью, пока нет.

В настоящее время на площадке ООН осуществляется доработка проекта такого универсального документа, принятие которого стало возможным благодаря усилиям Российской Федерации, внесшей 27 июля 2021 года российский проект договора (соглашения) по борьбе с киберпреступностью в Спецкомитет ООН. Итоговый проект документа Спецкомитет должен представить в ходе 78-й сессии Генассамблеи ООН (в 2024 году)[3].

Переходя к анализу правового регулирования взаимодействия стран Содружества, следует констатировать, что в рамках СНГ сформирована межгосударственная нормативная правовая база, регламентирующая вопросы борьбы с преступлениями, совершаемыми с использованием ИКТ.

[1] Концепция дальнейшего развития Содружества Независимых Государств (Решение Совета глав государств СНГ от 18 декабря 2020 года). URL: https://e-cis.info/page/3775/?ysclid=lkqw61ke3j399343766

[2] Сборник «О состоянии преступности и результатах расследования преступлений» на территории государств-участников СНГ за период 2019–2022 гг. (Форма № 785). М.: ФКУ «ГИАЦ МВД России».

[3] URL: https://mid.ru/ru/foreign_policy/news/1910382/

В числе основополагающих договорно-правовых документов следует назвать: Конвенцию о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам (г. Минск, 22 января 1993 года)[1]; Конвенцию о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам (г. Кишинев, 7 октября 2002 года)[2]; Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступностью (г. Москва, 25 ноября 1998 года)[3]; Соглашение об обмене информацией в сфере борьбы с преступностью (г. Астана, 22 мая 2009 года)[4]; Соглашение о сотрудничестве государств – участников СНГ в области обеспечения информационной безопасности (г. Санкт-Петербург, 20 ноября 2013 г.)[5], где впервые был закреплен термин «информационная преступность», определяющий ее как использование информационных ресурсов и / или воздействие на них в информационном пространстве в противоправных целях; Соглашение о порядке создания и деятельности совместных следственно-оперативных групп на территориях государств – участников СНГ (16 октября 2015 года, п. Бурабай, Казахстан)[6]; Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий (г. Душанбе, 28 сентября 2018 года)[7].

Вместе с тем наличие сформированной межгосударственной правовой базы противодействия киберпреступности не всегда гарантирует успешную консолидацию усилий компетентных органов государств Содружества в указанной сфере. Поэтому актуально говорить о важности и необходимости сближения и гармонизации национальной нормативно-правовой базы обеспечения кибербезопасности. Исследование показало, что в государствах – участниках СНГ упомянутая база достаточно активно формируется.

В числе таких правовых актов, концептуально определяющих походы обеспечения кибербезопасности: Концепция информационной безопасности Республики Беларусь[8]; Концепция информационной безопасности Республики Молдова[9]; Стратегия информационной безопасности Республики Молдова на 2019–2024 годы и План действий по ее реализации[10],Доктрина информационной безопасности Российской Федерации[11]; Концепция кибербезопасности («Киберщит Казахстана»)[12]; Стратегия кибербезопасности Кыргызской Республики на 2019–2023 годы[13], Концепция информационной безопасности Республики Таджикистан[14]; Закон Республики Узбекистан от 15 апреля 2022 года № ЗРУ-764 «О кибербезопасности»[15]; Государственная программа по обеспечению кибербезопасности Туркменистана на 2022–2025 годы[16].

Как показал анализ национального законодательства государств – участников СНГ, к сожалению, там до сих пор наблюдается отсутствие единого подхода как в терминологии, так и в определении составов противоправных деяний, совершаемых в сфере ИКТ.

