Научная статья
Научная специальность
12.00.08 «Уголовное право и криминология; уголовно-исполнительное право»
12.00.10 «Международное право; европейское право»

УДК 341.45
DOI https://doi.org/10.26516/2071-8136.2022.3.90

К ПРОБЛЕМЕ СОВЕРШЕНСТВОВАНИЯ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

© Евдокимов К. Н.[1], Хобонкова К. В.[2], 2022
[1] Иркутский юридический институт (филиал) Университета прокуратуры Российской Федерации, г. Иркутск, Россия
[2] Иркутский национальный исследовательский технический университет, г. Иркутск, Россия

Исследуется проблема функционирования механизма международного сотрудничества в сфере противодействия киберпреступности. Определены понятие и основные признаки киберпреступности, система международных организаций, осуществляющих политику и нормативное регулирование в области борьбы с киберпреступлениями. Выделены основополагающие международные правовые акты, определяющие взаимодействие Российской Федерации с иностранными государствами в сфере предупреждения, выявления, раскрытия и расследования киберпреступлений. Сделан вывод о региональном характере, фрагментарности и неэффективности существующей правовой основы международного сотрудничества по противодействию киберпреступности. Вносятся предложения по совершенствованию международного уголовного права в рассматриваемой сфере и повышению качества международного сотрудничества по предупреждению, борьбе и минимизации (ликвидации) последствий киберпреступлений.

Ключевые слова: информационно-коммуникационные технологии, киберпреступность, киберпреступления, международное сотрудничество, международное уголовное право, Организация Объединенных Наций, Российская Федерация, Содружество Независимых Государств, Шанхайская организация сотрудничества.

ON THE PROBLEM OF IMPROVING INTERNATIONAL COOPERATION IN COUNTERING CYBERCRIME

© Evdokimov K. N.[1], Hobonkova K. V.[2], 2022
[1] Irkutsk Law Institute (branch) University of the Prosecutor's Office of the Russian Federation, Irkutsk, Russian Federation
[2] Irkutsk National Research Technical University, Irkutsk, Russian Federation

The problem of functioning of the mechanism of international cooperation in the field of countering cybercrime is investigated. The concept and main features of cybercrime, the system of international organizations implementing policy and regulatory regulation in the field of combating cybercrime are defined. The fundamental international legal acts defining the interaction of the Russian Federation with foreign states in the field of prevention, detection, disclosure and investigation of cybercrimes are highlighted. The authors conclude about the regional nature, fragmentation and inefficiency of the existing legal framework for international cooperation in countering cybercrime. Proposals are made to improve international criminal law in this area and to improve the quality of international cooperation in preventing, combating and minimizing (eliminating) the consequences of cybercrime.

Keywords: information and communication technologies, cybercrime, cybercrimes, international cooperation, international criminal law, United Nations, Russian Federation, Commonwealth of Independent States, Shanghai Cooperation Organization.

Введение

Современная киберпреступность носит высокотехнологичный, организованный и латентный характер, причиняя российскому обществу и экономике колоссальный вред.

По данным экспертов «Лаборатории Касперского», в случае успешной атаки киберпреступников крупные компании теряют около 20 млн руб., а предприятия среднего и малого бизнеса в среднем 780 тыс. руб. – за счет вынужденного простоя, упущенной прибыли и расходов на дополнительные услуги специалистов. На ликвидацию последствий инцидента и профилактику крупные компании дополнительно тратят около 2,1 млн руб., а небольшие – около 300 тыс. руб.[1]

В 2015 г. ущерб экономике России от киберпреступности уже превысил 200 млрд руб.[2], а в последующие годы он только возрастал в арифметической прогрессии: в 2018 г. ущерб российской экономике от киберугроз составил более 1,1 трлн руб.[3], в 2019 г. – около 2,5 трлн руб.[4], в 2020 г. – 3,5 трлн руб., а в 2021 г. предполагаемый экономический ущерб Российской Федерации

[1] Так ли страшен Интернет. О настоящей опасности киберугроз рассказывает «Газета.Ru». URL: http://www.gazeta.ru/tech/2014/11/05_a_6289085.shtml (дата обращения: 09.01.2022).

[2] Ущерб экономике России от киберпреступности превысил 200 млрд рублей. URL: http://ria.ru/economy/20160413/1409855094.html#ixzz45jCApNtn (дата обращения: 09.01.2022).

