УДК 343 Вестник СПбГУ. Право. 2022. Т. 13. Вып. 3

Международное сотрудничество в борьбе с киберпреступностью в контексте противодействия новым вызовам и угрозам

К. К. Клевцов

Московский государственный институт международных отношений (университет)
Министерства иностранных дел Российской Федерации,
Российская Федерация, 119454, Москва, пр. Вернадского, 76

Для цитирования: Клевцов, Кирилл К. 2022. «Международное сотрудничество в борьбе с киберпреступностью в контексте противодействия новым вызовам и угрозам». *Вестник Санкт-Петербургского университета. Право* 3: 678–695. https://doi.org/10.21638/spbu14.2022.306

Статья посвящена исследованию уголовно-процессуальных и других организационно-правовых аспектов международного взаимодействия государств в борьбе с киберпреступностью в условиях противодействия новым вызовам и угрозам. Цель исследования состоит в выявлении и рассмотрении формальных и неформальных мер международного сотрудничества, предпринимаемых в ответ на проблему транснациональной киберпреступности. Продемонстрировано, что такие преступления, как правило, носят международный характер, поскольку имеют негативные последствия на территории других суверенов. Автор анализирует различные формы международного сотрудничества в борьбе с преступностью, которые включают выдачу (экстрадицию), правовую помощь по уголовным делам, передачу уголовного преследования (судопроизводства), а также неофициальное сотрудничество между правоохранительными органами (международное полицейское сотрудничество), в частности в рамках такого закона США, как CLOUD Act. В качестве эмпирической базы исследования использованы материалы российской оперативной и следственной практики за 2018–2019 гг. и решения судов иностранных государств. Делается вывод, что большинство правоохранительных органов при расследовании киберпреступлений умышленно или без умысла прибегают к практике получения доказательств, физически находящихся на территории других государств, самостоятельным путем, не получив на это согласие данных государств. Это происходит посредством дистанционного подключения в режиме реального времени к абонентскому устройству уголовно преследуемого лица или изъятия такого устройства у потерпевшего или свидетеля, находящегося на территории государства, правоохранительные органы которого ведут производство по делу о киберпреступлении, с последующим осмотром для отыскания информации, имеющей значение для дела, а также путем применения иных законных методов.

Ключевые слова: киберпреступность, международное сотрудничество, юрисдикция, электронная информация, поставщик услуг, правовая помощь.

1. Введение

При рассмотрении вопросов взаимодействия государств в целях противодействия киберпреступности[1] можно выделить два важных аспекта: 1) официальное

[1] В настоящей статье под основой киберпреступности понимается не только исчерпывающий круг деяний, направленных против конфиденциальности, целостности и доступности компьютер-

© Санкт-Петербургский государственный университет, 2022

международное сотрудничество, в том числе выдача (экстрадиция) и оказание взаимной правовой помощи; 2) неофициальное сотрудничество.

Правовой анализ международного сотрудничества и национального законодательства различных государств свидетельствует об отсутствии единой практики в борьбе с киберпреступностью (Broadhurst et al. 2014, 2), несмотря на наличие ряда многосторонних договоров по данному вопросу, что, разумеется, негативным образом сказывается на таком направлении деятельности государств[2]. Например, одной из самых распространенных проблем, связанных с осуществлением международного сотрудничества в борьбе с киберпреступностью, является установление уголовной юрисдикции конкретного государства на основе территориального (Grant 2019; Maillart 2019) и экстратерриториального принципов (Ferzan 2020; Megret 2020; Soler 2019), а также разрешение конфликтов юрисдикций между суверенами (Zając 2020; Ring 2021). К процессуальным трудностям также стоит отнести длительные сроки получения электронной информации, необходимой для расследования обозначенных выше преступлений, в рамках исполнения запроса об оказании правовой помощи.

В основном это связано с отсутствием в многосторонних и двусторонних документах обязательства предоставлять ответ в течение определенного срока (Жубрин 2018, 13)[3]. Эффективность сотрудничества в борьбе с киберпреступлениями снижается из-за использования традиционных механизмов взаимодействия правоохранительных органов и из-за отсутствия закрепленных в международных договорах и отечественном законодательстве положений, позволяющих осуществить прямой доступ к данным, располагающимся за рубежом.

2. Основное исследование

2.1. Официальное международное сотрудничество

Нормативные предписания о международном сотрудничестве предусмотрены в ряде соглашений по киберпреступности, поскольку последние имеют транснаци-

---

ных данных или систем, но и деяния, предполагающие использование компьютера в целях извлечения личной или финансовой прибыли или причинения личного или финансового вреда, в том числе преступления, касающиеся использования персональных данных, и деяния, связанные с содержанием компьютерных данных.

[2] Многие законодательные и правоприменительные проблемы, с которыми сталкиваются различные государства в борьбе с киберпреступностью, обобщены в докладе Генерального секретаря ООН на 74-й сессии Генеральной Ассамблеи ООН, озаглавленном «Противодействие использованию информационно-коммуникационных технологий в преступных целях». Дата обращения 1 мая, 2020. https://www.unodc.org/documents/Cybercrime/SG_report/V1908184_R.pdf.

[3] В некоторых государствах срок исполнения запроса о международном сотрудничестве в сфере уголовного судопроизводства регламентируется национальными правовыми документами. Например, в силу п. 1.1.2.1 Указания Генеральной прокуратуры РФ от 16.01.2020 № 23/35 Главным управлениям и управлениям Генеральной прокуратуры РФ, Главной военной прокуратуре, прокурорам субъектов РФ, приравненным к ним военным и иным специализированным прокурорам предписывается в пределах их компетенции обеспечивать исполнение иностранных запросов о правовой помощи *в течение 30 суток* с даты их поступления непосредственно исполнителю, если иной срок не установлен международным договором РФ или Главным управлением международно-правового сотрудничества (здесь и далее ссылки на нормативно-правовые и подзаконные акты, а также на судебную практику, если не указано иное, приводятся по СПС «КонсультантПлюс». Дата обращения 1 июля, 2022. http://www.consultant.ru).

ональный характер[4]. Такие международно-правовые документы в основном содержат положения о выдаче и правовой помощи. Например, Конвенция о преступности в сфере компьютерной информации от 23.11.2001[5] (далее — Конвенция Совета Европы о компьютерных преступлениях), Конвенция Лиги арабских государств о борьбе с преступлениями в области информационных технологий от 21.12.2010[6] (далее — Конвенция Лиги арабских государств) и Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 01.06.2001 предусматривают выдачу (экстрадицию) за совершение преступлений, указанных в данных актах, и оказание взаимной правовой помощи по уголовным делам.

При этом международно-правовые документы устанавливают возможность использования оперативных средств связи (электронная почта, факс) для направления запросов в целях незамедлительного реагирования в целях фиксации ситуации, связанной с совершенным киберпреступлением. Однако подобная возможность не исключает последующего направления оригинала запроса по официальным каналам почтовой связью (Кунев 2019, 166).