Так, например, в рассмотренных внутригосударственных документах большинства стран Содружества раскрывается понятие «кибербезопасность», в то же время определение термина «киберпреступность» нормативно закреплено в законодательстве Узбекистана и Казахстана. Так, в Законе Республики Узбекистан от 15 апреля 2022 года № ЗРУ-764 «О кибербезопасности» киберпреступность определяется как совокупность преступлений, осуществляемых в киберпространстве с использованием программного обеспечения и технических средств, с целью завладения информацией, ее изменения, уничтожения или взлома информационных систем и ресурсов. В Казахстане данное понятие было закреплено в гл. 2 Стратегии кибербезопасности финансового сектора Республики Казахстан на 2018–2022 годы, где под киберпреступностью понимался вид преступности, подразумевающий преследуемые по закону деяния, совершаемые с

[1]URL: https://www.consultant.ru/document/cons_doc_LAW_5942/

[2]URL: https://www.consultant.ru/document/cons_doc_LAW_406603/

[3]URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=4699#v7riioT4lroiLlk4

[4]URL: https://online.zakon.kz/Document/?doc_id=30428639

[5]URL: http://publication.pravo.gov.ru/Document/View/0001201506040007

[6]URL: http://www.cis.minsk.by/reestrv2/doc/5224#text

[7]URL: http://publication.pravo.gov.ru/Document/View/0001202207180005

[8]Утверждена Постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 года № 1. URL: https://pravo.by/document/?guid=12551&p0=P219s0001&p1=1

[9]Утверждена Законом Республики Молдова от 21 декабря 2017 года № 299 URL: https://online.zakon.kz/Document/?doc_id=35391442

[10]Утверждена Решением Парламента Республики Молдова № 257 от 22 ноября 2018 года URL: https://www.legis.md/cautare/getResults?doc_id=111979&lang=r

[11]Утверждена Указом Президента Российской Федерации от 5 декабря 2016 года № 646 URL: https://www.consultant.ru/document/cons_doc_LAW_208191/

[12]Утверждена Постановлением Правительства Республики Казахстан от 30 июня 2017 года № 407. URL: https://base.spinform.ru/show_doc.fwx?rgn=98630

[13]Утверждена Постановлением Правительства Кыргызской Республики от 24 июля 2019 года № 369. URL: http://cbd.minjust.gov.kg/act/view/ru-ru/15478

[14]Утверждена Указом Президента Республики Таджикистан от 7 ноября 2003 года № 1175. URL:http://www.adlia.tj/show_doc.fwx?Rgn=5104

[15]URL: https://lex.uz/ru/docs/5960609

[16]Утверждена Постановлением Президента Туркменистана от 2 марта 2022 года № 2623. URL: https://turkmen.news/wp-content/uploads/2022/09

использованием информационных технологий в киберпространстве.

В то же время в Концепции информационной безопасности Республики Беларусь от 18 марта 2019 года понятие «киберпреступления» раскрывается в рамках понятия «преступления в информационной сфере». Его анализ показывает, что круг киберпреступлений ограничивается деяниями, посягающими исключительно на информационную безопасность. Иные преступления, предметом или средством совершения которых являются информация, информационные системы и сети, к числу киберпреступлений не относятся.

В соответствии со Стратегией кибербезопасности Киргизской Республики на 2019–2023 годы в числе ключевых направлений обеспечения кибербезопасности определено противодействие компьютерной преступности, как «растущей высокотехнологичной преступности, включая трансграничные компьютерные преступления, совершаемые в отношении отдельных лиц, организаций и государства как на территории Кыргызской Республики, так и из-за рубежа»[1].

Все это свидетельствует об отсутствии единого подхода в том числе и к криминализации деяний, совершаемых в киберпространстве.

В большинстве своем государства – участники СНГ, учитывая рекомендуемые положения Модельного уголовного кодекса для государств – участников СНГ (постановление Межпарламентской Ассамблеи государств – участников СНГ от 17 февраля 1996 г. № 7-5), «пошли по пути детализации уголовной ответственности за посягательства на отношения информационной безопасности и, как следствие, расширения перечня соответствующих составов» [Интеграция деятельности органов внутренних дел … 2021, с. 28].

Также в соответствии с положениями модельного уголовного закона в уголовных кодексах стран Содружества предусматривается ответственность за деяния, посягающие на другие охраняемые уголовным законом объекты (собственность, жизнь и здоровье, честь и достоинство личности, общественную безопасность и др.), где способ совершения преступления – использование компьютерной техники или информационно-телекоммуникационных сетей – выступает как признак объективной стороны либо как квалифицирующий признак. Причем круг этих преступлений подчас существенно различается.