[3] Сбербанк прогнозирует ущерб экономике России от киберугроз в 2018 году в 1,1 трлн рублей. URL: https://www.kommersant.ru/doc/3676752 (дата обращения: 09.01.2022).

[4] Сбербанк оценил ущерб экономике России от кибератак в 2019 году в 2,5 трлн рублей. URL: https://www.kommersant.ru/doc/4226302 (дата обращения: 09.01.2022).

от высокотехнологической киберпреступности достиг 7 трлн руб.[1]

При этом под киберпреступностью авторы понимают совокупность преступлений, совершенных лицами с использованием компьютерных и информационно-коммуникационных технологий за определенный период времени в национальном либо международном сегменте сети Интернет, а также иных информационно-коммуникационных сетях, мессенджерах, компьютерных системах и т. п., образующих так называемое киберпространство.

Следует также отметить сохраняющуюся тенденцию постоянного роста российской киберпреступности. Так, если в 2015 г. было зарегистрировано 43 816 киберпреступлений (деяний, совершенных с использованием информационно-коммуникационных и компьютерных технологий), то в 2018 г. – уже 174 674 подобных преступлений, в 2019 г. – 294 409, в 2020 г. – 510 396, а в 2021 г. – 517 722[2].

Вместе с тем данный вид преступности по своей природе является трансграничным и транснациональным, поскольку киберпространство не имеет государственных границ, а киберпреступники, являясь частью технического «андеграунда» мирового сообщества, не разделяют себя по национальному признаку и часто объединяются в международные организованные преступные группировки [1, с. 127; 3, с. 987].

Вышеуказанные свойства современной киберпреступности обусловливают необходимость международно-правового сотрудничества государств как для предупреждения данного негативного социального явления, так и в борьбе с киберпреступлениями.

Материалы и методы исследования

Авторы, используя базовые положения диалектического метода познания, в рамках которого применялась система общенаучных (логический, исторический, системно-структурный) и частнонаучных методов (историко-правовой, формально-юридический, сравнительно-правовой, правового моделирования), провели анализ международных правовых актов Организации Объединенных Наций, Содружества Независимых Государств, Шанхайской организации сотрудничества, определяющих взаимодействие государств-членов в сфере противодействия киберпреступности.

Результаты исследования

Важнейшую роль в координации действий правоохранительных органов по противодействию киберпреступности играют международные, межрегиональные и региональные межгосударственные организации. К их числу следует отнести Организацию Объединенных Наций (далее – ООН), Организацию экономического сотрудничества и развития (далее – ОЭСР), Совет Европы (далее – СЕ), Европейский союз (далее – ЕС), Содружество Независимых Государств (далее – СНГ), Шанхайскую организацию сотрудничества (далее – ШОС), БРИКС (Бразилия, Россия, Индия, Китай, Южно-Африканская Республика), а также такие международные правоохранительные организации, как Международная организация уголовной полиции (далее – Интерпол) и Полицейская служба Европейского союза (далее – Европол).

В период с 1983 по 1985 г., на этапе возникновения киберпреступности, экспертами ОЭСР были проанализированы существующие составы компьютерных преступлений, возможные угрозы и риски, исходящие от них. После чего 26 ноября 1992 г. Совет ОЭСР принимает Рекомендацию о руководящих принципах обеспечения безопасности информационных систем[3].

С 1990 г. в процесс международного сотрудничества по предупреждению киберпреступности активно включилась Организация Объединенных Наций. На VIII Конгрессе ООН по предупреждению преступности и обращению с правонарушителями была принята резолюция, призывающая государства – члены ООН увеличить усилия по борьбе с киберпреступностью, модернизировать национальное уголовное законодательство, содействовать развитию в будущем структуры международных принципов и стандартов предотвращения, судебного преследования и наказания в области киберпреступности[4].

Спустя несколько лет, на 56-й сессии Генеральной Ассамблеи ООН, была принята Резолюция № 56/261 от 31 января 2002 г., призывающая к усилению борьбы с киберпреступностью[5]. В Резолюции было предложено развивать национальные законодательства стран – членов ООН об уголовной ответственности за киберпресту-

[1] Сбербанк подсчитал потери российской экономики в 2021 году от киберпреступности. URL: https://tass.ru/ekonomika/8761953 (дата обращения: 09.01.2022).

