Журнал международного права и международных отношений. 2022. № 1-2 (100-101). С. 41—47.
Journal of International Law and International Relations. 2022. N 1-2 (100-101). P. 41—47.
УДК 341(476) DOI: 10.33581/2072-0513-2022-1-2-41-47

АКТУАЛЬНЫЕ АСПЕКТЫ УЧАСТИЯ РЕСПУБЛИКИ БЕЛАРУСЬ В ИНСТИТУЦИОНАЛЬНОМ МЕХАНИЗМЕ ПРОТИВОДЕЙСТВИЯ МЕЖДУНАРОДНОЙ КИБЕРПРЕСТУПНОСТИ

Марина Головенчик

Глобальный прорыв в развитии компьютеризации и цифровизации, произошедший в начале XXI в., открывает перед современным обществом широкие перспективы. Благодаря компьютеризации и цифровизации в последние годы значительно повысились мобильность и коммуникативность людей, активизировались политические процессы, стала более доступной самая разнообразная информация. Вместе с тем это же явление стало причиной возникновения и стремительного развития нового направления противоправной деятельности, получившего общее наименование «киберпреступность». В статье исследуются вопросы регионального сотрудничества правоохранительных органов Республики Беларусь в сфере противодействия киберпреступности в рамках таких региональных международных организаций, как Организация Договора о коллективной безопасности, Содружество Независимых Государств. В результате проведенного анализа сделан вывод о существовании различных механизмов взаимодействия между правоохранительными органами государств, входящих в названные организации. Вместе с тем для повышения эффективности дальнейшего сотрудничества в противодействии возникающим киберугрозам требуются совершенствование и унификация положений международных нормативных правовых актов, а также создание в рамках Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств — участников Содружества Независимых Государств специализированного подразделения, деятельность которого будет направлена на координацию взаимодействия правоохранительных органов в вопросах противодействия современным проявлениям киберпреступности, их предупреждения и профилактики.

Ключевые слова: институциональный механизм; кибербезопасность; киберпреступность; координация деятельности; международное сотрудничество; правоохранительные органы.

«Issues for the Participation of the Republic of Belarus in the Institutional Mechanism for Combating International Cybercrime» (Marina Goloventchik)

The exponential growth of computer and digital technology in the 21st century creates broad opportunities for human societies, such as increased mobility, ease of communication, political participation and access to information. Yet it has also given rise to a new type of criminal activity, broadly defined as cybercrime. The author considers the regional cooperation of law enforcement agencies in combating cybercrime via multilateral organisations such as the Collective Security Treaty Organization and the Commonwealth of Independent States. Several mechanisms of cooperation with the member states of these organisations are identified. The author presents an argument for modernisation and harmonisation of the international legal frameworks for fighting organized crime and other forms of criminal activity affecting the member states. A case is also made for the establishment of the specialised unit in the structure of Coordination Bureau for Organised Crime Control in the Commonwealth of Independent States countries.

Keywords: coordination of activities; cybercrime; cybersecurity; institutional mechanism; international cooperation; law enforcement agencies.

В настоящее время одной из глобальных проблем человечества является международная преступность, в рамках которой следует особо выделить преступления в сфере высоких технологий, или киберпреступления. Появление такой преступности обусловлено стремительным развитием цифровой глобализации экономики (от *globe* — земной шар), в ходе которой, как отмечает Г. Г. Головенчик, происходит сращивание национальных рын-

Автор:
Головенчик Марина Геннадьевна — аспирант кафедры уголовного права юридического факультета Белорусского государственного университета, *e-mail: marina.golovenchik@inbox.ru*
Белорусский государственный университет. Адрес: 4, пр. Независимости, Минск, 220030, БЕЛАРУСЬ

Author:
Goloventchik Marina — post-graduate student of the Department of Criminal Law of the Faculty of Law, Belarusian State University, *e-mail: marina.golovenchik@inbox.ru*
Belarusian State University. Address: 4, Nezavisimosti ave., Minsk, 220030, BELARUS

ков товаров, услуг и капиталов, а перемещение человеческого и информационного ресурсов не сдерживается национальными границами [4, с. 77].

