

Международное право

Правильная ссылка на статью:

Тебенёкова В.Н. — Отдельные проблемы экстратерриториальной исполнительной юрисдикции государств в киберпространстве // Международное право. – 2023. – № 4. – С. 36 - 48. DOI: 10.25136/2644-5514.2023.4.68724
EDN: WAGCHK URL: https://nbpublish.com/library_read_article.php?id=68724

Отдельные проблемы экстратерриториальной исполнительной юрисдикции государств в киберпространстве

Тебенёкова Виктория Николаевна

аспирант, кафедра международного права, Московский государственный юридический университет имени О. Е. Кутафина

123001, Россия, Москва, г. Москва, ул. Садовая-Кудринская, 9

✉ vikivik.teb@gmail.com



[Статья из рубрики "Теория и философия международного права"](#)

DOI:

10.25136/2644-5514.2023.4.68724

EDN:

WAGCHK

Дата направления статьи в редакцию:

11-10-2023

Дата публикации:

18-10-2023

Аннотация: Появление и активное использование информационно-коммуникационных технологий, прежде всего Интернета, привело к тому, что государства осуществляют такой вид экстратерриториальной исполнительной юрисдикции, как прямой доступ к данным, хранящимся на территории другого государства. Осуществление подобных действий представляется допустимым в случае, когда данные являются общедоступными или доступ осуществляется с согласия государства. Более спорной является ситуация, когда данные получены с законного и добровольного согласия лица, обладающего законными полномочиями на их раскрытие. Косвенный трансграничный доступ к информации, осуществляемый посредством направления поставщику информационных услуг запроса обязывающего согласно национальному законодательству раскрыть

информацию о своих абонентах вне зависимости от ее фактического местоположения, также можно расцениваться в качестве противоречащего международному праву. В связи с этим государства продолжают руководствоваться запросами о международной правовой помощи, что не способствует эффективному расследованию преступлений, связанных с использованием ИКТ и не учитывает природу электронных доказательств. Углубление международного сотрудничества внутри региональных объединений приводит к риску формирования страновых кластеров, в рамках которых существуют необходимые процедуры для сотрудничества между участниками, но которые по отношению к другим странам ограничиваются «традиционными» видами международного сотрудничества, не учитывающими особенности электронных доказательств. Таким образом, требуется разработка общих стандартов удаленного доступа к данным, находящихся на серверах и устройствах, расположенных на территории иностранного государства. Подобные документы должны определять процедуры и правила получения согласия лица, обладающего полномочиями на трансграничное раскрытие данных, расширять универсальное международное сотрудничество, в том числе путем признания возможности направления прямых запросов о предоставлении определенной информации об абонентах поставщикам информационных услуг, устанавливать механизмы раскрытия поставщиками информационных услуг данных, находящихся под их контролем, но хранящихся на серверах, расположенных на территории иностранных государств.

Ключевые слова:

юрисдикция в киберпространстве, киберпространство, международное право, экстратерриториальная юрисдикция, экстратерриториальная исполнительная юрисдикция, экстратерриториальный доступ, электронные доказательства, удаленный доступ, взаимная правовая помощь, доказательства в киберпространстве

Введение

Традиционно исполнительная юрисдикция, направленная на принудительное приведение в исполнение законодательства государства, носит территориальный характер, означающий, что государства могут реализовывать свои властные полномочия в полной мере только отношении лиц, объектов и событий, находящихся или происходящих на их территории.

Вместе с тем развитие и активное использование информационно-коммуникационных технологий, прежде всего Интернета, привело к появлению новых видов экстратерриториальной исполнительной юрисдикции, законность которых, с точки зрения международного права, вызывает вопросы. В частности, речь идет об осуществлении государствами доступа к информации, хранящейся на веб-сайтах, устройствах или серверах за пределами их территории (далее - трансграничный удаленный доступ к информации/данным; термины «информация» и «данные» в рамках настоящей статьи используются в качестве синонимов).

Данная проблема является особенно актуальной в свете увеличения числа и территориального охвата киберпреступлений, доказательства по которым нередко существуют только в электронной форме и могут быть расположены по всему земному шару.

Международные конвенции предусматривают такой способ получения информации, как

обращение с запросами о правовой помощи. Основные проблемы, однако, заключаются в том, что запросы о правовой помощи могут быть неэффективны в ситуации, когда данные находятся на устройствах и серверах, расположенных по всему земному шару. Более того, данные могут быть оперативно перемещены из одной юрисдикции в другую, изменены или удалены, могут храниться в разных юрисдикциях одновременно, что делает механизмы взаимной правовой помощи устаревшими и часто неосуществимыми.

