DOI 10.22394/2073-2929-2023-04-82-91

Международное сотрудничество государств СНГ по противодействию киберпреступности

Лепешкина О. И.
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (Северо-Западный институт управления), Санкт-Петербург, Российская Федерация
e-mail: lepeshkina-oi@ranepa.ru
ORCID: 0000-0002-8817-5838

РЕФЕРАТ

Киберпреступность угрожает не только национальной, но и международной информационной безопасности. В числе объектов киберугроз — экономическая безопасность, критическая информационная инфраструктура, информационный суверенитет государства. Необходимость принятия эффективных мер противодействия киберпреступности в настоящее время признается практически всем мировым сообществом. Активные меры предпринимаются во многих международных организациях, начиная с ООН и включая СНГ, ОДКБ, ШОС.

Цель. Целью статьи является определение основных направлений по эффективному противодействию киберпреступности, включающему создание нормативно-правовой основы на национальном, региональном и международном уровнях, меры по профилактике киберпреступлений, развитие международного сотрудничества.

Задачи. В задачи статьи входят содержательный анализ понятия киберпреступности, видов киберпреступлений и мер по их профилактике, а также анализ опыта государств — участников СНГ по противодействию киберпреступности и глобального правового механизма регулирования в данной области.

Методология. Противодействие киберпреступности в качестве научной основы предполагает выработку категориального аппарата, который должен соответствовать международным стандартам.

Результаты. В государствах СНГ в последние годы уделяется значительное внимание формированию правовой базы по обеспечению национальной и международной информационной безопасности, приняты Стратегии по кибербезопасности, совершенствуется уголовное законодательство в части ответственности за киберпреступления.

14 апреля 2023 г. Межпарламентская Ассамблея государств — участников СНГ приняла модельный закон «О противодействии киберпреступности», который и является основой дальнейшего совершенствования национального законодательства государств СНГ в области противодействия киберпреступности.

На создание единого международного правового механизма противодействия высокотехнологичной преступности направлен Проект Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях, внесенный Россией 30 июля 2021 г. в Генеральную Ассамблею ООН.

В результате проведенного исследования автором определены понятие и виды киберпреступлений в соответствии с международными стандартами, а также основные направления по противодействию киберпреступности на современном этапе.

Выводы. Имплементация положений модельного закона «О противодействии киберпреступности» позволит унифицировать национальное законодательство государств СНГ и будет способствовать укреплению и расширению международного сотрудничества между ними в области противодействия киберпреступности.

В России необходимо принять такой комплексный Федеральный закон «О противодействии киберпреступности» и Стратегию кибербезопасности.
Ключевые слова: противодействие киберпреступности, киберпреступность, киберпреступление, кибербезопасность, национальная, международная информационная безопасность, Содружество Независимых Государств, СНГ, ОДКБ, ШОС
Для цитирования: Лепешкина О. И. Международное сотрудничество государств СНГ по противодействию киберпреступности // Евразийская интеграция: экономика, право, политика. 2023. Т. 17. № 4. С. 82–91.
https://doi.org/10.22394/2073-2929-2023-04-82-91

International Cooperation of Member Nations of the CIS on Counteracting Cybercrime

Oksana I. Lepeshkina
Russian Presidential Academy of National Economy and Public Administration (North-Western Institute of Management of RANEPA), Saint Petersburg, Russian Federation
e-mail: lepeshkina-oi@ranepa.ru
ORCID: 0000-0002-8817-5838

ABSTRACT
Cybercrime is the threat to national and international informational security. The objects of cyberthreats are economics security, critical information structure, information state sovereignty. All states admit necessity to take effective measures for anti-cybercrime in this time. Such organizations, as Commonwealth of Independent States, Collective Security Treaty Organization, Shanghai Cooperation Organization are to take active measures on counteracting cybercrime.
Aim. The aim of this article is to define principal directions on effective counteracting cybercrime, including creation of law base on national, regional and international levels, measures for prevention cybercrime and development of international collaboration.
Tasks. There are following tasks in this article: to define “cybercrime”, categories of cybercrime and measures for prevention cybercrime, to analyze experience of member nations of the CIS and world law mechanism for cybercrime control.
Methods. There is necessity to define terminology in accordance with the international standards for cybercrime control.
Results. Member nations of the CIS are giving important attention to creation the law base for national and international security, and also Criminal Law about responsibility for cybercrime.
The Model Law “On counteracting cybercrime” was adopted by Interparliamentary Assembly of the CIS on 14 Aprile 2023, which is the base of development of national legislation in sphere of cybercrime control.
On 30 July 2021 Russia was carry in General Assembly of the United Nations the Project of Convention United Nations Countering the use of information and communications technologies for criminal purposes for creation of international law mechanism for anti-cybercrime.
In the result of this research author is defined cybercrime and it’s variety in accordance with international standards, and also principal directions of counteracting cybercrime in contemporary period.
Conclusion. Implementation by member nations of the CIS of Model Law “On counteracting cybercrime” will allow unify national legislation and assist strengthening and extension international cooperation between these states on combating cybercrime.
There is necessity to adopt such complex Federal Law “On counteracting cybercrime” and the Strategy on cybersecurity in Russia.
Keywords: counteracting cybercrime, cybercrime, cybersecurity, national, international informational security, Commonwealth of Independent States, CIS, CSTO, SCO