Правовой анализ национального законодательства различных иностранных государств позволяет отметить, что нормы большей частью регламентируют выдачу и оказание взаимной правовой помощи не по киберпреступлениям, а по общим уголовным преступлениям.

Задействование традиционных форм сотрудничества по киберпреступлениям не во всех случаях отвечает потребностям правоприменителей. При этом многие договоры, касающиеся сотрудничества в сфере уголовного судопроизводства, не содержат исчерпывающего перечня преступлений, по которым осуществляется выдача, за исключением политических и процессуальных действий, которые могут быть запрошены в рамках правовой помощи. Разумеется, это положительно сказывается на борьбе с киберпреступностью, поскольку открывает возможности запросить производство так называемых специальных действий (например, сохранения электронных данных).

Впрочем, некоторые государства не подписали и не ратифицировали многосторонние международные договоры в сфере борьбы с киберпреступностью. Не является исключением и Российская Федерация, также не ратифицировавшая

[4] Следует отличать *международные преступления* от *преступлений международного характера*, поскольку первые представляют собой наиболее опасные для человеческой цивилизации нарушения принципов и норм международного права. К ним относятся преступления против мира и человечности, военные преступления, геноцид, апартеид и др. Что же касается преступлений международного характера, то ими являются деяния, которые предусмотрены международным договором, но посягают на нормальные стабильные отношения между государствами. Стоит также отграничивать указанные понятия от *транснациональных преступлений*, которые представляют общеуголовные преступления, подпадающие под юрисдикцию двух или более государств (Волеводз 2014, 107–114). В связи с этим мы относим киберпреступления к преступлениям международного характера, поскольку они предусмотрены международными договорами, которые будут названы ниже.

[5] Convention on Cybercrime (ETS No. 185). Дата обращения 1 мая, 2020. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

[6] Arab Convention on Combating Information Technology Offences. Дата обращения 1 мая, 2020. https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf.

Конвенцию Совета Европы о компьютерных преступлениях[7], поэтому сегодня запросы, направленные в рамках международного сотрудничества в государства, не являющиеся участниками соответствующих соглашений, должны направляться в рамках традиционных двусторонних соглашений или на основании принципа взаимности (reciprocity principle)[8]. Содержание принципа взаимности также разъясняется в некоторых судебных актах[9].

Некоторые государства взаимодействуют только на основании заключенного между суверенами международного договора, а принцип взаимности, как правило, не признают. К таким странам стоит отнести в первую очередь США, особенно в том, что касается вопросов выдачи (экстрадиции) (Bassiouni 2014, 102–115).

Обобщение правоприменительной практики также свидетельствует о том, что при направлении запросов по уголовным делам о киберпреступлениях с целью обеспечения сохранности данных не учитываются некоторые особенности, которые могут повлечь в дальнейшем отказ в исполнении таких запросов или их отправление на доработку в запрашивающее государство. К таким особенностям относятся следующие: 1) отсутствие в запросе описания конкретного действия, которое следует провести правоохранительным органам запрашиваемого государства; 2) указание в запросе на принятие мер, не предусмотренных ни международным договором, ни национальным законодательством запрашиваемого государства; 3) отсутствие в направленном запросе детального обоснования взаимосвязи (причинно-следственной связи) между деянием и запрошенного процессуального действия; 4) непредоставление в запросе о получении конфиденциальной информации решений суда запрашивающего государства или отсутствие доказательств, обосновывающих необходимость получения таких данных, и др.

2.1.1. Условия международного сотрудничества по уголовным делам о киберпреступлениях

Одним из ключевых условий международного сотрудничества выступает принцип двойной криминальности (double criminality), суть которого заключается в том, что общественно опасное деяние, указанное в запросе о выдаче либо о взаимно-правовой помощи, является уголовно наказуемым как в запрашивающем, так

---

[7] «Российский дипломат назвал Будапештскую конвенцию по киберпреступлениям устаревшей». *ТАСС*. 04.12.2017. Дата обращения 1 мая, 2020. https://tass.ru/politika/4782506. — При этом Российская Федерация входит в топ-20 государств, пострадавших от киберпреступлений и занимает 11-е место в этом списке (Internet Crime Report 2018 of Federal Bureau Investigations — Internet Crime Complaint Center. Washington, 2018. P. 17).

[8] Данный принцип напрямую не раскрывается ни действующими международными договорами, ни российским уголовно-процессуальным законодательством. Взаимность подтверждается письменным обязательством одного государства оказать необходимую помощь по расследуемому или рассматриваемому уголовному делу другому государству (ст. 453, 457, 462, 469 Уголовно-процессуального кодекса РФ от 18.12.2001 № 174-ФЗ (УПК РФ)) и заключается в том, что в случае исполнения иностранным государством поручения об осуществлении уголовного преследования на основе взаимности Российская Федерация в аналогичной ситуации осуществит такие же действия (Щерба 2016).

[9] См., напр.: Постановление Пленума Верховного Суда РФ от 14.06.2012 № 11 «О практике рассмотрения судами вопросов, связанных с выдачей лиц для уголовного преследования или исполнения приговора, а также передачей лиц для отбывания наказания».

и в запрашиваемом государстве; данный принцип содействует формированию единообразного подхода при осуществлении международного сотрудничества в сфере уголовного судопроизводства (Plachta 1989, 107).

Так, некоторые государства могут отказать в исполнении запроса об оказании правовой помощи по уголовным делам о преступлениях в сфере информационных технологий, оценив их как политическое преступление или указав на несоблюдение международных обязательств в области прав человека (Currie 2000).

Однако при сотрудничестве государств — участников ЕС данный принцип действует рестриктивно, особенно при использовании таких правовых институтов, как европейский ордер на арест и на производство следственных действий (Vermeulen, De Bondt, Ryckman 2012, 111–115).

2.1.2. Практика реализации института выдачи (экстрадиции) и правовой помощи по уголовным делам о киберпреступлениях

Юридический анализ запросов об оказании правовой помощи по уголовным делам о киберпреступлениях наглядно свидетельствует о том, что они в большей степени касаются предоставления информации о базовой информации абонента (basic subscriber information), транзакциях (transactional information) и о содержании переписки (content) между абонентами, а также производства обыска или выемки компьютерных устройств.

Так, в Кратком руководстве по получению взаимной правовой помощи от США, подготовленном отделом по международным делам Управления по уголовным делам Министерства юстиции США[10], раскрываются следующие виды помощи, которые могут быть предоставлены американскими правоохранительными органами другим государствам в данной сфере: 1) обеспечение сохранения хранимых данных; 2) получение журналов подключений, информации об абоненте и содержании более старых хранимых сообщений электронной почты от поставщиков услуг интернета; 3) исполнение ордера на получение содержания новых хранимых сообщений электронной почты от поставщиков услуг интернета; 4) перехват телекоммуникаций или компьютерных данных в реальном времени.