[2] Форма федерального статистического наблюдения № 4-ЕГС «Сведения о состоянии преступности и результатах расследования преступлений» за 2015–2021 гг. // Портал правовой статистики. Генеральная прокуратура Российской Федерации : сайт. URL: http://crimestat.ru/analytics (дата обращения: 11.02.2022).

[3] Sieber U. Legal Aspects of Computer-Related Crime in the Information Society. URL: http://europa.eu.int/ISPO/legal/en/comcrime/sieber.doc (дата обращения: 09.01.2022).

[4] 8 th U.N. Congress on the Prevention of Crime and the Treatment of Offenders, U.N., U.N. Doc. A/CONF. 144/L.l 1. URL: http://www.un.org (дата обращения: 09.01.2022).

[5] Резолюция Генеральной Ассамблеи ООН от 31 янв. 2002 г. № 56/261 «Планы действий по осуществлению Венской декларации о преступности и правосудии: ответы на вызовы XXI века» (принята в г. Нью-Йорке на 93-м пленарном заседании 56-й сессии Генеральной Ассамблеи ООН) // КонсультантПлюс : справочная правовая система. (дата обращения: 09.01.2022).

пления и разработать комплекс мер по борьбе с преступлениями, связанными с использованием высоких технологий и компьютеров. Тем самым существование киберпреступности и необходимость предупреждения и борьбы с ней были признаны всем мировым сообществом. Так называемая проблема киберпреступности встала в один ряд наравне с международным терроризмом, работорговлей, торговлей наркотиками и оружием.

Следует подчеркнуть, что Российская Федерация как член Организации Объединенных Наций занимает активную позицию в вопросе противодействия киберпреступности путем участия в работе комитетов, экспертных комиссий и групп ООН, а также голосования за принятие соответствующих деклараций и резолюций ООН.

Важным фактом является то, что каждые пять лет ООН проводит Конгресс по предупреждению преступности и уголовному правосудию (до 2005 г. – Конгресс ООН по предупреждению преступности и обращению с правонарушителями), на котором в обязательном порядке в той или иной форме затрагивается вопрос о международном сотрудничестве по предупреждению и борьбе с киберпреступлениями, в том числе путем проведения семинаров, практикумов по разработке конкретных мер и методик противодействия преступлениям, совершенным с использованием компьютеров и IT-технологий.

Также следует отметить, что Российская Федерация осуществляет активное международное сотрудничество в сфере предупреждения киберпреступности с приграничными и дружественными государствами в формате таких региональных и межрегиональных межгосударственных организаций, как СНГ, ОДКБ, ШОС, БРИКС.

В частности, планирование и проведение скоординированных мероприятий и операций между правоохранительными органами государств – участников Содружества Независимых Государств по предупреждению преступлений в сфере компьютерной информации; обмен информацией; исполнение запросов о проведении оперативно-разыскных мероприятий, а также процессуальных действий; подготовка и повышение квалификации кадров, в том числе путем стажировки специалистов, организации конференций, семинаров, учебных курсов и др., проводятся в рамках недавно принятого Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий[1].

В свою очередь, ШОС и БРИКС стали для Российской Федерации межрегиональными государственными платформами для эффективного взаимодействия в области противодействия транснациональной киберпреступности.

Так, взаимодействие по различным направлениям противодействия киберпреступности (правовым, организационным, информационным, криминалистическим, экспертным, антитеррористическим, военно-техническим и др.) правоохранительных органов государств – участников ШОС осуществляется в рамках Соглашения между правительствами государств – членов Шанхайской организации сотрудничества в области обеспечения международной информационной безопасности от 16 июня 2009 г.[2]

Реализация положений Соглашения ШОС в области обеспечения международной информационной безопасности осуществляется на ежегодных совещаниях руководителей силовых министерств и ведомств ШОС, где особое внимание уделяется вопросам профилактики и борьбы с киберпреступностью, а также усиления сотрудничества в сферах противодействия терроризму, экстремизму и сепаратизму[3].

В свою очередь, международное сотрудничество по предупреждению и борьбе с киберпреступностью в рамках БРИКС географически выходит за пределы Евразийского континента, предоставляя еще большие возможности для взаимодействия правоохранительных органов в рассматриваемой сфере. Однако в настоящее время международное сотрудничество в области противодействия компьютерным преступлениям ведется в формате консультаций экспертных групп.