For citing: Lepeshkina O. I. International Cooperation of Member Nations of the CIS on Counteracting Cybercrime // Eurasian Integration: Economics, Law, Politics. 2023. V. 17. No. 4. P. 82–91. (In Rus.) https://doi.org/10.22394/2073-2929-2023-04-82-91

Введение

Необходимость поиска и принятия эффективных мер по противодействию киберпреступности в настоящее время признается практически всем мировым сообществом, государствами как с высоким, так и с низким уровнем кибербезопасности.

Киберпреступность угрожает не только национальной, но и международной информационной безопасности. В числе объектов киберугроз — экономическая безопасность, критическая информационная инфраструктура, информационный суверенитет государства.

Для эффективного противодействия киберпреступности требуется принятие комплекса мер — политического, правового, организационного характера, а также технологических, технических, криптографических и других. При этом приоритетным направлением является профилактика киберпреступлений.

Конкретные совместные меры в области противодействия киберпреступности, особенно в последние годы, предпринимаются в Содружестве Независимых Государств, Организации Договора о коллективной безопасности, Шанхайской организации сотрудничества.

Киберпреступность и киберпреступления

Ключевые термины в области обеспечения кибербезопасности, определяющие национальное законодательство и международно-правовые акты, содержатся в двух межгосударственных стандартах — Международной организации стандартизации (ИСО) и Международного союза электросвязи ООН.

В Международном стандарте «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности» (ISO/IEC 27032:2012 Information Technology — Security Techniques — Guidelines for Cybersecurity) определены такие термины, как «кибербезопасность», «киберпространство», а также сам термин «киберпреступление»[1].

«Кибербезопасность — сохранение конфиденциальности, целостности и доступности информации в киберпространстве.

Киберпространство — сложная среда, возникающая в результате взаимодействия людей, программного обеспечения и сервисов в сети «Интернет» посредством связанных с ней технологических устройств и сетей, не существующая в физической форме.

Киберпреступление — преступная деятельность, при которой сервисы или приложения киберпространства являются орудием или целью преступления или при которой само киберпространство является источником, инструментом, целью или местом преступления» [4, с. 67].

Термин «киберпреступность» был введен в юридический оборот Конвенцией о киберпреступности (Convention on Cybercrime) от 23 ноября 2001 г. Совета Европы. Конвенция открыта для подписания и государствами, не являющимися членами этой региональной организации, и из 68 государств, ратифицировавших Конвенцию, таковых 23, например, Канада, Израиль, США и Япония.

Отметим, что развитием установленного в рамках Совета Европы механизма противодействия киберпреступности является открытие 12 мая 2022 г. для подписания Второго Дополнительного протокола к Конвенции о киберпреступности о расширении сотрудничества и раскрытии электронных доказательств (ETS № 224)[2].

---

[1] ISO/IEC 27032:2012 Information Technology — Security Techniques — Guidelines for Cybersecurity [Электронный ресурс] // ISO (Международная организация по стандартизации). URL: https://www.iso.org/standard/44375.html (дата обращения: 30.03.2022).

[2] Второй Дополнительный протокол к Конвенции о киберпреступности о расширении сотрудничества и раскрытии электронных доказательств [Электронный ресурс] // Council of Europe. URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224 (дата обращения: 30.05.2023).

Из государств СНГ участниками Конвенции о киберпреступности являются Республика Армения, Республика Молдова и Азербайджанская Республика.