Как показывает статистика, количество данных преступлений неуклонно растет. Так, в мае 2022 г. заместитель начальника Главного управления центрального аппарата Следственного комитета Беларуси И. Судникович отметил, что «число киберпреступлений за последние 5 лет выросло в 10 раз. В среднем в год фиксируется 25 тыс. таких фактов, то есть каждое четвертое преступление…» [см.: 2].

Безусловно, будучи серьезным асоциальным явлением, обладающим признаком экстерриториальности, киберпреступность не могла не стать предметом пристального внимания со стороны как отдельных государств, так и межгосударственных образований, поскольку только совместные усилия правоохранительных органов большинства мировых держав позволят противостоять международной преступности как современной глобальной проблеме человечества.

Вопросы противодействия киберпреступности достаточно часто становятся предметом научных исследований. Так, аспекты международно-правовой помощи по уголовным делам о киберпреступлениях и иные аспекты международно-правовых основ сотрудничества государств в рамках обозначенной проблематики освещены в работах таких белорусских и российских ученых-правоведов, как Е. В. Батуева [3], А. А. Данилевич, В. И. Самарин [5], В. П. Зимин [7], Е. Г. Моисеев [9], Н. О. Мороз [10; 11], А. И. Мысина [12], В. Ч. Родевич, С. С. Тупеко [21], В. П. Талимончик [27] и др.

Рассматривая вопросы взаимодействия государств в области борьбы с транснациональной преступностью в целом, следует отметить, что такое сотрудничество проявляется в двух основных формах: договорно-правовой (конвенционной) и организационно-правовой (институциональной). Причем именно последнюю, согласно опубликованным Исполнительным комитетом Содружества Независимых Государств (далее — СНГ) материалам аналитического отдела информационно-аналитического департамента, следует считать наиболее эффективной, поскольку она базируется на достижении консенсуса относительно принципиальных положений, затрагивающих национальные интересы участников различных международных организаций [16]. А. А. Данилевич, напротив, утверждает, что «наиболее эффективные результаты приносит взаимодействие, основанное на международных договорах и разработанном национальном законодательстве…» [5, с. 6], отмечая, таким образом, наибольшую эффективность конвенционной формы сотрудничества.

Следует согласиться с точкой зрения Н. О. Мороз, отмечавшей, что деятельность международных организаций, направленная на разработку соглашений, анализа состояния преступности, проведения специализированных международных конференций, позволяет скорее находить пути решения тех или иных транснациональных проблем. Однако преимущественно решения органов международных организаций носят рекомендательный характер. В связи с этим особую актуальность приобретает работа подобных организаций (ООН, Интерпол, СНГ и др.) в деле кодификации норм международного права. Таким образом, институциональная форма находится в теснейшем взаимоотношении с конвенционной, и зачастую первая как бы переходит во вторую [11, с. 317—318].

Мнение о двух основных формах подтверждается и в иных источниках. В частности, на это указывает В. П. Зимин [7, с. 10].

Исходя из вышеизложенного, государства, понимая опасность данного вида преступности, прилагают максимум усилий, чтобы активно противостоять этому асоциальному явлению, в том числе посредством заключения и реализации международных соглашений в рассматриваемой сфере. Однако, несмотря на всю опасность исследуемого явления, в настоящее время не в полной мере регламентированы процедуры взаимоотношений между государствами в области противодействия киберпреступлениям. В таких условиях особое значение приобретают региональные международные соглашения, нормы которых направлены на регулирование вопросов сотрудничества правоохранительных и судебных органов государств по вопросам борьбы с киберпреступлениями, их предупреждения и профилактики.