Например, на 12-м саммите БРИКС (17 ноября 2020 г., г. Москва) в принятой Московской декларации глав государств была отмечена

[1] Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий: заключено в г. Душанбе 28 сентября 2018 г. // КонсультантПлюс : справочная правовая система.

[2] Соглашение между правительствами государств – членов Шанхайской организации сотрудничества в области обеспечения международной информационной безопасности (Екатеринбург, 16 июня 2009 г.) : утверждено распоряжением Правительства РФ от 16 июля 2009 г. № 984-р // Бюллетень международных договоров. 2012. № 1. С. 13–21.

[3] Главы МВД стран ШОС в Душанбе обсудят вопросы борьбы с киберпреступностью. URL: http://infoshos.ru/ru/?idn=14147 (дата обращения: 09.01.2022); В Таджикистане состоялось заседание Генеральных прокуроров государств – членов Шанхайской организации сотрудничества. URL: http://genproc.gov.ru/smi/news/genproc/news-1454024/ (дата обращения: 09.01.2022); Страны ШОС усилят взаимодействие в области кибербезопасности. URL: https://ria.ru/20200915/kiberbezopasnost-1577270454.html (дата обращения: 09.01.2022).

обеспокоенность увеличением числа и растущей сложностью использования информационно-компьютерных технологий (далее – ИКТ) в преступных целях, а также необходимость разработки под эгидой ООН всеобъемлющей международной конвенции по борьбе с использованием ИКТ в преступных целях[1].

Между тем, проводя криминологический анализ международно-правового сотрудничества России с зарубежными странами по противодействию киберпреступности, следует отметить, что в настоящее время наибольший практический эффект дает участие Российской Федерации в Международной организации уголовной полиции (Интерпол). Интерпол на сегодняшний день – крупнейшая в мире международная полицейская организация, в которую входят более 190 государств.

В 1995 г. Интерполом была проведена первая международная конференция по киберпреступности, подтвердившая обеспокоенность международного сообщества распространением киберпреступлений. Участники конференции подчеркнули, что вызывает тревогу отсутствие международного механизма для рационального и эффективного противостояния этому виду преступности[2]. В дальнейшем конференции по предупреждению и борьбе с киберпреступностью проводились Интерполом постоянно с периодичностью в 2 года: 1996, 1998, 2000, 2002, 2004, 2006, 2008, 2010, 2012, 2014, 2016, 2018[3], и только пандемия коронавирусной инфекции COVID-19 прервала очередность проведения вышеуказанных научно-практических мероприятий.

В соответствии с Указом Президента РФ от 30 июля 1996 г. № 1113 «Об участии Российской Федерации в деятельности Международной организации уголовной полиции – Интерпола»[4] было создано Национальное центральное бюро Интерпола МВД России, территориальные подразделения которого действуют в практически во всех субъектах Российской Федерации[5].

Учитывая, что большинство киберпреступлений (неправомерный доступ к компьютерной информации, мошенничество в сфере компьютерной информации и др.) относятся к подследственности следователей органов внутренних дел, то возможности российской полиции по проведению различных следственных и оперативно-разыскных мероприятий в рамках данной международной организации трудно переоценить.

В настоящее время международное сотрудничество с Интерполом в сфере противодействия киберпреступности на постоянной основе осуществляют сотрудники НЦБ Интерпола и Управления «К» БСТМ МВД России[6], что не исключает возможности участия в раскрытии и расследовании киберпреступлений других правоохранительных органов (например, ФСБ РФ, СК РФ).

Нельзя не отметить, что Европейский союз также отреагировал на проблему межгосударственного взаимодействия по борьбе с киберпреступностью, создав в январе 2013 г. при объединенной полицейской службе Европейского союза (Европол)[7] центр по борьбе с киберпреступностью, деятельность которого направлена на противодействие киберпреступности в Европейском союзе и защиту информационных прав европейских граждан, бизнеса и государственных структур[8].

В 2004 г. приказом МВД России № 859[9] в структуре НЦБ Интерпола МВД России был создан Российский национальный контактный пункт по взаимодействию с Европолом (РНКП), которому были поставлены задачи по обеспечению обмена информацией между компетентными органами Российской Федерации (МВД, ФСБ, ФТС, ФСКН России, Росфинмониторинг) и Европолом в сфере предупреждения и борьбы с киберпреступлениями, а также выработке мер, направленных на совершенствование механизма международного сотрудничества в указанной сфере[10].