Россия, намереваясь в 2005 г. стать участницей указанной Конвенции, в итоге ее не ратифицировала, посчитав, что «положения пункта «b» статьи 32 Конвенции … могут нанести ущерб суверенитету и национальной безопасности государств-участников, правам и законным интересам их граждан и юридических лиц»[1]. В пункте «b» ст. 32 Конвенции содержится положение о возможности трансграничного доступа к компьютерным данным, хранящимся на территории другого государства, без его согласия.

В международных правовых актах, регулирующих вопросы ответственности за преступления международного характера, как правило, преступление определяется путем указания перечня преступлений данного вида.

В Конвенции о киберпреступности выделены два вида киберпреступлений: 1) компьютерные преступления против данных и систем (offences against the confidentiality, integrity and availability of computer data and systems); 2) преступления, связанные с компьютером (computer-related offences).

В целом с позиции криминологии киберпреступность можно определить как совокупность киберпреступлений, совершенных на определенной территории за определенный период времени.

Киберпреступление — это преступление, совершенное в киберпространстве. Это, на наш взгляд, самое общее и наименее дискуссионное определение, которое и было включено нами в проект модельного закона для государств СНГ «О противодействии киберпреступности» при его разработке (ст. 2)[2].

Криминологами используются и другие понятия: «компьютерная преступность», «высокотехнологичная преступность», а с учетом развития высоких технологий, в том числе, как указывает К. Н. Евдокимов, «когнитивных, космических, робототехнических», им предложено понятие «технотронная преступность» [2, с. 49].

При определении видов киберпреступлений следует согласиться с С. Ю. Трофимцевой, что критерием классификации «является соотнесение компьютера как программно-аппаратного устройства с объективной стороной совершенного преступления» [5, с. 77].

Исходя из международных правовых актов, к киберпреступлениям относятся преступления двух видов: 1) компьютерные преступления против систем и данных (computer crimes); 2) преступления, связанные с компьютером (computer-related crimes)[3].

Именно эти виды киберпреступлений предусмотрены в российском уголовном законодательстве.

Иной позиции придерживается В. Ф. Джафарли, по мнению которого к киберпреступлениям относятся только «киберпреступления, основные действия и последствия которых происходят исключительно в киберпространстве», а «преступления, действия в которых в той или иной мере связаны с использованием ИКТ-средств», к таковым не относятся [1, с. 61–62].

Противодействие киберпреступности

Термин «противодействие» преступности уже устоялся в российском законодательстве, и в отличие от термина «борьба» с преступностью включает не только задачу уголовного преследования, т. е. деятельность по выявлению, предупреждению, пресечению, раскрытию и расследованию преступлений, но и их профилактику. При этом меры по профилактике преступлений имеют приоритет.

В соответствии со ст. 2 модельного закона для государств — участников СНГ «О противодействии киберпреступности» «противодействие киберпреступности — деятельность органов государственной власти, органов местного самоуправления, институтов гражданского общества, организаций и физических лиц в пределах их полномочий по:

---

[1] О подписании Конвенции о киберпреступности: распоряжение Президента Российской Федерации от 15 ноября 2005 г. № 557-рп // Собрание законодательства Российской Федерации. 2005. № 47. Ст. 4929.

[2] Разработчики данного модельного закона: О. И. Лепешкина, Т. Н. Дронова, А. В. Коротков.

[3] Термин “computer-related crime” был введен Рекомендацией Комитета министров Совета Европы № R (89)9 от 13 сентября 1989 г. Recommendation No. R (89) 9 of the Committee of Ministers to member states on computer-related crime [Электронный ресурс]. URL: https://rm.coe.int/09000016804f1094 (дата обращения: 09.07.2023).

1) предупреждению киберпреступности (профилактика);

2) выявлению, предупреждению, пресечению, раскрытию и расследованию киберпреступлений;

3) минимизации и (или) ликвидации последствий киберпреступлений»[1].

По нашему мнению, противодействие киберпреступности должно осуществляться по следующим направлениям: 1) создание и совершенствование нормативно-правовой основы в области противодействия киберпреступности на национальном, региональном и международном уровнях; 2) повышение эффективности профилактики киберпреступлений; 3) развитие международного сотрудничества в области противодействия киберпреступности.

Вполне прогнозируемый дальнейший рост киберпреступности, как следствие цифровизации общественных отношений, масштабность экономического ущерба и другие, связанные с ее распространением угрозы, включая так называемые «гибридные» войны [3], требуют выработки соответствующего механизма противодействия, но нормативно-правовая база для этого еще создается, в том числе на глобальном уровне.