В национальном законодательстве большинства государств отсутствуют нормы, подробно регламентирующие указанные выше действия, поэтому только некоторые из них сообщили о возможности проведения таких специализированных действий на своей территории на основе традиционного механизма взаимодействия — взаимной правовой помощи.

Одной из самых главных проблем остается длительность сроков исполнения запросов об оказании правовой помощи. Например, общий срок рассмотрения и исполнения запросов о правовой помощи по уголовным делам, направляемых компетентными органами РФ в иностранные государства, составляет от 3 до 12 месяцев и более (Волеводз 2016). Зачастую срок исполнения запросов об оказании правовой помощи исключительно по уголовным делам о киберпреступлениях за-

[10] "Brief guide to obtaining mutual legal assistance from the United States". *Office of International Affairs, Criminal Division, U. S. Dept. of Justice.* 03.08.2011. (Источник: архив автора, ведомственный документ, передан через посольство)

нимает 120 дней, а по запросам о выдаче — 150 дней[11]. Механизмы официального сотрудничества, как правило, требуют определения «центрального органа» (Шаталов 2015, 128), который отвечает за обработку входящих и исходящих запросов по обычной или дипломатической почте[12].

Подчеркнем, что информация, предоставляемая в электронном виде, является непостоянной, поскольку имеет определенные сроки «существования», поэтому официальные механизмы международного взаимодействия (оказания правовой помощи и выдачи) могут потребовать много времени и, следовательно, негативно отразиться на досудебном производстве по уголовным делам о киберпреступлениях. Впрочем, как отмечено выше, некоторые международные соглашения и внутригосударственные законы в определенных ситуациях позволяют использовать оперативные средства связи в целях сокращения сроков исполнения запросов о международном сотрудничестве и получения информации, являющейся по своей природе неустойчивой.

2.2. Неофициальное сотрудничество по уголовным делам о киберпреступлениях

Помимо механизмов официального сотрудничества, многие государства осуществляют так называемое международное полицейское сотрудничество (law enforcement, police-to-police cooperation (enquiries)) в рамках заключенных международных соглашений межведомственного характера, которое, в свою очередь, позволяет оптимизировать расследование уголовных дел о преступлениях в сфере киберпространства.

Подобное сотрудничество используется до направления официального запроса об оказании правовой помощи в иностранное государство или для оказания содействия официальному запросу. Такая форма сношений предусмотрена в ряде международных договоров, а именно в Конвенции Совета Европы о компьютерных преступлениях и Конвенции Лиги арабских государств.

Неформальное сотрудничество осуществляется в основном посредством прямых связей между правоохранительными органами, в том числе через каналы Интерпола и Европола. В ряде договоров по киберпреступлениям предусмотрено нормативное предписание относительно обязанности государств-участников создать «специализированный контактный центр» при органах национальной полиции, который призван обеспечить предоставление оперативной информации в осу-

[11] Comprehensive Study on Cybercrime (Draft-February 2013). *United Nations Office on Drugs and Crime (UNODC)*. New York, 2013. P. 230. Дата обращения 1 мая, 2020. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

[12] Например, Российская Федерация в рамках взаимодействия с государствами — членами Совета Европы (Страсбург, 20 апреля 1959 г.) ратифицировала Второй Дополнительный протокол к Европейской конвенции о взаимной правовой помощи по уголовным делам от 08.11.2001. Так, Федеральным законом от 06.06.2019 № 120-ФЗ «О ратификации Второго дополнительного протокола к Европейской конвенции о взаимной правовой помощи по уголовным делам» установлены условия прямого сотрудничества российских органов, осуществляющих предварительное следствие, дознание и оперативно-разыскную деятельность, с зарубежными партнерами (Информационное письмо Генеральной прокуратуры РФ от 30.12.2019 № Инф-90-14629-19 «О Втором дополнительном протоколе к Европейской конвенции о взаимной правовой помощи по уголовным делам»).

ществлении уголовного преследования, связанного с компьютерными технологиями, и в сборе информации, предоставляемой в электронном виде[13].

Многие государства, предусматривающие в своем национальном законодательстве использование механизмов неофициального сотрудничества, отмечают, что такие инструменты, как правило, применяются должным образом на основе международных договоров в рамках сетей, которые приветствуются международными организациями (например, Интерпол, Европол и Евроюст) и дипломатическими (консульскими) должностными лицами, а также офицерами связи.

Неофициальный канал взаимодействия обычно позволяет в рамках межправительственных и межведомственных договоров решать общие технические и юридические вопросы посредством консультаций, организованных между правоохранительными органами в целях оптимизирования в дальнейшем официальных действий, но такое сотрудничество не направлено на сбор доказательств, имеющих уголовно-процессуальную подоплеку (Литвишко 2015).

В то же время круглосуточные специализированные контактные центры чаще всего предоставляют запрошенную информацию в течение нескольких дней, что свидетельствует об эффективности использования механизма международного полицейского сотрудничества. Обобщение правоприменительной практики показывает, что неофициальное сотрудничество используется для предоставления идентификационной или абонентской информации, а также в целях оперативного обеспечения сохранности электронных данных и данных о трафике (Малов, 2018).

Многие государства признают, что фактические данные, полученные на основе неофициального взаимодействия, не могут рассматриваться в качестве доказательств в суде. При этом в российской практике и юридической литературе указывается, что с учетом конкретных обстоятельств данные сведения могут быть использованы в качестве доказательств при соблюдении всех требований, предъявляемых к доказательствам УПК РФ, в частности: 1) посредством исполнения запросов о содействии в рамках межправительственных и межведомственных соглашений; 2) посредством предоставления информации через Национальное центральное бюро Интерпола МВД России, Бюро по координации борьбы с организованной преступностью и иными видами преступлений на территории государств — участников СНГ; 3) через каналы офицеров связи правоохранительных органов иностранных государств, аккредитованных при загранучреждениях; 4) через Росфинмониторинг от органов финансовой разведки иностранных государств; 5) путем предоставления сведений должностными лицами дипломатических и консульских учреждений МИД России; 6) через получение непосредственно от находящегося за рубежом физического или юридического лица добровольно переданных по электронной или почтовой связи сведений или предметов должностному

[13] Например, в ст. 35 Конвенции Совета Европы о компьютерных преступлениях постулируется, что каждое государство — участник данного международно-правового документа должно назначить контактный центр, работающий 24 часа в сутки семь дней в неделю, чтобы обеспечить оказание неотложной помощи в целях расследований или судебных разбирательств уголовных преступлений, имеющих отношение к компьютерным системам и данным, или в целях сбора доказательств в электронной форме по уголовным преступлениям. Такая помощь включает содействие или, если это допускается внутригосударственным правом либо практикой, непосредственное применение следующих мер: 1) оказания технической консультативной помощи; 2) обеспечения сохранности данных; 3) сбора доказательств, предоставления законной информации и установления места нахождения подозреваемых лиц.