В связи с этим многие государства признают удаленный доступ к информации, хранящейся на веб-сайтах, компьютерах или серверах за пределами их территории, правомерным, а доказательства, полученные таким образом, законными.

Примером может являться Решение Верховного суда Норвегии по делу Tidal (Tidal Music AS v. The Public Prosecution Authority, HR-2019-610-A, case №19-010640STR-HRET, March 28, 2019), в котором суд признал допустимым действия правоохранительных органов Норвегии, которые во время проведения обыска в помещениях компаний в Норвегии, через находящиеся там компьютеры скачали определенные данные с серверов, находящихся в США и в других европейских странах. По мнению суда действия правоохранительных органов не затронули другое государство в той степени, в какой это представляет собой нарушение принципа суверенитета, так как поиск данных был проведен в норвежской компании с использованием учетных данных доступа, которые компания в лице своих сотрудников предоставила норвежским правоохранительным органам.

Другой иллюстрацией является закон США о разъяснении законного использования данных за рубежом, также известный как «CLOUD Act» (The Clarifying Lawful Overseas Use of Data Act or CLOUD Act (H.R. 4943), March 23, 2018), который напрямую не санкционирует право осуществления правоохранительными органами удаленного трансграничного доступа к информации, но обязывают поставщиков информационно-коммуникационных услуг на основании ордера или повестки в суд предоставлять информацию, находящуюся под их контролем вне зависимости от места положения данных.

Таким образом можно выделить два способа, используемых государствами для получения трансграничного доступа к информации, хранящейся на территории другого государства:

- прямой доступ к данным с использованием технологических средств или
- косвенный доступ через направления запроса поставщикам информационно-коммуникационных услуг (далее – поставщики услуг) [\[1, с.540\]](#).

Несмотря на практическое применение данных способов, вопрос о том, могут ли государства с точки зрения международного права осуществлять подобные действия и при каких обстоятельствах, остается открытым.

Приступая к анализу данного вопроса, отметим, что согласно общепризнанному подходу международное право применяется к деятельности государств, связанной с использованием информационно-коммуникационных технологий [\[2\]](#). В связи с этим экстратерриториальная исполнительная юрисдикция в данной сфере должна отвечать требованиям международного права.

Экстратерриториальная исполнительная юрисдикции государств в международном праве.

Термин экстратерриториальная юрисдикции в международном праве применяется для обозначения осуществления суверенного права или полномочий какого-либо государства за пределами его территории [\[3, с.273-274\]](#).

В связи с тем, что осуществление экстратерриториальной юрисдикции государства может затрагивать суверенные права и представлять собой незаконное вмешательство во внутренние дела иностранных государств, проблема осуществления подобной юрисдикции является важнейшей в международном праве.

Существенное значение для рассмотрения вопроса о том, каким образом международное право регулирует экстратерриториальную юрисдикцию, имеет классификация юрисдикции на предписывающую юрисдикцию, выражающуюся в установлении правовых норм, и исполнительную юрисдикцию, обеспечивающую исполнение правовых норм путем применения правового принуждения [\[4, с.33-37\]](#).

Установления экстратерриториальной предписывающей юрисдикции основывается на признанных международным правом принципах экстратерриториальной юрисдикции, демонстрирующих законные интересы государства при утверждении его юрисдикции в том или ином случае на основе достаточной связи с соответствующими лицами, имуществом и действиями [\[3, с.275\]](#).

По мнению Комиссии международного права ООН такими принципами, позволяющими государству распространять действие национального законодательства за пределы собственной территории, являются: а) принцип объективной территориальности; б) доктрина последствий; с) принцип защиты; d) принцип гражданства; и е) принцип пассивной правосубъектности [\[3, с.275\]](#).

В свою очередь осуществление исполнительной юрисдикции носит более строгий территориальный характер и ее экстратерриториальное проявление может осуществляться только при наличии разрешительной нормы международного права или с согласия государства.