Так, например, в УК Республики Молдова ответственность за преступления в сфере информационных технологий (то есть посягающих на информационную безопасность) предусмотрена в гл. XI «Информационные преступления и преступления в области электросвязи». Вместе с тем круг иных деяний, где использование информационно-коммуникационных сетей является способом совершения преступных посягательств на иные объекты уголовно-правовой охраны, сводится только лишь к доведению до самоубийства или содействию совершению самоубийства (ст. 150), нарушению авторского права и смежных прав (ст. 185-1), манипулированию на рынке капитала (статья 245-1).

И совершенно другой подход, более обстоятельный, мы видим в законодательстве Российской Федерации. В УК РФ кроме преступлений в сфере компьютерной информации, содержащихся в гл. 28 «Преступления в сфере компьютерной информации», в целом ряде статей (30) содержится конструктивный либо квалифицирующий признак совершения деяния «с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети "Интернет"». Это преступления: против жизни и здоровья (п. «д» ч. 2 ст. 110, п. «д» ч. 3 ст. 110^1, ч. 2 ст. 110^2), против свободы, чести и достоинства личности (ч. 2 ст. 128^1), против половой неприкосновенности и половой свободы личности (п. «б» ч. 3 ст. 133), против конституционных прав и свобод человека и гражданина (ч. 3 ст. 137), против семьи и несовершеннолетних (п. «в» ч. 2 ст. 151^2), против собственности (п. «г» ч. 3 ст. 158, ст. 159^3, ст. 159^6), в сфере экономической деятельности (ст. 171^2, ст. 185^3, ст. 187), против общественной безопасности (ч. 2 ст. 205^2, п. «в» ч. 3 и п. «в» ч. 5 ст. 222, п. «в» ч. 3 и п. «в» ч. 5 ст. 222^1, п. «в» ч. 3 и п. «в» ч. 5 ст. 222^2), против здоровья населения и общественной нравственности (п. «б» ч. 2 ст. 228^1, п. «д» ч. 2 ст. 230, ч. 1^1, 2, 3 ст. 238^1, п. «б» ч. 3 ст. 242, п. «г» ч. 2 ст. 242^1, п. «г» ч. 2 ст. 242^2, п. «г» ч. 2 ст. 245), экологические преступления (ч. 1^1, п. «б» ч. 2 ст. 258^1), преступления против основ конституционного строя и безопасности государства (ч. 2 ст. 280, ч. 2 ст. 280^1, п. «в» ч. 2 ст. 280^4, ст. 282), против мира и безопасности человечества (п. «в» ч. 2, ч. 4 ст. 354^1).

Такой же основательный подход к установлению ответственности за преступления в киберпространстве мы можем проследить, например, при анализе норм УК Казахстана [Исмагулова, Галиаскарова, 2016; Мухамеджанова, 2022].

В результате анализа уголовного законодательства стран Содружества следует сделать однозначный вывод об отсутствии единого подхода к криминализации деяний, совершаемых в информационно-телекоммуникационном пространстве.

[1]См.: п. 19 Стратегии кибербезопасности Кыргызской Республики на 2019–2023 годы (Постановление Правительства КР от 24 июля 2019 года № 369). URL: http://cbd.minjust.gov.kg/act/view/ru-ru/15479?ysclid=lktzzpw1v1843676215. В приведенной цитате сохранены авторские правописание, орфография и пунктуация

Как совершенно верно отмечают специалисты, «государства – участники СНГ, развивая национальное законодательство в сфере противодействия киберпреступности, должны стремиться максимально его гармонизировать в рамках Содружества» [Интеграция деятельности органов внутренних дел … 2021, с. 45].

Безусловно, ориентиром для законодательных органов государств – участников в процессе сближения национального законодательства и создания на территории Содружества единого правового механизма противодействия киберпреступности служат модельные законы. Помимо вышеупомянутого Модельного уголовного кодекса для государств – участников СНГ следует указать и Модельный информационный кодекс для государств – участников СНГ (постановление МПА СНГ от 23.11.2012 № 38–6), Модельный закон «Об основах регулирования Интернета» (постановление МПА СНГ от 25 ноября 2016 года № 45–12); Модельный закон «Об информации, информатизации и обеспечении информационной безопасности (постановление МПА СНГ от 28.11.2014 № 41–15); Рекомендации по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности (постановление МПА СНГ от 23 ноября 2012 года № 38-20) и др.