Республика Беларусь является участницей нескольких региональных международных организаций, в частности наше государство входит в состав Организации Договора о коллективной безопасности (далее — ОДКБ), а также СНГ. Изначально спроектированный как международное соглашение о военном сотрудничестве государств (в преамбуле отмечается необходимость согласованных действий Вооруженных Сил договаривающихся сторон, а также выполнения международных соглашений в сфере сокращения объема вооружений), Договор о коллективной безопасности [6] постепенно расширил границы своего влияния, а его участники действуют с целью обеспечить адекватные меры реагирования на любую внешнюю угрозу (не только военного характера).

Одним из документов, принятых в рамках ОДКБ, является Протокол о взаимодействии государств — членов ОДКБ по противодействию преступной деятельности в информационной сфере, подписанный в Москве 23 декабря 2014 г. (далее — Протокол). В соответствии с названным Протоколом государства — участ-

ники ОДКБ приняли на себя обязательство осуществлять сотрудничество для противодействия использованию национальных сегментов сети Интернет в целях, запрещенных национальным законодательством, в том числе взаимодействовать при раскрытии и расследовании преступлений, совершаемых с применением информационно-коммуникационных технологий (далее — ИКТ). При этом содержащаяся в Протоколе дефиниция «преступления в сфере информационных технологий» справедливо включает в себя только те умышленно совершенные общественно опасные деяния, которые запрещены уголовным законом какой-либо из договаривающихся сторон (ст. 1) [20].

В то же время Протокол охватывает достаточно узкий круг преступных деяний, для предупреждения и расследования которых предусмотрена необходимость взаимодействия государств и их правоохранительных органов. В соответствии со статьей 3 Протокола в их число вошли преступления против конституционного строя и безопасности государства, против мира и безопасности человечества, а также преступления в сфере информационных технологий [20].

Следует отметить, что Уголовный кодекс Республики Беларусь (далее — УК) включает главы, посвященные регулированию названных групп преступлений: в главе 32 УК собраны преступления против государства, нормы главы 17 УК содержат перечень преступлений против мира и безопасности человечества, а глава 31 УК посвящена установлению уголовной ответственности за преступления против компьютерной безопасности [28]. Вместе с тем буквальное толкование положений, содержащихся в Протоколе, приводит к выводу о том, что преступления, отраженные в других главах УК, хотя и совершенные с использованием ИКТ, не подпадают под действие указанного Протокола. На практике же большинство преступлений, сопряженных с применением последних достижений в области средств связи и телекоммуникаций, обладают корыстной направленностью и способны причинить существенный вред субъектам хозяйствования. Так, известны многочисленные факты кибератак на объекты банковской системы. Данные атаки, в свою очередь, могут негативно отразиться на экономической безопасности государства.

Кроме того, отдельным видом преступления из числа охватываеваемых понятием «киберпреступность» принято называть распространение материалов, содержащих элементы детской порнографии. Безусловно, подобные деяния следует считать преступными. В частности, за вышеуказанное преступление в статье 343-1 УК (входящей в гл. 30 УК «Преступления против общественного порядка и общественной нравственности») предусмотрена уголовная ответственность [28]. Не вызывает сомнений и тот факт, что данное деяние способно причинить существенный вред сразу нескольким объектам: в отношении несовершеннолетнего, принимавшего участие в съемке, — нарушение его нормального психического и нравственного развития, в отношении иных лиц — существенный подрыв их моральных качеств, что не позволяет считать их полноценными членами здорового гражданского общества. В любом случае социальная и культурная безопасность государства находятся под угрозой. Вместе с тем данное деяние также не входит в число преступлений, в отношении которых следует задействовать механизм межгосударственного сотрудничества, оговоренный в приведенном Протоколе.

В 2017 г. государствами — членами ОДКБ было заключено Соглашение о сотрудничестве в области обеспечения информационной безопасности (далее — Соглашение; вступило в силу 1 апреля 2019 г.) [25].