лицу, в производстве которого находится уголовное дело или материал проверки (ст. 144 УПК РФ) (Литвишко 2011, 15).

Практика США, касающаяся использования механизмов неофициального сотрудничества по уголовным делам о киберпреступлениях, довольно интересна. Например, американские правоохранительные органы зачастую используют так называемые тактические операции по выманиванию[14], или «приманки»[15], а вместо традиционной экстрадиции используется ее альтернатива — депортация (высылка, принудительная рендиция) в рамках административных процедур, предоставляющая совсем другой уровень гарантий, нежели выдача лиц в уголовно-процессуальном порядке (Клевцов 2018, 86; Нурбеков 2011, 128).

В связи с этим многообразие видов неофициального сотрудничества и расхождение их в международно-правовых документах и национальном законодательстве государств свидетельствуют о трудностях, которые могут возникнуть у правоохранительных органов при расследовании транснациональных киберпреступлений.

2.3. Предоставление поставщиками услуг электронной информации, находящейся за рубежом

В ходе осуществления международного сотрудничества в борьбе с киберпреступлениями власти, помимо тех проблем, о которых сказано выше (длительные сроки исполнения запросов, различие в национальном законодательстве относительно получения электронной информации), сталкиваются с особенностью, заслуживающей самостоятельного изучения, — проблемой установления поставщика услуг, которому следует направить запрос о правовой помощи или о содействии в рамках неофициального сотрудничества.

Такая сложность возникает в силу дифференциации географического расположения серверов и центров обработки данных, в частности облачных услуг. Зачастую физическое оборудование, которое предоставляет облачные услуги, «находится в местах для обработки данных, стратегически расположенных для минимизации задержек в предоставлении таких услуг, а также затрат на электроэнергию и охлаждение оборудования»[16]. Например, Google может предоставлять своим

[14] В Кратком руководстве для прокуроров США указано, что, если невозможно добиться экстрадиции уголовно преследуемого лица (такие причины обязательно должны быть задокументированы), необходимо использовать альтернативу выдачи, а точнее, предпринять другие действия, которые могут вернуть такое лицо в США или ограничить его способность существовать и путешествовать за рубежом (U.S. Attorneys Manual 9-15.100, 9-15.630. Дата обращения 1 мая, 2020. https://www.justice.gov/jm/jm-9-15000-international-extradition-and-related-matters).

[15] В США принято использовать «приманки», или «наживки» (lures), чтобы побудить обвиняемого покинуть государство, на территории которого он находится, для дальнейшего задержания в США, в открытом море, воздушном пространстве или в третьей стране. Однако, прежде чем использовать такую приманку, следует проконсультироваться с Управлением по международным делам США, поскольку некоторые государства могут расценить подобные действия как посягательство на их суверенитет. «Наживки» могут представлять собой сложные схемы или быть столь же простыми, как приглашение беглеца по телефону на вечеринку в Америку (U. S. Attorneys Manual 9-15.630. Дата обращения 1 мая, 2020. https://www.justice.gov/jm/jm-9-15000-international-extradition-and-related-matters 9-15.220).

[16] "Comprehensive study on cybercrime (Draft — February 2013)". *United Nations Office on Drugs and Crime (UNODC).* New York, 2013. P. 241. Дата обращения 1 мая, 2020. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

пользователям доступ к сведениям, которые находятся и обрабатываются в Северной Америке, Юго-Восточной Азии, Северной или Западной Европе[17].

В правоприменительной практике иногда сложно или почти невозможно оперативно установить, где физически располагаются облачные данные, поскольку они могут находиться одновременно в нескольких местах (государствах), являющихся центрами обработки данных или их копий. В качестве примера приведем следующее уголовное дело.

> В рамках производства по уголовному делу по признакам преступления, предусмотренного ч. 4 ст. 159[6] Уголовного кодекса РФ от 13.06.1996 № 63-ФЗ, возникла необходимость в получении сведений об учетных и иных сохраненных данных, об IP-адресах, с которых производилась регистрация электронной почты «k*****@gmail.com», об идентификаторе устройства, о сетевых картах и других возможных технических реквизитах компьютера, с которого осуществлялся вход в интернет. В результате следователь Следственного департамента Министерства внутренних дел РФ, в производстве которого находилось данное уголовное дело, направил вместе с санкцией суда запрос о предоставлении указанных выше данных в ООО «Гугл», от которого был в дальнейшем получен письменный ответ следующего содержания: «Данное общество не имеет возможности предоставить запрошенные сведения, поскольку оно не является владельцем сервиса Gmail, не имеет доступа к этому сервису, не ведет его техническую поддержку и администрирование, а также не является и владельцем доменного имени gmail.com, поскольку находится в распоряжении иностранной компании "Google LLC" (США)»[18].

Следовательно, центры обработки, имеющие систему облачных вычислений, могут физически располагаться на территориях нескольких государствах (Peterson, Gondree, Beverly 2011, 1–5). Вместе с тем договорные отношения между такими поставщиками услуг и их пользователями не всегда определяют месторасположение центра обработки данных (Benson, Dowsley, Shacham 2011).

Впрочем, некоторые поставщики услуг все же предоставляют право пользователям выбрать конкретную страну, в которой будут храниться и обрабатываться электронные данные, а в случае изменения «местонахождения первоначальных данных» провайдер должен проинформировать об этом пользователей. На начальном этапе досудебного производства по уголовным делам о киберпреступлениях, как правило, отсутствует техническая возможность определить местонахождение интересующей правоохранительные органы информации.

Даже при первоначальном установлении местонахождения центра обработки данных власти могут столкнуться с тем, что этот центр является «транзитным» по отношению к данным, а следовательно, не имеющим прямого доступа к ним. При определении местонахождения данных органы предварительного расследования обычно ориентируются на официальное именование поставщика услуг[19].

---

[17] Discover our data center locations. Дата обращения 1 мая, 2020. http://www.google.com/about/datacenters/inside/locations/index.html.

[18] Источник: Архив автора.

[19] В результате авторского социологического исследования, в ходе которого были проинтервьюированы 69 следователей различных подразделений Следственного комитета (58 респондентов) и Следственного департамента МВД (11 респондентов), получены следующие данные: 62 респон-

Для установления местонахождения центра обработки данных облачных услуг должностное лицо, в производстве которого находится уголовное дело о киберпреступлении, направляет запрос об оказании правовой помощи по уголовным делам, используя тем самым традиционный механизм сотрудничества. В первую очередь это вытекает из требований, закрепленных в национальном законодательстве, и корпоративных правил самих поставщиков услуг.