Несмотря на политические, экономические, научно-технические и иные санкции со стороны государств G7 (Великобритания, Германия,

[1] Московская декларация XII саммита БРИКС. URL: http://www.kremlin.ru/supplement/5581 (дата обращения: 09.01.2022).

[2] Interpol, Steering Committee for Information Technology Crime. URL: hrtp://www.interpol.int/Public/TechnologyCrime/WorkingParties/Default.asp#steeringCom (дата обращения: 09.01.2022).

[3] В Сингапуре прошла совместная конференция Интерпола и Европола по борьбе с киберпреступностью. URL: http://xn--b1aew.xn--p1ai/mvd/structure1/Upravlenija/uos/P (дата обращения: 09.01.2022).

[4] Об участии Российской Федерации в деятельности Международной организации уголовной полиции – Интерпола : указ Президента РФ от 30 июля 1996 г. № 1113 (ред. от 27.10.2011) // КонсультантПлюс : справочная правовая система.

[5] Национальное центральное бюро Интерпола МВД России. URL: https://mvd.ru/mvd/structure1/Upravlenija/Nacionalnoe_centralnoe_bjuro_Interpola (дата обращения: 09.01.2022).

[6] При участии МВД России в рамках международной полицейской операции ликвидировано вредоносное программное обеспечение. URL: https://mvd.ru/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii/Publikacii_i_vistuplenija/item/7126918/ (дата обращения: 09.01.2022).

[7] Europol : офиц. сайт. URL: https://www.europol.europa.eu/content/page/history-149 (дата обращения: 09.01.2022).

[8] Europol : официальный сайт. URL: https://www.europol.europa.eu/ec3/cyber-strategy(дата обращения: 09.01.2022).

[9] О создании в структуре Национального центрального бюро Интерпола при МВД России Российского национального контактного пункта по взаимодействию с Европолом : приказ МВД России от 23 дек. 2004 г. № 859 // КонсультантПлюс : справочная правовая система.

[10] НЦБ Интерпола МВД России. Взаимодействие с Европолом. URL: https://mvd.ru/mvd/structure1/Upravlenija/Nacionalnoe_centralnoe_bjuro_Interpola/Vzaimodejstvie_s_Evropolom (дата обращения: 09.01.2022).

Италия, Канада, США, Франция, Япония) и Европейского союза в отношении России, а также проводимую ими в последние годы враждебную антироссийскую политику, Российская Федерация не отказалась от дальнейшего международного сотрудничества в сфере противодействия киберпреступности.

Поэтому важным шагом стал тот факт, что 28 декабря 2019 г., несмотря на активное противостояние США и европейских стран, Генеральная Ассамблея ООН (далее – ГА ООН) принимает предложенную Российской Федерацией резолюцию[1] по разработке международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях (в поддержку резолюции № 74/247 ГА ООН от 27 декабря 2019 г. высказались 79 государств, 60 проголосовали против, 33 страны воздержались), и с этой целью создается специальный Межправительственный комитет экспертов открытого состава под эгидой ООН[2].

Принятие вышеуказанной Конвенции ООН является назревшей необходимостью, признаваемой большинством как развитых, так и развивающихся стран.

Обсуждения и заключения

В настоящее время международное сотрудничество в сфере противодействия киберпреступности носит блоковый и фрагментарный характер, что обусловлено геополитическими, экономическими, национальными интересами отдельных государств и отсутствием соответствующего международно-правового акта Организации Объединенных Наций в вышеуказанной сфере, который бы определил общие для всех стран правовые, организационные, политические, информационные, научные, технические и иные аспекты противодействия киберпреступлениям.

Анализ научных работ [2; 4–7] и международных правовых актов позволяет авторам прийти к следующим выводам.

Для достижения эффективных результатов в противодействии международной киберпреступности, а также обеспечения глобальной информационной безопасности полагаем логичным шагом разработку и принятие Организацией Объединенных Наций двух отдельных международных правовых актов, а именно: конвенции ООН о противодействии киберпреступности и конвенции ООН о международной информационной безопасности.