Нормы названного Соглашения обладают более широким диапазоном действия, нежели нормы Протокола. В частности, в качестве угроз информационной безопасности статья 3 Соглашения называет деструктивное информационное воздействие на ОДКБ в целом и на государства, являющиеся ее членами, использование ИКТ террористическими и экстремистскими организациями, организованными преступными группами и преступными организациями (сообществами), осуществление иной противоправной деятельности, сопряженной с использованием ИКТ [25].

При подобном подходе взаимодействие между государствами — участниками ОДКБ становится возможным при совершении любого преступления, сопряженного с применением ИКТ, независимо от того, к какой главе национального уголовного законодательства государства-участника оно относится. Акцент при определении возможности задействования механизма межгосударственного сотрудничества смещается в сторону определения угрозы в том виде, в котором она сформулирована в статье 3 Соглашения [25].

Вместе с тем подобный подход также нельзя признать до конца удачным. Выражение «осуществление противоправной деятельности с использованием ИКТ» является слишком размытым и предполагает возможность включения в него неопределенного круга деяний, ограниченных лишь способом совершения, без учета характера и объема причиненного вреда. Иными словами, сюда следует отнести любые правонарушения, в том числе не являющиеся преступлениями. В этой связи целесообразно ограничить круг случаев, требующих задействования механизма межгосударственного сотрудничества, лишь серьезными случаями преступной деятельности. Для этого представляется возможным использовать

формулу, в соответствии с которой реализация механизма межгосударственного сотрудничества должна осуществляться в случае совершения опасного преступления, за которое уголовным законодательством государства, на территории которого оно имело место, предусмотрено наказание в виде лишения свободы на срок более четырех лет или иное более строгое наказание.

Таким образом, в рамках деятельности ОДКБ существует самостоятельный механизм, позволяющий консолидировать усилия правоохранительных органов в борьбе с преступлениями, сопряженными с использованием ИКТ.

Не менее важным, в том числе в плане противодействия международной преступности, является участие Республики Беларусь в СНГ. Следует отметить, что региональное соглашение в сфере противодействия киберпреступности, принятое в 2001 г. [24], стало одним из первых подобных договоров в мировой практике. Однако с течением времени некоторые его нормы утратили свою актуальность, что потребовало его пересмотра и обновления. Новое Соглашение о сотрудничестве государств — участников СНГ в борьбе с преступлениями в сфере информационных технологий [23] было подписано в Душанбе в сентябре 2018 г. (вступило в силу 12 марта 2020 г.). Следует отметить, что Республика Беларусь одной из первых ратифицировала данное Соглашение (Закон № 207-З от 16 июля 2019 г. [15]).

Характеризуя деятельность нашего государства в рассматриваемой сфере, В. Ю. Арчаков справедливо отмечает, что «Беларусь активно и последовательно поддерживает международное взаимодействие в области обеспечения информационной безопасности, принимает и ратифицирует заключенные соглашения, участвует в разработке концептуальных подходов, модельного законодательства и в целом весьма настойчиво выступает за минимизацию общих угроз Содружества, в том числе и в информационной сфере» [1, с. 7].

Необходимо отметить, что взаимодействие государств — участников СНГ по вопросам противодействия международной преступности входит в полномочия сразу нескольких межправительственных органов: Совета министров внутренних дел государств — участников СНГ, Координационного совета генеральных прокуроров государств — участников СНГ, Совета руководителей органов безопасности и специальных служб государств — участников СНГ. Кроме того, в целях согласования действий министерств внутренних дел государств — участников СНГ в борьбе с организованной преступностью, терроризмом, незаконным оборотом наркотиков и иными опасными видами преступлений создано специальное Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств — участников СНГ [19]. В структуру Бюро входит управление по координации борьбы с организованной преступностью, терроризмом, незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров, которое состоит из двух отделов:

— содействия в межгосударственном розыске, экстрадиции, проведении специальных мероприятий и борьбе с терроризмом;

— координации борьбы с незаконным оборотом наркотических средств, психотропных веществ, и их прекурсоров (в том числе Региональная оперативная группа в Центрально-Азиатском регионе) [26].