В Российской Федерации резкий рост преступлений, при совершении которых используются информационно-телекоммуникационные технологии, а также в сфере компьютерной информации, объединяемых в официальной статистической отчетности в одну группу, произошел в 2019 г. (+68,5%)[2], и эта тенденция сохраняется.

По данным Банка России, на основе выявленных операций без согласия клиентов в 2022 г. у граждан и организаций было похищено 14 165,44 млн руб. (в 2021 г. — 13 582,23 млн руб., в 2020 г. — 9 777,3 млн руб.)[3].

В России принят ряд правовых стратегических, концептуальных актов, в которых киберпреступность рассматривается как одна из угроз национальной и международной информационной безопасности и противодействие ей признается приоритетным в государственной политике: Стратегия национальной безопасности Российской Федерации (п. 42)[4], Доктрина информационной безопасности Российской Федерации (п. 2)[5], Основы государственной политики Российской Федерации в области международной информационной безопасности (пп. «г» п. 8)[6].

В некоторых государствах СНГ приняты стратегии именно по кибербезопасности, определяющие терминологию и основные направления государственной политики в этой более узкой сфере информационной безопасности: Концепция кибербезопасности («Киберщит Казахстана») от 30 июня 2017 г.[7], Стратегия кибербезопасности Кыргызской Республики на 2019–2023 годы от 24 июля 2019 г.[8]

Законодательство государств СНГ в рассматриваемой сфере активно развивается буквально в последние годы.

В Законе Республики Узбекистан от 15 апреля 2022 г. № ЗРУ-764 «О кибербезопасности» содержится понятие киберпреступности: «Киберпреступность — совокупность преступлений, осуществляемых в киберпространстве с использованием программного обеспечения и технических средств,

---

[1] Модельный закон для государств — участников СНГ «О противодействии киберпреступности». Принят постановлением МПА СНГ от 14.04.2023 № 55-20 [Электронный ресурс] // Межпарламентская Ассамблея государств — участников Содружества Независимых Государств. URL: https://iacis.ru/baza_dokumentov/modelnie_zakonodatelnie_akti_i_rekomendatcii_mpa_sng/modelnie_kodeksi_i_zakoni (дата обращения: 27.06.2023).

[2] Официальный сайт Министерства внутренних дел Российской Федерации [Электронный ресурс]. URL: https://мвд.рф/ (дата обращения: 24.04.2023).

[3] Обзор операций, совершенных без согласия клиентов финансовых организаций [Электронный ресурс] // Банк России. URL: https://www.cbr.ru/analytics/ib/operations_survey_2022/ (дата обращения: 20.04.2023).

[4] О Стратегии национальной безопасности Российской Федерации : указ Президента Российской Федерации от 2 июля 2021 г. № 400 // Собрание законодательства Российской Федерации. 2021. N 27 (Часть II). Ст. 5351.

[5] Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента Российской Федерации от 5 декабря 2016 г. № 646 // Собрание законодательства Российской Федерации. 2016. N 50. Ст. 7074.

[6] Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности : указ Президента Российской Федерации от 12 апреля 2021 г. № 213 // Собрание законодательства Российской Федерации. 2021. N 16 (Часть I). Ст. 2746.

[7] Об утверждении Концепции кибербезопасности («Киберщит Казахстана») : постановление Правительства Республики Казахстан от 30 июня 2017 г. № 407 [Электронный ресурс] // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». URL: https://adilet.zan.kz/rus/docs/P1700000407 (дата обращения: 30.05.2023).

[8] Об утверждении Стратегии кибербезопасности Кыргызской Республики на 2019–2023 годы : постановление Правительства Республики Кыргызстан от 24 июля 2019 г. № 369 [Электронный ресурс] // Министерство Юстиции Кыргызской Республики. URL: http://cbd.minjust.gov.kg/act/view/ru-ru/15479?cl=ru-ru (дата обращения: 30.05.2023).

с целью завладения информацией, ее изменения, уничтожения или взлома информационных систем и ресурсов»[1].

Заслуживает внимания опыт государств СНГ в части уголовной ответственности за киберпреступления. В Уголовном кодексе Республики Казахстан от 3 июля 2014 г. предусмотрена ответственность за «неправомерные изменения идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства» (ст. 213)[2].