Данный вывод был подчеркнут в деле Лотус (The «Lotus» Case, 7 September 1927. PCIJ A., № 10. 1927), в котором Постоянная палата международного правосудия, фактически проводя различие между предписывающей и исполнительной юрисдикцией указала, что международное право не запрещает государствам распространять применение своих законов на лиц, имущество и действия за пределами их территории и в дальнейшем осуществлять юрисдикцию на своей собственной территории, однако «...при отсутствии разрешающей нормы об обратном государство не может осуществлять свою власть в какой бы то ни было форме на территории другого государства. В этом смысле юрисдикция, безусловно, является территориальной; она не может осуществляться государством за пределами его территории, кроме как в силу разрешительной нормы, вытекающей из международного обычая или конвенции».

В докладе Комиссии международного права ООН, посвященном экстратерриториальной юрисдикции, особо подчеркивается, что государство не может исполнять свое уголовное законодательство, то есть расследовать преступления или подвергать аресту подозреваемых на территории другого государства без согласия этого другого государства [\[3, с.278\]](#).

Прямой трансграничный доступ к данным

Прямой трансграничный доступ правоохранительных органов к информации, хранящейся на серверах и устройствах, расположенных за пределами территории государства, является одним из видов экстратерриториальной исполнительной юрисдикции, так как предполагает осуществление правоохранительных функций, направленных на получение электронных доказательств, за пределами территории государства.

При этом в настоящий момент не существует нормы обычного или универсального конвенционного международного права, позволяющей государствам осуществлять подобный вид экстратерриториальной юрисдикции. В связи с этим прямой удаленный доступ к информации на территории другого государств без его согласия будет представлять собой нарушение международного права.

Данный вывод можно подкрепить ссылкой на нормы действующих международных конвенций регионального характера, регламентирующих среди прочего международное сотрудничество по уголовным делам, связанным с использованием ИКТ, которые прямо ограничивают возможность осуществления прямого удаленного доступа к информации территорией государства. В частности, подобные положения установлены в статье 19 Конвенции о преступности в сфере компьютерной информации 2001 года (Будапештская конвенция) [\[5\]](#) и статье 4 Конвенции Лиги арабских государств о борьбе с преступлениями в области информационных технологий 2010 года [\[6\]](#).

В разрабатываемом в настоящий момент проекте конвенции ООН о киберпреступности также предлагается закрепить положение о том, что государство-участники не обладают правом осуществлять на территории другого государства юрисдикцию и функции, которые входят исключительно в компетенцию органов этого другого государства в соответствии с его внутренним законодательством, а деятельность по сбору электронных доказательств должна быть ограничена собственной территорией государства [\[7\]](#).

Кроме того, отметим, что государства обладают исключительной юрисдикцией в отношении ИКТ-инфраструктуры, расположенной на их территории. При этом в соответствии с принципом невмешательства, государства не должны прямо или косвенно вмешиваться во внутренние дела другого государства, в том числе с помощью ИКТ [\[2\]](#).

Таким образом, прямой трансграничный доступ будет приводить к нарушениям суверенитета государства, на территории которого данные находятся, а также представлять собой неоправданное вмешательство в дела, входящие во внутреннюю компетенцию государства, что может рассматриваться как нарушение принципа невмешательства.

Существует, однако, ряд случаев, когда прямой трансграничный доступ к информации рассматривается как допустимый международным правом.

Профессор Седрик Рингарт, в частности, указывает на допустимость подобных действий в случаях, если информация общедоступна, территориальное государство разрешает такие поиски или владелец информации дает свое согласие [8. с.81].

Действительно в случаях, когда речь идет об общедоступных данных и общедоступных источниках информации, например, интернет-сайтах, страниц в социальных сетях, речь вряд ли может идти о неправомерном доступе к информации, которая уже разглашена для всеобщего сведения.

Осуществление прямого трансграничного доступа на основании согласия государства, на территории которого хранятся данные, также будет соответствовать международному

праву.

Более сложным вопросом является возможность доступа к информации на основании согласия ее «владельца».

Подобное основание содержится в подпункте b статьи 32 Будапештской конвенции и подпункте 2 статьи 40 Конвенции Лиги арабских государств о борьбе с преступлениями в области информационных технологий 2010 г.

Так, в подпункте b статьи 32 Будапештской конвенции указано, что сторона может без согласия другой стороны получать через компьютерную систему на своей территории доступ к хранящимся на территории другой стороны компьютерным данным или получать их, если эта Сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой Стороне через такую компьютерную систему.

Вместе с тем упомянутые договоры не являются универсальными и распространяют свое действие исключительно на государств-членов.

При этом, наш взгляд, выводы о том, что получение доступа на основании согласия уполномоченного лица будет рассматриваться всеми государствами в качестве соответствующего международному праву, являются преждевременными.