В Бюро не создано специализированное подразделение, деятельность которого была бы направлена на борьбу с киберпреступлениями или же на координацию деятельности правоохранительных органов государств — участников СНГ в этой сфере. При этом в соответствии с статьей 2.1 Положения о Бюро одним из направлений его координационной деятельности является противодействие организованной преступности, незаконному обороту наркотиков, терроризму и иным опасным видам преступлений [19]. Таким образом, перечень направлений координационной деятельности Бюро остается открытым. Вместе с тем киберпреступления являются столь же опасными, как и организованная преступность и преступления террористического характера. В этой связи представляется возможным отдельно выделить данную группу преступлений в статье 2.1 Положения о Бюро для того, чтобы данная сфера однозначно охватывалась взаимодействием государств. Кроме того, в Бюро может быть создано специальное подразделение, направленное на борьбу с киберпреступлениями, что, на наш взгляд, позволит повысить эффективность работы Бюро в рассматриваемом направлении.

Для обмена информацией в Бюро создан и функционирует Специализированный банк данных, Инструкция о деятельности которого утверждена решением Совета министров внутренних дел государств — участников СНГ от 2 сентября 2015 г. [13]. В указанном банке данных содержится информация по восьми направлениям: организованная преступность, терроризм, незаконный оборот наркотиков, экономическая преступность, незаконная миграция, неформальные объединения болельщиков спортивных команд, торговля людьми, иная информация. Таким образом, самостоятельного направления «киберпреступность» указанный банк не включает (как представляется, она относится к «иной информации»). В то же время отдельные преступления, сопряженные с использованием ИКТ, могут содержаться в разделах «экономическая преступность», «терроризм», «организованная преступность», «торговля людьми».

Всего же на начало 2022 г. в Специализированном банке данных Бюро содержалась информация в отношении 3920 объектов учета, в том числе: по линии организованной преступности — 455, терроризма — 1516, незаконного оборота наркотиков — 169, экономической преступности — 12, незаконной миграции — 315, торговли людьми — 14, неформальных объединений болельщиков — 1439 [17, с. 25]. Собранные сведения используются органами внутренних дел стран Содружества, в том числе при организации и проведении необходимых оперативно-розыскных мероприятий.

Анализ нормативной базы взаимодействия Бюро с иными органами отраслевого сотрудничества был проведен Н. В. Сидоровой и Н. Р. Весельской [22]. Согласно исследованиям указанных авторов, нормативную базу взаимодействия Бюро с иными органами отраслевого сотрудничества образуют соответствующие договоры, к числу которых относятся Протокол о взаимодействии с Координационной службой Совета командующих Пограничными войсками от 7 февраля 2000 г., Протокол об информационном взаимодействии с Секретариатом Координационного совета генеральных прокуроров государств — участников СНГ от 30 ноября 2005 г., Протокол об информационном взаимодействии с Комитетом глав правоохранительных подразделений Совета руководителей таможенных служб от 21 сентября 2009 г., Протокол о сотрудничестве с Советом руководителей подразделений финансовой разведки государств — участников СНГ 2014 г.

Эффективность работы Бюро подтверждается ежегодными результатами его деятельности за отчетный период. Так, согласно данным за 2021 г., при участии сотрудников Бюро было раскрыто 3026 преступлений (для сравнения, в 2020 г. этот показатель составил 2400, а в 2019 г. — 3083 преступлений) [17, с. 15]. В рамках реализации своих полномочий работниками Бюро в 2020 г. оказана практическая помощь трем оперативным группам, командированным в государства — участники СНГ (в том числе один раз в Республику Беларусь).