Например, в Руководящих принципах Facebook* отмечается, что для раскрытия иностранным органам следствия информации об учетной записи в их аккаунте следует направлять запрос в рамках официального сотрудничества. При этом, несмотря на то что центр обработки данных пользователей Facebook* физически расположен в одном из государств Северной Европы, он все же предоставляет данные в соответствии с законами США[20]. Однако согласно § 2703(d) разд. 18 Свода закона США[21] местным правоохранительным органам необходимо получить судебное решение (распоряжение D), которое выдается, если американский суд убедится в наличии конкретных и поддающихся описанию фактов, демонстрирующих, что имеются разумные основания считать информацию значимой для текущего расследования. Следовательно, такие данные в полной мере контролируются тем государством, которое юридически обладает ими, а не страной, где физически располагается центр обработки данных (Sieber 2012, 112).

Более того, прежде чем делать официальный запрос правоохранительным органам, рекомендуется через круглосуточную сеть организовать сохранение данных, требуемых от поставщика услуг, находящегося за рубежом. Например, в США поставщики услуг сохраняют электронные данные или записи в течение 90 дней, при необходимости это время может быть продлено, но предварительно рекомендуется обеспечить сохранение данных как можно скорее через круглосуточную сеть, а затем уже приступить к направлению официального запроса об оказании правовой помощи[22]. В связи с этим официальная процедура получения сведений, предоставляемых в электронном виде, от поставщиков услуг, которые располагаются в другом государстве, слишком трудоемка и длительна, вследствие чего отрицательно сказывается на досудебном производстве по уголовным делам о киберпреступлениях.

После принятия в 2018 г. в США CLOUD Act — Clarifying Lawful Overseas Use of Data Act (далее — Закон об облачности) правоохранительные органы Америки могут иметь прямой доступ к электронным данным, которые американские компании хранят на зарубежных серверах (Schomburg, Lagodny 2020, 53; Abraha 2020; Galbraith 2018). Иными словами, полиция или Федеральное бюро расследований

дента указали, что при установлении местонахождения центра обработки данных, имеющих значение для уголовного дела о киберпреступлениях, они руководствуются местонахождением головного офиса поставщика услуг, который такими данными юридически обладает; 7 респондентов опираются на местонахождение ближайшего официального представительства поставщика услуг.

* Meta признана экстремистской организацией в РФ.

[20] Информация для правоохранительных органов. Дата обращения 1 мая, 2020. https://www.facebook.com/safety/groups/law/guidelines. Meta признана экстремистской организацией в РФ.

[21] 18 U. S. C. Title 18 — Crimes and Criminal Procedure. 1948. Дата обращения 1 мая, 2020. https://www.govinfo.gov/content/pkg/USCODE-2018-title18/pdf/USCODE-2018-title18.pdf.

[22] Российско-Американские встречи по сотрудничеству в сфере борьбы с киберпреступностью (16 и 17 декабря 2010 г.): сб. материалов отдела по международным делам Управления по уголовным делам Министерства юстиции США. С. 3 (источник: архив автора, получено через посольство).

вправе обязать Google или Facebook* предоставить данные их пользователей, если они физически хранятся, например, в Европе. Поэтому сегодня такие компании не смогут отказать в предоставлении электронной информации, даже если это запрещено законодательством другого государства, как было ранее в судебной практике США[23]. Кроме того, существуют различные криминалистические хитрости, позволяющие принудить интернет-провайдеров предоставить интересующую правоохранительные органы информацию (Goldfoot 2011).

Проблемы получения и использования экстратерриториальных данных муссируются учеными и практиками долгое время, о чем, в частности, свидетельствуют рабочие встречи по подготовке проекта Конвенции Совета Европы о компьютерных преступлениях.

Так, в силу ст. 32 («Трансграничный доступ к хранящимся компьютерным данным с соответствующего согласия или к общедоступным данным») Конвенции Совета Европы о компьютерных преступлениях государства-участники могут без согласия другого государства-участника: a) получать доступ к общедоступным (открытому источнику) компьютерным данным независимо от их географического местоположения; b) получать через компьютерную систему на своей территории доступ к хранящимся на территории другого государства компьютерным данным или получать их, если это государство имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные государству через такую компьютерную систему.

Правовой анализ указанной статьи позволяет заключить, что доступ одного государства к компьютерным данным, находящимся на территории другого суверена, возможен в одностороннем порядке без направления официального запроса об оказании правовой помощи по уголовным делам и без предварительного и последующего уведомления этого государства. Очевидно, что такая международная правовая норма не совсем согласуется с принципом суверенитета и невмешательства во внутренние дела государства, на территории которого находятся интересующие другую сторону электронные данные.

На данное положение можно посмотреть под иным углом зрения, например в контексте предварительного уведомления государств о планируемых или проведенных действиях, связанных с односторонним получением данных, находящихся на территории другого государства.

Немалым преимуществом ст. 32 Конвенции Совета Европы о компьютерных преступлениях является то, что она позволяет правоохранительным органам получать необходимые данные при получении законного и добровольного согласия владельца информации.

В оперативно-разыскной и следственной практике сегодня в большей степени задействуются официальные каналы получения сведений, имеющих значение для уголовных дел о киберпреступлениях.

---

[23] Microsoft Cooperation v. United States, 829 F. 3d 197 (2nd Cir. 2016). Дата обращения 1 мая, 2020. https://casetext.com/case/microsoft-corp-v-united-states-in-re-a-warrant-to-search-a-certain-en-dashmail-account-controlled-maintained-by-microsoft-corp; United States v. Microsoft Cooperation, 584 U. S. 138 S. Ct. 1186 (2nd Cir 2018). Дата обращения 1 мая, 2020. https://casetext.com/case/united-states-v-microsoft-corp-9.

* Meta признана экстремистской организацией в РФ.

2.4. Концептуализация прямого доступа к информационным данным, находящимся за рубежом

В целях наиболее комплексного и системного рассмотрения вопросов, связанных с получением доступа к экстратерриториальным данным без обращения к официальным механизмам международно-правовой помощи по уголовным делам, предлагаем рассмотреть условную ситуацию: 1) США выступают поставщиком услуг с центральным офисом и центрами обработки данных; 2) Северная Ирландия является дополнительным центром обработки данных; 3) в Российской Федерации имеется представительство данного поставщика услуг; 4) сторона обвинения в России желает получить электронные сообщения, находящиеся в ведении поставщика услуг, центральный офис которого официально зарегистрирован в США.