К сожалению, несмотря на достаточное число модельных законов, решить вопрос о создании в национальном законодательстве государств – участников СНГ единого правового механизма противодействия киберпреступности пока не удалось.

Решению этого вопроса должно способствовать принятие модельного закона «О противодействии киберпреступности» [Крайнова, 2022].

14 апреля 2023 года на пятьдесят пятом пленарном заседании Межпарламентской ассамблеи СНГ был принят модельный закон «О противодействии киберпреступности», в котором определены понятия кибербезопасности, киберпространства, киберпреступности, представлен перечень киберпреступлений, устанавливаемый вариативно в соответствии с национальным законодательством, а также международными договорами государства, закреплены другие основополагающие понятия противодействия киберпреступности.

В документе определены организационные основы противодействия киберпреступности путем закрепления полномочий президента, парламента, правительства, совета безопасности, судебных, правоохранительных и иных органов государственной власти и органов местного самоуправления.

Так же в рассматриваемом модельном законе закреплен перечень мер по профилактике киберпреступлений, положение о привлечении к уголовной ответственности граждан, иностранных граждан и лиц без гражданства за совершение киберпреступлений в соответствии с законодательством государства. Кроме того, предложен вариант привлечения к уголовной ответственности юридических лиц в соответствии с законодательством государства, что распространяется в специально предусмотренных случаях и на иностранные юридические лица.

В рамках отдельной главы закреплена правовая основа, цели, формы международного сотрудничества в области противодействия киберпреступности, определена юрисдикция государства в области противодействия киберпреступности.

Думается, что принятие данного модельного закона действительно будет способствовать созданию на территории стран Содружества единого правового механизма противодействия киберпреступности.

Кроме того, существенно повысить эффективность упомянутого механизма взаимодействия государств – участников СНГ может хорошо налаженный информационный обмен. Учитывая трансграничность киберпреступности, актуальным является создание на базе Межгосударственного информационного банка, держателем которого является МВД России, межгосударственного информационного ресурса МВД государств СНГ, содержащего криминалистический учет преступлений, совершенных с использованием ИКТ, по способам их совершения (с указанием идентификационных признаков (сведений): IP-адрес, никнейм пользователя, доменное имя сетевого ресурса, e-mail, счет электронного кошелька и т.д.). Функционирование такого учета как на национальном уровне, так и на межгосударственном уровне может существенно повлиять на оперативность в раскрытии киберпреступлений.

Еще одним важным фактором, влияющим на оперативность при раскрытии киберпреступлений, является скорость исполнения запросов об оказании содействия, срок исполнения которых в Соглашении о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий (Душанбе, 28 сентября 2018 г.) не конкретизирован. Указывается только, что запрашиваемая сторона принимает все необходимые меры для исполнения запроса в сроки, обозначенные запрашивающей стороной. На практике этот процесс часто затягивается.

Отметим, что такая же неопределенная ситуация складывается и с исполнением поручений об

оказании правовой помощи по уголовным делам по киберпреступлениям. В соответствии со ст. 62 Кишиневской конвенции поручения об оказании правовой помощи по уголовным делам исполняются в срок, предусмотренный законодательством запрашиваемого государства. Но вот, например, в уголовно-процессуальном законодательстве Российской Федерации этот срок не установлен. На практике в запросе, как правило, содержится просьба о производстве следственного или иного процессуального действия в кратчайшие сроки, что вполне может быть закреплено в рамках правового регулирования.

Вместе с тем возможность повысить оперативность взаимодействия государств в непростых условиях информационного обмена существует. Так, например, при выявлении факта совершения трансграничного киберпреступления целесообразно сразу же направлять максимальный объем информации правоохранительным органам той страны, где находится злоумышленник. Это в целом соответствует положению п. 1 ст. 6 Соглашения о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий 2018 года, в котором оговаривается возможность передачи информации компетентному органу другой стороны без запроса об оказании содействия, если есть основание полагать, что она представляет интерес для указанного компетентного органа.

ЗАКЛЮЧЕНИЕ

Таким образом, в числе актуальных направлений совершенствования противодействия киберпреступности в странах Содружества можно выделить:

- создание в национальном законодательстве государств – участников Содружества Независимых Государств единого правового механизма противодействия киберпреступности;
- совершенствование практики межгосударственного сотрудничества в рамках информационного обмена.