В рамках оперативно-профилактических мероприятий, предусмотренных Межгосударственной программой совместных мер борьбы с преступностью на 2019—2023 годы [14] на основании выявления преступлений исследуемой группы были установлены и привлечены к уголовной ответственности в 2019 г. 242, в 2020 г. — 403, а в 2021 г. — 890 человек. В 2021 г. пресечена деятельность 1093 информационных ресурсов, работа которых осуществлялась с нарушением действующего законодательства (2020 г. — 512, в 2019 г. — 42) [17, с. 18].

Как видно, Бюро активно включилось в работу по выявлению возникающих киберугроз и нейтрализации преступных посягательств на информационную безопасность. В целях усиления роли Бюро и повышения эффективности сотрудничества между правоохранительными органами государств — участников СНГ необходимо конкретизировать (а при необходимости — расширить) компетенцию этого межправительственного органа, распространив ее на преступления в сфере информационной безопасности (поскольку никакого иного специализированного органа, действующего в указанной сфере, как было отмечено, на территории СНГ не создано). Включение координации деятельности правоохранительных органов в рассматриваемой области в компетенцию Бюро будет способствовать повышению эффективности противодействия и предупреждения киберпреступности.

В то же время координационные функции Бюро не следует чрезмерно расширять, устанавливая его обязательное участие в рассмотрении всех без исключения правонарушений, сопряженных с применением компьютерных или иных телекоммуникационных технологий. Вмешательство Бюро, как верно отмечает Н. О. Мороз, требуется лишь при наиболее опасных и серьезных преступных киберугрозах, способных причинить значительный вред стратегически важным экономическим объектам, государственным информационным системам, а также в случае выявления фактов распространения цифровых материалов, связанных с детской порнографией, либо кибератак, совершенных организованными преступными группами [10, с. 13]. В качестве критерия определения значения киберугрозы указанный автор справедливо предлагает использовать правило, содержащееся в пункте *b* статьи 2 Конвенции Организации Объединенных Наций против транснациональной организованной преступности от 15 ноября 2000 г.: «серьезное преступление означает преступление, наказуемое лишением свободы на максимальный срок не менее четырех лет или более строгой мерой наказания» [8].

Анализ отдельных составляющих институционального механизма международного сотрудничества Республики Беларусь в борьбе с киберпреступностью показал, что самостоятельные элементы такого сотрудничества усматриваются в рамках действия Соглашения ОДКБ, однако используемые в нем дефиниции требуют совершенствования и унификации с действующими уголовно-правовыми нормами.

В рамках СНГ сформирован и функционирует достаточно устойчивый и разносторонний институциональный механизм взаимодействия правоохранительных органов, целью которого является осуществление комплексного подхода в вопросах противодействия транснациональной преступности, включая преступления, совершаемые с использованием ИКТ. В то же время представляется важным формирование в рамках Бюро по координа-

ции борьбы с организованной преступностью и иными опасными видами преступлений самостоятельного подразделения, специализацией которого стала бы координация деятельности правоохранительных органов в вопросах противодействия современным проявлениям киберпреступности, их предупреждения и профилактики.