На региональном уровне в рамках Содружества Независимых Государств задачам обеспечения кибербезопасности и противодействия информационной преступности уделено внимание в ряде основополагающих актов сотрудничества и, прежде всего, в Стратегии обеспечения информационной безопасности государств — участников Содружества Независимых Государств[3].

Согласно Концепции дальнейшего развития Содружества Независимых Государств, одним из приоритетных направлений является сотрудничество государств СНГ «в области обеспечения международной информационной безопасности и противодействия преступлениям в сфере информационно-коммуникационных технологий» (п. 4.6)[4].

В Соглашении о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 г.[5] непосредственно определяются формы сотрудничества, регулируются вопросы выдачи, оказания взаимной правовой помощи.

В Межгосударственной программе совместных мер борьбы с преступностью на 2019–2023 годы указаны организационно-правовые, организационно-практические мероприятия, информационное и научное обеспечение в сфере противодействия преступлениям, совершаемым с использованием информационных технологий[6].

Следует указать на развитие модельного законодательства, которое после имплементации его в национальные правовые системы государств СНГ позволит его унифицировать в части определения перечня киберпреступлений, осуществления мер по профилактике, международного сотрудничества.

14 апреля 2023 г. на 55-м пленарном заседании Межпарламентской Ассамблеи государств СНГ был принят модельный закон «О противодействии киберпреступности»[7].

Россия сотрудничает с государствами СНГ и в других региональных организациях.

В рамках Организации Договора о коллективной безопасности 30 ноября 2017 г. заключено Соглашение о сотрудничестве государств — членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности[8].

---

[1] О кибербезопасности : закон Республики Узбекистан от 15 апреля 2022 г. № ЗРУ-764 [Электронный ресурс] // LexUZ on-line. URL https://lex.uz/ru/docs/5960609 (дата обращения 30.05.2023).

[2] Уголовный кодекс Республики Казахстан от 3 июля 2014 г. № 226-V ЗРК [Электронный ресурс] // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». URL: https://adilet.zan.kz/rus/docs/K1400000226 (дата обращения: 30.05.2023).

[3] Стратегия обеспечения информационной безопасности государств — участников Содружества Независимых Государств : решение Совета глав правительств СНГ от 25 октября 2019 г. [Электронный ресурс] // Официальный сайт Содружества Независимых Государств. URL: https://www.cis.minsk.by/reestrv2/doc/6162#text (дата обращения: 24.04.2023).

[4] О Концепции дальнейшего развития Содружества Независимых Государств и Плане основных мероприятий по ее реализации : решение Совета глав государств СНГ от 18 декабря 2020 г. [Электронный ресурс] // Официальный сайт Содружества Независимых Государств. URL: https://cis.minsk.by/reestrv2/doc/6363#text (дата обращения: 24.04.2023).

[5] Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 г. [Электронный ресурс] // Официальный сайт Содружества Независимых Государств. URL: https://www.cis.minsk.by/reestrv2/doc/5864#text (дата обращения: 24.04.2023).

[6] Межгосударственная программа совместных мер борьбы с преступностью на 2019–2023 годы : решение Совета глав государств СНГ от 28 сентября 2018 г. [Электронный ресурс] // Официальный сайт Содружества Независимых Государств. URL: https://www.cis.minsk.by/reestrv2/doc/5863#text (дата обращения: 24.04.2023).

[7] Модельный закон для государств — участников СНГ «О противодействии киберпреступности». Принят постановлением МПА СНГ от 14.04.2023 № 55–20 [Электронный ресурс] // Межпарламентская Ассамблея государств — участников Содружества Независимых Государств. URL: https://iacis.ru/baza_dokumentov/modelnie_zakonodatelnie_akti_i_rekomendatcii_mpa_sng/modelnie_kodeksi_i_zakoni (дата обращения: 27.06.2023).

[8] Соглашение о сотрудничестве государств-членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности от 30 ноября 2017 г. [Электронный ресурс] // Консорциум КОДЕКС. URL: https://docs.cntd.ru/document/542645728 (дата обращения: 30.05.2023).

Кроме того, по инициативе Республики Беларусь для взаимодействия государств по защите критической информационной инфраструктуры в ОДКБ разрабатывается проект модельного закона «О защите информации и кибербезопасности»[1].

Россией также заключено Соглашение между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г.[2]

Основная проблема, затрудняющая, на наш взгляд, взаимодействие государств по противодействию киберпреступности, состоит в отсутствии соответствующего единого международного правового механизма, универсального международного акта.