Думаем, что первый юридический документ должен носить организационно-методический и уголовно-правовой характер, содержать: понятийно-терминологический аппарат; общие организационно-правовые принципы; перечень составов киберпреступлений; комплекс уголовно-правовых, криминологических, криминалистических и организационно-технических мер по противодействию киберпреступности; процедурный механизм международного взаимодействия правоохранительных органов в указанной сфере.

В свою очередь, второй документ, по мнению автора, должен носить не столько юридический, сколько политический, технический и организационный характер, регулируя такие вопросы, как принципы и правила обеспечения международной информационной безопасности в киберпространстве; международно-правовые нормы, запрещающие преступные деяния политической направленности, например планирование, подготовку, развязывание или ведение войны в киберпространстве; создание, использование и распространение «кибероружия» и др.

Данная конвенция, по нашему мнению, должна предусматривать альтернативный механизм осуществления правосудия за совершение указанных деяний как национальной судебной юстицией, так и Международным уголовным судом (например, в случае спора о юрисдикции между судами нескольких государств либо отказе отдельного государства вершить правосудие), так как рассматриваемые киберпреступления носят международный характер и направлены на причинение вреда миру и безопасности человечества.

При этом авторы не разделяют точку зрения тех ученых [5, с. 95; 6], которые предлагают создать самостоятельный международный трибунал по преступлениям, совершенным в киберпространстве, для достижения мира и безопасности. Думается, что такой международный трибунал будет дублировать функции общепризнанного Международного уголовного суда в Гааге.

Кроме того, возникает ряд проблем политического, правового, процессуального и организационного характера, препятствующих деятельности такого судебного учреждения, например: вмешательство в информационное пространство суверенных государств и юрисдикцию национальных судов; различия в уголовном законодательстве зарубежных стран в части дифференциации ответственности за киберпреступления; отсутствие между государствами соответствующих многосторонних и

[1] Противодействие использованию информационно-коммуникационных технологий в преступных целях : резолюция принята Генеральной Ассамблеей ООН 27 дек. 2019 г., № 74/247 // КонсультантПлюс : справочная правовая система.

[2] ГА ООН приняла резолюцию России по разработке конвенции для борьбы с киберпреступлениями. URL: https://tass.ru/mezhdunarodnaya-panorama/7439717 (дата обращения: 17.01.2021).

двухсторонних соглашений о правовой помощи по уголовным делам, в том числе в части экстрадиции киберпреступников; нежелание ряда развитых стран признавать юрисдикцию данного международного суда и др.

Поэтому создание правовой основы и механизма межгосударственного сотрудничества в сфере противодействия киберпреступности под эгидой Организации Объединенных Наций, по мнению авторов, является более совершенной и эффективной формой борьбы с данным видом высокотехнологичной преступности. Оно значительно расширяет географию государств – участников международного взаимодействия в указанной сфере, а также предоставляет возможность получения квалифицированной правовой, информационной, организационно-технической и иной помощи в борьбе с киберпреступлениями не только технологически развитым странам Европы и Северной Америки, но и развивающимся странам Азии, Африки и Южной Америки.

СПИСОК ЛИТЕРАТУРЫ

1. Евдокимов К. Н. Особенности расследования преступлений в сфере компьютерной информации // Трансформация государства и права в условиях глобальной цифровизации общества : материалы Всероссийской научно-практической конференции (Иркутск, 26 октября 2019 г.). Иркутск, 2019. С. 123–128.

2. Ефремова М. А., Агапов П. В. Международно-правовые основы обеспечения информационной безопасности участников Содружества Независимых Государств // Юридическая наука и правоохранительная практика. 2015. № 1 (31). С. 176–183.

3. Криминология : учебник для вузов / О. С. Капинус [и др.] ; под общ. ред. О. С. Капинус. 2-е изд., перераб. и доп. М. : Юрайт, 2020. 1132 с.

4. Скляров С. В., Евдокимов К. Н. Проблемные вопросы международного сотрудничества России в сфере противодействия киберпреступности // Библиотека криминалиста. Научный журнал. 2017. № 4 (33). С. 269–275.

5. Тропина Т. Л. Борьба с киберпреступностью: возможна ли разработка универсального механизма? // Международное правосудие. 2012. № 3. С. 86–95.

6. Schjolberg S. Proposals for new legal mechanisms on combatting cybercrime and global cyberattacks. An International Criminal Court or Tribunal for Cyberspace (ICTC). URL: http://www.cybercrimelaw.net/documents/International_Criminal_Court_or_Tribunal_for_Cyberspace_(ICTC). pdf (дата обращения: 09.01.2022).