Полагаем, здесь возможны следующие варианты:

— потерпевший или иное лицо, находящееся в России, имеет законный доступ к таким данным; доступ к ним возможен на основании разрешения этого лица (например, в смартфоне потерпевшего содержится переписка с обвиняемым), либо правоохранительные органы использовали связь с предоставленного законным владельцем устройства в режиме реального времени;
— владелец устройства, на котором содержатся необходимые данные, находится в США; соответственно, электронные сообщения могут быть получены с его разрешения;
— поставщик услуг, расположенный в США, самостоятельным путем предоставляет информацию, интересующую органы следствия;
— дополнительный офис в России также может предоставить местным правоохранительным органам необходимую информацию (если к ней имеется доступ), руководствуясь неформальными договоренностями;
— дополнительный центр обработки данных в Северной Ирландии может направить в рамках как официального, так и неофициального сотрудничества данные или их копии.

Возможный вектор развития ситуации свидетельствует об организационных трудностях получения прямого доступа к данным, находящимся за рубежом. При этом органы, осуществляющие уголовное преследование, также способны предпринять попытку получить доступ к данным без разрешения лица или поставщика услуг, используя различные оперативно-разыскные комбинации или криминалистические хитрости с применением специально-технических средств (электронного досмотра, оперативно-технического опроса и др.).

Проведенное обобщение следственной практики явно указывает на то, что почти все поставщики услуг обязуются раскрыть информацию только после предоставления судебного решения, приложенного к запросу об оказании правовой помощи по уголовным делам[24], вследствие чего такие компании не реагируют

[24] Practical Guide for Requesting Electronic Evidence Across Borders. United Nations Office on Drugs and Crime (UNODC); United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED); International Association of Prosecutors (IAP); EuroMed Justice; EuroMed Police.

должным образом на запросы, направляемые в рамках неофициального взаимодействия (в том числе через каналы Интерпола), за исключением ситуаций направления просьб в рамках полицейского сотрудничества о принятии мер по обеспечению сохранности электронных данных до направления официального запроса об оказании правовой помощи. Например, социальная сеть Twitter указывает, что она предоставляет иностранным правоохранительным органам данные о пользователях только при наличии судебного решения и запроса об оказании правовой помощи, направленного в рамках международного договора[25]. Следовательно, получив данные от поставщика услуг, находящегося за рубежом, на основе его прямого согласия, российские правоохранительные органы будут испытывать сложности с проверкой таких сведений на соответствие требованиям ст. 455 УПК РФ.

3. Выводы

Киберпреступления являются транснациональными, если какой-либо элемент состава преступления или последствия имеются на территории другого государства, что неизбежно затрагивает вопросы суверенитета государств и международного взаимодействия.

Принимая во внимание неустойчивый характер электронной информации, государствам следует оптимизировать международное сотрудничество в сфере уголовного судопроизводства в области киберпреступности, регламентировав на национальном уровне своевременное предоставление ответов на запросы об оказании правовой помощи, поскольку в ходе досудебного производства по указанной категории уголовных дел превалируют традиционные механизмы сотрудничества в рамках многосторонних или двусторонних договоров либо на основе принципа взаимности.

При расследовании компьютерных преступлений некоторые государства прибегают к различным видам неофициального сотрудничества, осознавая, в свою очередь, ограниченность такого механизма. Декларативно также закреплено определенное количество сетей неофициального взаимодействия по борьбе с киберпреступлениями, позволяющих оптимизировать сроки получения необходимой информации до нескольких дней, а в исключительных случаях и пары часов. В результате особую актуальность приобрели такие каналы международного полицейского сотрудничества, как Интерпол, Европол и Евроюст.

Вследствие появления облачных технологий и из-за непостоянного характера электронной информации на практике возникают сложности в установлении местонахождения центра обработки данных и оперативного их получения правоохранительными органами, поэтому традиционные механизмы сотрудничества в области правовой помощи теряют актуальность. В связи с этим органы, осуществляющие уголовное преследование, зачастую используют альтернативные варианты получения необходимой им экстратерриториальной информации (подключение с помощью специальных технических средств к устройству в режиме ре-

New York, 2019. P. 60–137. Дата обращения 1 мая, 2020. https://sherloc.unodc.org/cld/en/st/evidence/practical-guide.html.

[25] Рекомендации для правоохранительных органов. Дата обращения 1 мая, 2020. https://help.twitter.com/ru/rules-and-policies/twitter-law-enforcement-support.

ального времени, изъятие иного устройства на котором такая информация может храниться, с последующим его осмотром и др.) без согласия другого государства, на территории которого указанные данные физически находятся. В редких случаях, как показывает практика, сотрудники правоохранительных органов могут получить электронные данные напрямую от поставщиков услуг, находящихся за рубежом.

Проблемы, возникающие в процессе расследования киберпреступлений, требуют кардинального пересмотра с учетом текущих реалий и технических аспектов данной сферы. Полагаем, вариантами их решения станут создание общих правовых стандартов и выработка соответствующего уровня гарантий, обеспечивающих баланс реализации публичных и защиты частных интересов.

Одним из способов оптимизации международного сотрудничества в борьбе с киберпреступностью автор настоящей статьи видит унификацию правил работы правоохранительных органов в данной сфере. Кратко опишем эту унификацию.

Установление уголовной юрисдикции ↔ направление запроса иностранным поставщикам услуг связи: 1) прямой контакт с провайдером (официальный запрос, направленный на адрес электронной почты компании); 2) неофициальное сотрудничество (через каналы Интерпола, Европола или в рамках оперативно-разыскной деятельности в целях предварительного сохранения данных); ↔ *официальное международное сотрудничество*: 1) направление запроса в рамках взаимной правовой помощи для сбора доказательственной базы (экстратерриториальной электронной информации); 2) выдача лица, обвиняемого в совершении киберпреступления; 3) передача уголовного преследования (судопроизводства) в государство, где находится обвиняемый; 4) заочное уголовное судопроизводство.

Предложенная схема международного сотрудничества в борьбе с киберпреступностью — предмет научных дискуссий. Однако она представляется необходимой в целях оптимизации данного направления деятельности.

Библиография

Волеводз, Александр Г. 2014. *Международное уголовное правосудие и права человека*. М.: Российский университет дружбы народов.

Волеводз, Александр Г. 2016. «Некоторые аспекты планирования расследования при международном сотрудничестве в сфере уголовного судопроизводства». *Уголовное судопроизводство* 3: 26–33.

Жубрин, Роман В. 2018. «Сроки исполнения запросов о правовой помощи по уголовным делам». *Законность* 5: 12–14.

Клевцов, Кирилл К. 2018. *Досудебное производство в отношении лиц, уклоняющихся от уголовной ответственности за пределами территории Российской Федерации*. М.: Юрлитинформ.

Кунев, Денис А. 2019. Противодействие перемещению преступных активов за рубеж и их возврата в Российскую Федерацию: уголовно-процессуальные аспекты. Дис. … канд. юрид. наук, Московский государственный институт международных отношений (университет) МИД РФ.