С целью создания такого правового механизма Российская Федерация 30 июля 2021 г. внесла в Генеральную Ассамблею ООН проект Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях (Резолюция ГА ООН 75/980, принята на 75-й сессии 10 августа 2021 г.)[3].

В проекте этой Конвенции предусматривается криминализация 22 видов киберпреступлений против данных, систем и сетей и тех, при совершении которых могут быть использованы электронные технологии.

Перечень киберпреступлений второго вида в российском проекте значительно расширен, по сравнению с Конвенцией о киберпреступности 2001 г., и отражает современные угрозы. К таковым отнесены «преступления, связанные с террористической и экстремистской деятельностью, с незаконным оборотом наркотических средств и психотропных веществ, оружия, реабилитация нацизма, оправдание геноцида или преступлений против мира и человечности, подстрекательство к подрывной или вооруженной деятельности и др. (ст. 6–27)» [4, с. 68].

Профилактика киберпреступлений

Приоритетным направлением в противодействии киберпреступности, как это общепризнанно в криминологии, является профилактика киберпреступлений, которая направлена на выявление и устранение детерминирующих ее причин и условий.

В числе основных мер по профилактике киберпреступлений можно указать следующие: 1) мониторинг компьютерных атак на информационную инфраструктуру государства, в том числе критическую информационную инфраструктуру; 2) выявление и пресечение распространения в информационно-телекоммуникационных сетях, включая сеть «Интернет», информации и (или) материалов, содержащих признаки киберпреступлений (удаление таких материалов и информации); 3) контроль за доступом к персональным данным и их обработкой в информационных системах персональных данных; 4) контроль за осуществлением финансовых операций в целях противодействия легализации (отмыванию) доходов, полученных в результате совершения киберпреступлений, финансированию терроризма и финансированию распространения оружия массового уничтожения; 5) контроль за деятельностью бирж цифровых валют (криптовалют); 6) информационно-пропагандистская и консультационная деятельность; 7) привлечение общественных объединений, в том числе кибердружин, организаций и граждан к деятельности по предупреждению киберпреступлений.

Легализация активов, полученных в результате киберпреступлений, и способствующая их совершению, осуществляется в том числе путем конвертации цифровой валюты в фиатные деньги на биржах цифровых валют, в связи с чем и нужен контроль за их деятельностью.

---

[1] Официальный сайт Парламентской Ассамблеи Организации Договора о коллективной безопасности [Электронный ресурс]. URL: https://paodkb.org/ (дата обращения: 20.02.2023).

[2] Об утверждении Соглашения между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности : распоряжение Правительства Российской Федерации от 16 июля 2009 г. № 984-р // Собрание законодательства Российской Федерации. 2009. N 30. Ст. 3879.

[3] Письмо Временного поверенного в делах Постоянного представительства Российской Федерации при Организации Объединенных Наций от 30 июля 2021 г. на имя Генерального секретаря [Электронный ресурс] // Организация Объединенных Наций. URL: https://undocs.org/ru/A/75/980 (дата обращения: 05.03.2022).

Установление контроля за биржами цифровых валют рекомендовано Группой разработки финансовых мер борьбы с отмыванием денег (ФАТФ) (Рекомендация 15 «Новые технологии»), а в качестве мер обязательное лицензирование, предоставление отчетности, индивидуализация клиентов.

В числе государств СНГ оборот цифровой валюты легализован в Республике Беларусь Декретом Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики»[1]. По Указу Президента Республики Беларусь от 14 февраля 2022 г. № 48 «О реестре адресов (идентификаторов) виртуальных кошельков и особенностях оборота криптовалюты»[2] установлен порядок ведения реестра адресов виртуальных кошельков, использованных (используемых) для осуществления противоправной деятельности.

В Российской Федерации, согласно Федеральному закону от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[3], оборот цифровой валюты ограничен инвестиционной деятельностью и возможностью ее купли-продажи. Вместе с тем утвержденная 8 февраля 2022 г. Правительством РФ «Концепция законодательного регламентирования механизмов организации оборота цифровых валют»[4] предусматривает легализацию цифровой валюты, в том числе создание бирж цифровых валют.

Международное сотрудничество

Киберпреступность имеет транснациональный характер, и без международного сотрудничества эффективное противодействие ей невозможно. При совершении киберпреступления виновный и потерпевший могут находиться в разных юрисдикциях, в связи с чем возникает ряд вопросов: об определении места совершения преступления, о получении электронных доказательств, выдаче лиц, совершивших киберпреступления, для их уголовного преследования или исполнения приговора, поскольку экстрадиция возможна, только если преступление наказуемо в обоих государствах.