Список использованных источников

1. Арчаков, В. Ю. О теоретико-методологических подходах к обеспечению международной информационной безопасности / В. Ю. Арчаков // Журн. междунар. права и междунар. отношений. — 2019. — № 3-4 (90-91). — С. 3—11.
2. Баранова, Е. СК: в Беларуси за последние пять лет количество киберпреступлений увеличилось в 10 раз / Е. Баранова [Электронный ресурс] // СБ — Беларусь сегодня. — Режим доступа: <https://www.sb.by/articles/sk-v-belarusi-za-poslednie-pyat-let-kolichestvo-kiberprestupleniy-uvelichilos-v-10-raz-.html>. — Дата доступа: 29.06.2022.
3. Батуева, Е. В. Американская концепция угроз информационной безопасности и ее международно-политическая составляющая: дис. ... канд. полит. наук: 23.00.04 / Е. В. Батуева. — М., 2015. — 207 л.
4. Головенчик, Г. Г. Цифровизация белорусской экономики в современных условиях глобализации / Г. Г. Головенчик. — Минск: Изд. центр БГУ, 2019. — 257 с.
5. Данилевич, А. А. Международная правовая помощь по уголовным делам: уголовно-процессуальный аспект / А. А. Данилевич, В. И. Самарин. — Минск: БГУ, 2009. — 127 с.
6. Договор о коллективной безопасности: [подп. в г. Ташкенте 15 мая 1992 г.] [Электронный ресурс] // Единый реестр правовых актов и других документов Содружества Независимых Государств. — Режим доступа: <http://cis.minsk.by/reestr/ru/index.html#reestr/view/text?doc=79>. — Дата доступа: 05.04.2022.
7. Зимин, В. П. Международное сотрудничество в области борьбы с преступностью и охраны общественного порядка / В. П. Зимин. — М., 1993. — 157 с.
8. Конвенция Организации Объединенных Наций против транснациональной организованной преступности [Электронный ресурс] // Система официальной документации ООН. — Режим доступа: <https://undocs.org/ru/A/RES/55/25>. — Дата доступа: 17.05.2022.
9. Моисеев, Е. Г. Международно-правовые основы сотрудничества стран СНГ / Е. Г. Моисеев; под ред. К. А. Бекяшева. — М.: Юристъ, 1997. — 265 с.
10. Мороз, Н. О. Актуальные вопросы международного сотрудничества в борьбе с преступностью в сфере высоких технологий в рамках СНГ / Н. О. Мороз // Междунар. уголов. право и междунар. юстиция. — 2016. — № 3. — С. 12—14.
11. Мороз, Н. О. Формы и направления международного сотрудничества в борьбе с преступностью в сфере высоких технологий / Н. О. Мороз // Учен. записки Таврич. нац. ун-та им. В. И. Вернадского. Сер. «Юридические науки».— 2011. — Т. 24 (63), № 1. — С. 315—325.
12. Мысина, А. И. К вопросу о региональных правовых основах сотрудничества государств по противодействию преступлениям в сфере информационных технологий / А. И. Мысина // Рос. юстиция. — 2019. — № 5. — С. 20—24.
13. Об утверждении Инструкции о порядке функционирования Специализированного банка данных Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств — участников Содружества Независимых Государств: решение Совета министров внутренних дел государств — участников Содружества Независимых Государств от 02.09.2015 г. // Сотрудничество министерств внутренних дел государств — участников Содружества Независимых Государств: сб. актуальных док. Совета министров внутренних дел. Т. II. Ч. II (2008—2018 гг.). — М. : Москов. ун-т МВД России им. В. Я. Кикотя, 2019. — С. 164—173 [Электронный ресурс] // Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств — участников СНГ. — Режим доступа: <https://www.bkbopcis.ru/upload/iblock/f53/f53eaf45a704079d2b713c5e838179e8.pdf>. — Дата доступа: 14.06.2022.
14. О Межгосударственной программе совместных мер борьбы с преступностью на 2019—2023 годы: решение Совета глав государств СНГ: [принято в г. Душанбе 28 сент. 2018 г.] [Электронный ресурс] // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. — Минск, 2022.
15. О ратификации Соглашения о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий: Закон Респ. Беларусь от 16 июля 2019 г. № 207-З [Электронный ресурс] // Там же.
16. Организационно-правовой механизм сотрудничества в противодействии транснациональной преступности в рамках Содружества Независимых Государств [Электронный ресурс] // Исполнительный комитет СНГ. — Режим доступа: <http://www.cis.minsk.by/page/13962>. — Дата доступа: 01.02.2022.
17. О результатах деятельности Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств — участников Содружества Независимых Государств за 2021 год. — М., 2022. — 58 с. [Электронный ресурс] // Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств — участников СНГ. — Режим доступа: <https://www.bkbopcis.ru/bkbop/dokumenty/%D0%B8%D1%81%D0%BF.%2020.06.2022.pdf>. — Дата доступа: 14.06.2022.
18. О ходе реализации Решения СМВД от 2 сентября 2015 года «О развитии информационного обмена органов внутренних дел (полиции) государств — участников Содружества Независимых Государств по предупреждению противоправных деяний со стороны членов неформальных объединений болельщиков спортивных команд, в том числе в период проведения международных массовых спортивных и зрелищных мероприятий»: решение Совета министров внутренних дел государств — участников Содружества Независимых Государств от 06.09.2016 г. // Сотрудничество министерств внутренних дел государств — участников Содружества Независимых Государств: сб. актуальных док. Совета министров внутренних дел. Т. II. Ч. II (2008—2018 гг.). — М. : Москов. ун-т МВД России им. В. Я. Кикотя, 2019. — С. 186—189 [Электронный ресурс] // Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств — участников СНГ. — Режим доступа: <https://www.bkbopcis.ru/upload/iblock/f53/f53eaf45a704079d2b713c5e838179e8.pdf>. — Дата доступа: 14.06.2022.
19. Положение о Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств — участников Содружества Независимых Государств: решение Совета глав правительств Содружества Независимых Государств: [принято в г. Москве 25 нояб. 2005 г.] [Электронный ресурс] // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. — Минск, 2022.
20. Протокол о взаимодействии государств — членов Организации Договора о коллективной безопасности по противодействию преступной деятельности в информационной сфере: [подп. в г. Москве 23 дек. 2014 г.] [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. — 31.07.2015, 3/3137. — Режим доступа: <https://www.pravo.by/document/?guid=12551&p0=E71400003&p1=1>. — Дата доступа: 15.03.2022.