Литвишко, Петр А. 2011. «Вопросы процессуальной самостоятельности органов предварительного расследования Российской Федерации при осуществлении международного сотрудничества». *Российский следователь* 18: 13–18.

Литвишко, Петр А. 2015. «Интеграция предварительного расследования и оперативно-розыскной деятельности: иностранный и международный опыт». *Библиотека криминалиста. Научный журнал* 3: 309–319.

Малов, Александр. 2018. «Получение электронных доказательств от иностранных юрисдикций (на примере США)». *Законность* 9: 56–60.

Нурбеков, Искендер М. 2011. «Криминалистические аспекты взаимодействия с иностранными компетентными органами при расследовании преступлений международного характера». *Библиотека криминалиста. Научный журнал* 1: 117–129.

Шаталов, Александр С. 2015. «Правовой механизм сотрудничества в сфере уголовного судопроизводства». *Право. Журнал Высшей школы экономики* 1: 126–149.

Щерба, Сергей П. 2016. «Международное сотрудничество России в сфере выдачи для уголовного преследования на основе принципа взаимности». *Международное уголовное право и международная юстиция* 4: 3–8.

Abraha, Halefom. 2020. "Regulating law enforcement access to electronic evidence across borders: The United States approach". *Information & Communications Technology Law* 29: 1–30.

Bassiouni, Cherif M. 2014. International extradition: United States law and practice. 6th rev. ed. New York: Oxford University Press.

Benson, Karyn, Rafael Dowsley, Hovav Shacham. 2011. "Do you know where cloud files are?" *Proceedings of the 3rd ACM Workshop on Cloud Computing Security*: 73–82. New York: Association for Computing Machinery.

Broadhurst, Roderic, Peter Grabosky, Mamoun Alazab, Steve Chon. 2014. "Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime". *International of Journal of Cyber Criminology* 8 (1): 1–20.

Currie, Robert J. 2000. "Human rights and international mutual legal assistance: Resolving the tension". *Criminal Law Forum* 11 (2): 143–181.

Ferzan, Kimberly. 2020. "The reach of the realm. Criminal law". *Philosophy* 14: 335–345. https://doi.org/10.1007/s11572-020-09541-w.

Galbraith, Jean. 2018. "Congress enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, reshaping U. S. law governing cross-border access to data". *American Journal of International Law* 112 (3): 486–493. https://doi.org/10.1017/ajil.2018.61.

Goldfoot, Josh. 2011. "Compelling online providers to produce evidence under ECPA". *The United States Attorneys Bulletin (Obtaining and Admitting Electronic Evidence)* 59 (6): 35–41.

Grant, Christensen. 2019. "The extraterritorial reach of Tribal Court criminal jurisdiction". *Hastings Constitutional Law Quarterly* 46 (294): 1–18. http://dx.doi.org/10.2139/ssrn.3231533.

Maillart, Jean-Baptiste. 2019. "The limits of subjective territorial jurisdiction in the context of cybercrime". *ERA Forum* 19: 375–390. https://doi.org/10.1007/s12027-018-0527-2.

Megret, Frederic. 2020. "Do not do abroad what you would not do at home?: An exploration of the rationales for extraterritorial criminal jurisdiction over a state's nationals". *Canadian Yearbook of International Law / Annuaire canadien de droit international* 57: 1–40.

Peterson, Zachary N. J., Mark Gondree, Robert Beverly. 2011. "A position on data sovereignty: The importance of geolocating data in the cloud". *HotCloud: Proceedings of the 3rd USENIX conference of Hot topic in Cloud computing. ResearchGate*. Дата обращения 1 мая, 2020. https://www.researchgate.net/publication/236626434_A_Position_Paper_on_Data_Sovereignty_The_Importance_of_Geolocating_Data_in_the_Cloud.pdf.

Plachta, Michal. 1989. "The role of double criminality in international cooperation in penal matters". *Double Criminality Studies in International Criminal Law.* Ed. by Nils Jareborg, 84–134. Uppsala: Iustus Forlag.

Ring, Tim. 2021. "Europol: The Al hacker threat to biometrics". *Biometric Technology Today* 2: 9–11.

Schomburg, Wolfgang, Otto Lagodny. 2020. *Internationale Rechtshilfe in Strafsachen (International Cooperation in Criminal Matters)*. Kommentar. 6., vollig neu bearbeitete Auflage. Munchen: C. H. Beck.

Sieber, Ulrich. 2012. *Straftaten und Strafverfolgung im Internet. Gutachten C zum 69. Deutschen Juristentag.* Munich: C. H. Beck.

Soler, Christopher. 2019. "Aut dedere aut judicare". *The global prosecution of core crimes under international law*, 319–401. The Hague: T. M. C., Asser Press. https://doi.org/10.1007/978-94-6265-335-1_13.

Vermeulen, Gert, Wendy De Bondt, Charlotte Ryckman, eds. 2012. *Rethinking international cooperation in criminal matters in the EU. Moving beyond actors, bringing logic back, footed in reality.* Antwerpen, Apeldoorn: Portland Maklu.

Zając, Dominik. 2020. “Criminal jurisdiction over the Internet: Jurisdictional links in the cyber era”. *Cambridge Law Review* 4 (2): 1–28.

Статья поступила в редакцию 10 января 2021 г.;
рекомендована к печати 27 мая 2022 г.

Контактная информация:

Клевцов Кирилл Константинович — канд. юрид. наук, доц.; klevtsov001@gmail.com

International cooperation in the fight against cyberpression in the context of response to new challenges and threats

K. K. Klevtsov

MGIMO-University,
76, pr. Vernadskogo, Moscow, 119454, Russian Federation

For citation: Klevtsov, Kirill K. 2022. “International cooperation in the fight against cyberpression in the context of response to new challenges and threats”. *Vestnik of Saint Petersburg University. Law* 3: 678–695. https://doi.org/10.21638/spbu14.2022.306 (In Russian)

This article explores criminal procedure and other organizational and legal aspects of international cooperation between states in the fight against cybercrime in the face of new challenges and threats. The aim is to identify and consider formal and informal measures of international cooperation in response to transnational cybercrime. Through legal analysis, we demonstrate that such crimes, as a rule, have an international character, as they have negative consequences on the territory of other sovereign countries. The author analyzes various forms of international cooperation in the fight against crime, which include extradition (extradition), legal assistance in criminal matters, transfer of criminal prosecution (judicial proceedings), as well as informal cooperation between law enforcement agencies (international police cooperation), in particular within the framework of US law called “CLOUD Act”. As an empirical basis for the study, materials of Russian operational and investigative practice for 2018–2019, as well as decisions of courts of foreign states, were used. However, the majority of law enforcement agencies deliberately or without intent resort to the practice of obtaining evidence on cybercrimes that are physically located on the territory of another country, independently, without obtaining the consent of this state. This happens through a remote connection in real time to the subscriber device of a criminally prosecuted person or its withdrawal from a victim or witness located on the territory of the state by law enforcement agencies that conduct proceedings on a cybercrime case with subsequent inspection to find information relevant to the case, as well as through the use of other legal methods.