Международное сотрудничество также необходимо для оказания взаимной правовой помощи, признания актов судебных органов, выявления и наложения ареста на активы, полученные в результате совершения киберпреступлений, а также для противодействия легализации таких доходов, и решения других вопросов.

Полагаем, что целями международного сотрудничества в области противодействия киберпреступности, наряду с уголовным преследованием и осуждением лиц, виновных в совершении киберпреступлений, являются: 1) обеспечение информационного суверенитета государства; 2) координация деятельности государств; 3) повышение эффективности противодействия киберпреступности, в том числе преступлениям террористической и экстремистской направленности и их финансированию; 4) предупреждение, выявление и пресечение международных переводов активов, используемых или предназначенных для совершения киберпреступлений, а также полученных в результате совершения киберпреступлений; 5) возврат перемещенных за границу активов, используемых или предназначенных для совершения киберпреступлений, а также полученных в результате совершения киберпреступлений; 6) осуществление деятельности по профилактике киберпреступлений.

В качестве основных форм международного сотрудничества в рассматриваемой сфере можно указать на следующие: 1) обмен информацией; 2) оказание взаимной правовой помощи и правоохранительного содействия; 3) розыск, задержание и выдача лиц, совершивших киберпреступления; 4) передача лица, осужденного к лишению свободы за совершение киберпреступления, для отбывания наказания

---

[1] О развитии цифровой экономики : декрет Президента Республики Беларусь от 21 декабря 2017 г. № 8 [Электронный ресурс] // Президент Республики Беларусь. URL: https://president.gov.by/ru/documents/dekret-8-ot-21-dekabrja-2017-g-17716 (дата обращения: 24.04.2023).

[2] О реестре адресов (идентификаторов) виртуальных кошельков и особенностях оборота криптовалюты : указ Президента Республики Беларусь от 14 февраля 2022 г. № 48 [Электронный ресурс] // Президент Республики Беларусь. URL: https://president.gov.by/ru/documents/ukaz-no-48-ot-14-fevralya-2022-g (дата обращения: 24.04.2023).

[3] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации : федеральный закон от 31 июля 2020 г. № 259-ФЗ // Собрание законодательства Российской Федерации. 2020. N 31. Ст. 5018.

[4] Концепция законодательного регламентирования механизмов организации оборота цифровых валют [Электронный ресурс]. URL: http://static.government.ru/media/files/Dik7wBqAubc34ed649ql2Kg6HuTANrqZ.pdf (дата обращения: 30.06.2023).

в государстве, гражданином которого оно является; 5) признание актов судебных и иных компетентных органов иностранных государств; 6) проведение совместных и (или) скоординированных мероприятий по противодействию киберпреступности; 7) оказание содействия в розыске, наложении ареста, конфискации и возврате перемещенных за границу активов, используемых или предназначенных для совершения киберпреступлений, а также полученных в результате совершения киберпреступлений; 8) создание специализированных банков данных и иных информационных банков; 9) оказание методической и технической помощи; 10) содействие в подготовке, профессиональной переподготовке и повышении квалификации кадров; 11) проведение совместных научных и научно-технических исследований и мероприятий; 12) обмен передовым опытом в области противодействия киберпреступности.

Заключение

В новой Концепции внешней политики Российской Федерации «в целях содействия адаптации мироустройства к реалиям многополярного мира» Россия указала о своем намерении уделять приоритетное внимание «укреплению потенциала и повышению международной роли межгосударственного объединения БРИКС, Шанхайской организации сотрудничества (ШОС), Содружества Независимых Государств (СНГ), Евразийского экономического союза (ЕАЭС), Организации Договора о коллективной безопасности (ОДКБ), РИК (Россия, Индия, Китай) …» (пп. 4 п. 19)[1].

По Глобальному индексу кибербезопасности, который публикует Международный союз электросвязи, в 2020 г. (последний обзор) государства СНГ занимали следующие места: Россия — 5-е место, Казахстан — 31-е, Азербайджан — 40-е, Молдова — 63-е, Узбекистан — 70-е, Беларусь — 89-е, Армения — 90-е, Кыргызстан — 92-е, Таджикистан — 138-е, Туркменистан — 144-е[2].