СПИСОК ИСТОЧНИКОВ

1. Волков Р. А. Современное состояние транснациональной преступности на территориях государств – участников Содружества Независимых Государств в условиях глобализации информационного пространства // Стратегические аспекты сотрудничества органов внутренних дел (полиции) стран Содружества в противодействии транснациональной преступности в контексте развития информационного общества под эгидой Совета министров внутренних дел государств – участников Содружества Независимых Государств: сборник тезисов выступлений на Международной научно-практической конференции. 2022. С. 12–17.
2. Интеграция деятельности органов внутренних дел (полиции) государств – участников СНГ по выявлению, предупреждению, пресечению и раскрытию киберпреступлений / Н. А. Губанова и др. М.: ФГКУ «ВНИИ МВД России», 2021.
3. Исмагулова А. Т., Галиаскарова А. М. Уголовные правонарушения в сфере информатизации и связи в Республике Казахстан. Костанай: New Line Media, 2016.
4. Мухамеджанова А. Д. Особенности динамики киберпреступности в Республике Казахстан и ее влияние на вопросы ее предупреждения // Российско-азиатский правовой журнал. 2022. № 2. С. 49–55.
5. Крайнова Н. А. О концепции модельного закона стран – участниц СНГ «О борьбе с киберпреступностью» // Право и цифровая экономика. 2022. № 2 (16). С. 48–56.

REFERENCES

1. Volkov, R. A. (2022). Sovremennoe sostoyanie transnacional'noj prestupnosti na territoriyakh gosudarstv – uchastnikov Sodruzhestva Nezavisimykh Gosudarstv v usloviyakh globalizacii informacionnogo prostranstva = The current state of transnational crime in the territories of the member States of the Commonwealth of Independent States in the context of globalization of the information space. Strategicheskie aspekty sotrudnichestva organov vnutrennikh del (policii) stran Sodruzhestva v protivodejstvii transnacional'noj prestupnosti v kontekste razvitiya informacionnogo obshchestva pod ehgidoj Soveta ministrov vnutrennikh del gosudarstv – uchastnikov Sodruzhestva Nezavisimykh Gosudarstv (pp. 12–17): sbornik tezisov vystuplenij na Mezhdunarodnoj nauchno-prakticheskoj konferencii. (In Russ.)
2. Gubanova, N. A. et al. (2021). Integraciya deyatel'nosti organov vnutrennikh del (policii) gosudarstv – uchastnikov SNG po vyyavleniyu, preduprezhdeniyu, presecheniyu i raskrytiyu kiberprestuplenij = Integration of the activities of the internal affairs bodies (police) of the CIS member states on the detection, prevention, suppression and disclosure of cybercrimes. Moscow: FGKU "VNII MVD Rossii". (In Russ.).

3. Ismagulova, A. T., Galiaskarova, A. M. (2016). Ugolovnye pravonarusheniya v sfere informatizacii i svyazi v Respublike Kazakhstan = Criminal offenses in the field of informatization and communication in the Republic of Kazakhstan. Kostanay: New Line Media. (In Russ.)
4. Mukhamedzhanova, A. D. (2022). Features of the dynamics of cybercrime in the Republic of Kazakhstan and its impact on the issues of its prevention. Russian-Asian Legal Journal, 2, 49–55. (In Russ.)
5. Krainova, N. A. (2022). On the concept of the model law of the CIS member states «On combating cybercrime». Law and Digital Economy, 2(16), 48–56. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Прокофьева Татьяна Вячеславовна

кандидат юридических наук, доцент
доцент кафедры уголовно-правовых дисциплин
Института международного права и правосудия
Московского государственного лингвистического университета

INFORMATION ABOUT THE AUTHOR

Prokofieva Tatyana Vyacheslavovna

PhD in Law, Associate Professor
Associate Professor of the Department of Criminal Law Disciplines,
Institute of International Law and Justice, Moscow State Linguistic University

Статья поступила в редакцию	10.06.2023	The article was submitted
одобрена после рецензирования	15.07.2023	approved after reviewing
принята к публикации	20.09.2023	accepted for publication