Keywords: cybercrime, international cooperation, jurisdiction, electronic information, service provider.

References

Abraha, Halefom. 2020. “Regulating law enforcement access to electronic evidence across borders: The United States approach”. *Information & Communications Technology Law* 29: 1–30.

Bassiouni, Cherif M. 2014. International extradition: United States law and practice. 6th rev. ed. New York, Oxford University Press.

Benson, Karyn, Rafael Dowsley, Hovav Shacham. 2011. “Do you know where cloud files are?” *Proceedings of the 3rd ACM Workshop on Cloud Computing Security*, 73–82. New York, Association for Computing Machinery.

Broadhurst, Roderic, Peter Grabosky, Mamoun Alazab, Steve Chon. 2014. "Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime". *International of Journal of Cyber Criminology* 8 (1): 1–20.

Currie, Robert J. 2000. "Human rights and international mutual legal assistance: Resolving the tension". *Criminal Law Forum* 11 (2): 143–181.

Ferzan, Kimberly. 2020. "The reach of the realm. Criminal law". *Philosophy* 14: 335–345. https://doi.org/10.1007/s11572-020-09541-w.

Galbraith, Jean. 2018. "Congress enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, reshaping U. S. law governing cross-border access to data". *American Journal of International Law* 112 (3): 486–493. https://doi.org/10.1017/ajil.2018.61.

Goldfoot, Josh. 2011. "Compelling online providers to produce evidence under ECPA". *The United States Attorneys Bulletin (Obtaining and Admitting Electronic Evidence)* 59 (6): 35–41.

Grant, Christensen. 2019. "The extraterritorial reach of tribal court criminal jurisdiction". *Hastings Constitutional Law Quarterly* 46 (294): 1–18. http://dx.doi.org/10.2139/ssrn.3231533.

Klevtsov, Kirill K. 2018. *Pre-trial proceedings against persons evading criminal responsibility outside the territory of the Russian Federation*. Moscow, Iurlitinform Publ. (In Russian)

Kunev, Denis A. 2019. "Countering the movement of criminal assets abroad and their return to the Russian Federation: Criminal procedural aspects". PhD diss., Moskovskii gosudarstvennyi institut mezhdunarodnykh otnoshenii (universitet) MID RF. (In Russian)

Litvishko, Petr A. 2011. "Issues of procedural independence of the bodies of preliminary investigation of the Russian Federation in the implementation of international cooperation". *Rossiiskii sledovatel'* 18: 13–18. (In Russian)

Litvishko, Petr A. 2015. "Integration of preliminary investigation and search operations: Foreign and international experience". *Biblioteka kriminalista. Nauchnyi zhurnal* 3: 309–319. (In Russian)

Maillart, Jean-Baptiste. 2019. "The limits of subjective territorial jurisdiction in the context of cybercrime". *ERA Forum* 19: 375–390. https://doi.org/10.1007/s12027-018-0527-2.

Malov, Aleksandr. 2018. "Obtaining electronic evidence from foreign jurisdictions (for example, USA)". *Zakonnost'* 9: 56–60. (In Russian)

Megret, Frederic. 2020. "Do not do abroad what you would not do at home?: An exploration of the rationales for extraterritorial criminal jurisdiction over a state's nationals". *Canadian Yearbook of international Law / Annuaire canadien de droit international* 57: 1–40.

Nurbekov, Iskender M. 2011. "Forensic aspects of interaction with foreign competent authorities in the investigation of crimes of an international nature". *Biblioteka kriminalista. Nauchnyi zhurnal* 1: 117–129. (In Russian)

Peterson, Zachary N. J., Mark Gondree, Robert Beverly. 2011. "A position on data sovereignty: The importance of geolocating data in the cloud". *HotCloud: Proceedings of the 3rd USENIX conference of Hot topic in Cloud computing. ResearchGate*. Accessed May 1, 2020. https://www.researchgate.net/publication/236626434_A_Position_Paper_on_Data_Sovereignty_The_Importance_of_Geolocating_Data_in_the_Cloud.pdf.

Plachta, Michal. 1989. "The role of double criminality in international cooperation in penal matters". *Double Criminality Studies in International Criminal Law.* Ed. by Nils Jareborg, 84–134. Uppsala, Iustus Forlag.

Ring, Tim. 2021. "Europol: The Al hacker threat to biometrics". *Biometric Technology Today* 2: 9–11.

Schomburg, Wolfgang, Otto Lagodny. 2020. *Internationale Rechtshilfe in Strafsachen (International Cooperation in Criminal Matters)*. Kommentar. 6., vollig neu bearbeitete Auflage. Munchen, C. H. Beck.

Shatalov, Alekasandr S. 2015. "Legal mechanism for cooperation in the field of criminal justice". *Pravo. Zhurnal Vysshei shkoly ekonomiki* 1: 126–149. (In Russian)

Shcherba, Sergei P. 2016. "International cooperation of Russia in the field of extradition for criminal prosecution based on the principle of reciprocity". *Mezhdunarodnoe ugolovnoe pravo i mezhdunarodnaia iustitsiia* 4: 3–8. (In Russian)

Sieber, Ulrich. 2012. *Straftaten und Strafverfolgung im Internet. Gutachten C zum 69. Deutschen Juristentag.* Munich, C. H. Beck.

Soler, Christopher. 2019. "Aut Dedere Aut Judicare". *The global prosecution of core crimes under international law*, 319–401. The Hague, T. M. C., Asser Press. https://doi.org/10.1007/978-94-6265-335-1_13.

Vermeulen, Gert, Wendy De Bondt, Charlotte Ryckman, eds. 2012. *Rethinking international cooperation in criminal matters in the EU. Moving beyond actors, bringing logic back, footed in reality.* Antwerpen, Apeldoorn, Portland Maklu.

Volevodz, Aleksandr G. 2014. *International criminal justice and human rights*. Moscow, Rossiiskii universitet druzhby narodov Publ. (In Russian)

Volevodz, Aleksandr G. 2016. "Some aspects of investigation planning in international cooperation in criminal matters". *Ugolovnoe sudoproizvodstvo* 3: 26–33. (In Russian)

Zając, Dominik. 2020. "Criminal jurisdiction over the Internet: Jurisdictional links in the cyber era". *Cambridge Law Review* 4 (2): 1–28.

Zhubrin, Roman V. 2018. "Deadlines for the execution of requests for legal assistance in criminal matters". *Zakonnost'* 5: 12–14. (In Russian)

Received: January 10, 2021
Accepted: May 27, 2022

Author's information:

Kirill K. Klevtsov — PhD in Law, Associate Professor; klevtsov001@gmail.com