21. Родевич, В. Ч. Транснациональная преступность: теория и практика борьбы в Республике Беларусь / В. Ч. Родевич, С. С. Тупеко. — Минск: Акад. МВД Респ. Беларусь, 2012. — 143 с.
22. Сидорова, Н. В. Институциональный механизм сотрудничества государств — участников Содружества Независимых Государств в сфере противодействия преступности / Н. В. Сидорова, Н. Р. Весельская // Общественная безопасность, законность и правопорядок в III тысячелетии. – 2019. — № 5-3. — С. 141—145.
23. Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий: [закл. в г. Душанбе 28 сент. 2018 г.] [Электронный ресурс] // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. — Минск, 2022.
24. Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации: [закл. в г. Минске 1 июня 2001 г.] [Электронный ресурс] // Исполнительный комитет СНГ. — Режим доступа: <http://cis.minsk.by/page/866>. — Дата доступа: 10.05.2022.
25. Соглашение о сотрудничестве государств — членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности [Электронный ресурс]: [закл. в г. Минске 30 нояб. 2017 г.] // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. — Минск, 2022.
26. Структура Бюро [Электронный ресурс] // Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств — участников Содружества Независимых Государств. — Режим доступа: <https://www.bkbopcis.ru/bkbop/struktura-byuro/>. — Дата доступа: 14.06.2022.
27. Талимончик, В. П. Конвенции о киберпреступности и унификация законодательства / В. П. Талимончик // Информ. право. — 2008. — № 2. — С. 27—30.
28. Уголовный кодекс Республики Беларусь от 9 июля 1999 г. № 275-З: принят Палатой представителей 2 июня 1999 г.: одобр. Советом Респ. 24 июня 1999 г.: текст по сост. на 1 июня 2021 г. [Электронный ресурс] // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. — Минск, 2022.

Статья поступила в редакцию 1 декабря 2021 г., доработана в июне 2022 г.