Тем не менее в рамках СНГ создана достаточная нормативно-правовая основа сотрудничества в области противодействия киберпреступности.

Имплементация модельного закона для государств — участников СНГ «О противодействии киберпреступности», принятого 14 апреля 2023 г. на 55-м пленарном заседании Межпарламентской Ассамблеи государств СНГ, позволит унифицировать национальное законодательство в данной области.

На создание единого международного правового механизма противодействия киберпреступности направлен российский проект Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях.

В России настоятельно требуется принятие Федерального закона «О противодействии киберпреступности» и Стратегии по кибербезопасности, что рекомендовано Международным союзом электросвязи ООН.

Литература

1. *Джафарли В. Ф.* Криминология кибербезопасности: в 5 т. Т. 2: Уголовно-правовое обеспечение криминологической кибербезопасности / под ред. С. Я. Лебедева. М. : Проспект, 2021.
2. *Евдокимов К. Н.* К вопросу совершенствования специальных мер противодействия технотронной преступности в Российской Федерации // Криминалистика: вчера, сегодня, завтра. 2022. № 2. С. 45–55. DOI: 10.55001/2587-9820.2022.93.56.006
3. *Иващенко М. А.* К вопросу о понятии и признаках гибридной войны // Российский следователь. 2021. № 12. С. 39–41. EDN: AANCJA. DOI: 10.18572/1812-3783-2021-12-39-41
4. *Лепешкина О. И.* Киберпреступность как угроза национальной безопасности России // Теоретическая и прикладная юриспруденция. 2022. № 2. С. 65–69. Доступ: URL: https://www.taljournal.ru/jour/article/view/181 (дата обращения: 24.11.2022). DOI: 10.22394/2686-7834-2022-2-65-69

[1] Об утверждении Концепции внешней политики Российской Федерации : указ Президента Российской Федерации от 31 марта 2023 г. № 229 // Собрание законодательства Российской Федерации. 2023. N 14. Ст. 2406.

[2] Global Cybersecurity Index 2020. P. 25–27 [Электронный ресурс]. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (дата обращения: 30.06.2023).

5. *Трофимцева С. Ю.* Проблема выделения дефиниций базовых терминов при анализе киберпреступности // Евразийский юридический журнал. 2017. № 7. С. 75–77. EDN: ZDOVBP

Об авторе:

Лепешкина Оксана Ивановна, доцент кафедры уголовного права Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (Северо-Западный институт управления) (Санкт-Петербург, Российская Федерация), кандидат юридических наук, доцент;
e-mail: lepeshkina-oi@ranepa.ru; ORCID: 0000-0002-8817-5838

References

1. Dzhafarli V. F. Criminology of Cybersecurity: in 5 vol. Vol. 2: Criminal Law Preservation of Criminology Cybersecurity. Editor-in Chief S. Ya. Lebedev. Moscow : Prospekt, 2021. 280 p. (In Rus.)
2. Evdokimov K. N. On the Issue of Improving Special Measures to Counteract Technotronic Crime in the Russian Federation // Forensics: Yesterday, Today, Tomorrow [Kriminalistika: vchera, segodnya, zavtra], 2022. No. 2. P. 45-55. (In Rus.) DOI: 10.55001/2587-9820.2022.93.56.006
3. Ivaschenko M. A. On the Concept and Attributes of a Hybrid War // Russian Examiner [Rossiiskii Sledovatel']. 2021. No. 12. P. 39–41. (In Rus.) EDN: AANCJA. DOI: 10.18572/1812-3783-2021-12-39-41
4. Lepeshkina O. I. Cybercrime as Threat of National Security of Russia // Theoretical and Applied Law [Teoreticheskaya i prikladnaya yurisprudentsiya]. 2022. No. 2. P. 65–69. (In Rus.) DOI: 10.22394/2686-7834-2022-2-65-69
5. Trofimtseva S. Yu. The Problem of Basic Terms Definitions Emphasizing during the Analysis of Cybercrime // Eurasia Law Jornal [Evraziiskii yuridicheskii zhurnal]. 2017. No. 7 (110). (In Rus.) EDN: ZDOVBP

About the author:

Oksana I. Lepeshkina, Associate Professor of the Department of Criminal Law Faculty of Law of North-West Management Institute of the RANEPA (Saint Petersburg, Russian Federation), PhD in Jurisprudence, Associate Professor;
e-mail: lepeshkina-oi@ranepa.ru; ORCID: 0000-0002-8817-5838