REFERENCES

1. Evdokimov K.N. Osobennosti rassledovaniya prestuplenii v sfere komp'yuternoi informatsii [Features of the investigation of crimes in the field of computer information] *Transformatsiya gosudarstva i prava v usloviyakh global'noi tsifrovizatsii obshchestva : materialy Vserossiiskoi nauchno-prakticheskoi konferentsii* (Irkutsk, 26 okt. 2019 g.) [Transformation of the state and law in the context of global digitalization of society: materials of the All-Russian Scientific and Practical Conference (Irkutsk, October 26, 2019)]. Irkutsk, 2019, pp. 123-128. (in Russian)

2. Efremova M.A., Agapov P.V. Mezhdunarodno-pravovye osnovy obespecheniya informatsionnoi bezopasnosti uchastnikov Sodruzhestva Nezavisimykh Gosudarstv. [International legal bases of ensuring information security of participants of the Commonwealth of Independent States]. *Yuridicheskaya nauka i pravookhranitel'naya praktika* [Legal science and law enforcement practice], 2015, no. 1 (31), pp. 176-183. (in Russian)

3. *Kriminologiya :* uchebnik dlya vuzov / O.S. Kapinus [i dr.] ; pod obshchei redaktsiei O.S. Kapinus. 2-e izd., pererab. i dop. [Criminology: textbook for universities. O.S. Kapinus [et al.]; under the general editorship of O. S. Kapinus. 2nd ed., reprint. and additional]. Moscow, 2020, 1132 p. (in Russian)

4. Sklyarov S.V., Evdokimov K.N. Problemnye voprosy mezhdunarodnogo sotrudnichestva Rossii v sfere protivodeistviya kiberprestupnosti [Problematic issues of Russia's international cooperation in countering cybercrime]. *Biblioteka kriminalista. Nauchnyi zhurnal* [Library of Criminalist. Scientific journal], 2017, no. 4 (33), pp. 269-275. (in Russian)

5. Tropina T.L. Bor'ba s kiberprestupnost'yu: vozmozhna li razrabotka universal'nogo mekhanizma? [Fighting cybercrime: is it possible to develop a universal mechanism?] *Mezhdunarodnoe pravosudie* [International justice], 2012, no. 3, pp. 86-95. (in Russian)

6. Schjolberg S. Proposals for new legal mechanisms on combatting cybercrime and global cyberattacks. An International Criminal Court or Tribunal for Cyberspace (ICTC). Available at: http://www.cybercrimelaw.net/documents/International_Criminal_Court_or_Tribunal_for_Cyberspace_(ICTC). pdf (date of access: 09.01.2022).

Статья поступила в редакцию 11.02.2022; одобрена после рецензирования 02.06.2022; принята к публикации 07.09.2022

Received on 11.02.2022; approved on 02.06.2022; accepted for publication on 07.09.2022

Евдокимов Константин Николаевич – кандидат юридических наук, доцент, доцент кафедры государственно-правовых дисциплин, Иркутский юридический институт (филиал) Университета прокуратуры Российской Федерации (Россия, 664035, г. Иркутск, ул. Шевцова, 1), ORCID: 0000-0002-7040-7039, Scopus Author ID: 56578347900, e-mail: kons-evdokimov@yandex.ru

Evdokimov Konstantin Nikolaevich – Candidate of Juridical Sciences, Associate Professor, Associate Professor of the Department of State and Legal Disciplines, Irkutsk Law Institute (branch) University of the Prosecutor's Office of the Russian Federation (1, Shevtsova st., Irkutsk, 664035, Russian Federation), ORCID: 0000-0002-7040-7039, Scopus Author ID: 56578347900, e-mail: kons-evdokimov@yandex.ru

Хобонкова Ксения Вадимовна – студентка 4-го курса, Институт экономики, управления и права, Иркутский национальный исследовательский технический университет (Россия, 664074, г. Иркутск, ул. Лермонтова, 83), e-mail: ksenia98h@yandex.ru

Hobonkova Ksenia Vadimovna – 4th year student, Institute of Economics, Management and Law, Irkutsk National Research Technical University (83, Lermontov st., Irkutsk, 664074, Russian Federation), e-mail: ksenia98h@yandex.ru