Подобные сомнения вызывает тот факт, что положение о возможности получения прямого трансграничного доступа к данным на основании согласия было исключено из разрабатываемого в настоящий момент проекта конвенции ООН о киберпреступности.

Так, в статье 72 проекта конвенции, рассмотренного в ходе пятой переговорной сессии специального комитета [\[9\]](#) содержалось положение о том, что государство-участник может без разрешения другого государства-участника получать через компьютерную систему на своей территории доступ к хранящимся компьютерным данным, находящимся в другом государстве-участнике, или сами такие данные, если государство-участник, осуществляющее доступ к данным или получающее такие данные, получает законное и добровольное согласие лица, имеющего законные полномочия на раскрытие данных этому государству-участнику через эту компьютерную систему.

По результатам переговорной сессии специального комитета данный пункт был исключен из проекта конвенции и не содержался в сводном переговорном документе, обсуждаемом на шестой сессии [\[10\]](#).

Полагаем, что основные причины исключения данного положения связаны с опасениями государств относительно возможного нарушения суверенитета государств-участников при осуществлении данного типа доступа и отсутствия правовой определенности терминов «законного и добровольного согласия», а также «законных полномочий».

В частности, Российская Федерация отмечает, что не ясно чей закон и кем должен применяться при оценке «законного и добровольного согласия» и «законных полномочий», а также не понятно, будут ли поставщики услуг обладать такими «законными полномочиями» для трансграничного раскрытия данных своих [\[11\]](#).

По нашему мнению, сама природа киберпространства, подразумевающего возможность хранения данных по всему миру, приводит к тому, что прямой трансграничный доступ к информации на основании законного и добровольного согласия лица, имеющего

законные полномочия на раскрытие данных, должен рассматриваться в качестве допустимого.

В ином случае направление запроса о международной помощи требуется и в том случае, когда законный «владелец» информации готов добровольно предоставить ее правоохранным органам. Данный подход обладает целым рядом недостатков, так как приводит к неоправданному затягиванию расследований, связанному с необходимостью прибегать к механизмам взаимной правовой помощи, и нарушает прав «владельца» информации на свободное распоряжение ею. Кроме того, данный подход вряд ли способен в полной мере быть реализован в практической действительности так как и «владелец» информации и правоохранные органы часто могут не знать фактическое место хранения данных, особенно если речь идет о хранении данных поставщиком облачных услуг, которые, как правило, имеют сервера в целом ряде государств.

В связи с этим требуется достижение международного консенсуса, направленного на решение спорных вопросов, связанных с получением информации на основании согласия ее «владельца».

По нашему мнению, лицом, обладающим законными полномочиями на раскрытие данных, должен являться непосредственный «владелец» данных, например, физическое лицо или его законный представитель, если речь идет о персональных данных, информации на его электронной почте, аккаунтах в приложениях, социальных сетях, веб-сайтах, компьютерных устройствах.

При этом оценка терминов «законного и добровольного согласия» и «законных полномочий» должна трактоваться в соответствии с законодательством государства «владельца» данных.

Поставщики информационных услуг, по общему правилу, не должны рассматриваться в качестве лиц, обладающих законными полномочиями на трансграничное раскрытие данных своих абонентов. Обращение к поставщикам услуг должно осуществляться через запросы о правовой помощи, либо посредством признания возможности прямого направления запроса поставщику услуг на основании двухстороннего или многостороннего международного договора.

Примером подобного международного сотрудничества может являться Второй дополнительный протокол 2022 года к Конвенции о киберпреступности о расширении сотрудничества и раскрытии электронных доказательств [\[12\]](#).

В дополнительном протоколе предусмотрено два вида запросов, которые государство-участник конвенции может направлять напрямую к поставщикам услуг в другом государстве-участнике:

- запрос в адрес поставщика услуги по регистрации доменных имен на территории другой стороны, информации для идентификации владельца регистрации доменного имени или связи с ним (статья 6);
- запрос в адрес поставщика услуг на территории другой стороны, с целью раскрытия информации о конкретном абоненте (Статья 7).

При этом государства должны принять законодательные меры, обязывающие поставщиков услуг на их территории предоставлять данные по запросу государства-участника.

Косвенный трансграничный доступ

Косвенный трансграничный доступ предполагает получение информации об абонентах поставщика услуг, хранящейся на территории другого государства, путем направления обязательных для исполнения согласно национальному законодательству запросов поставщику услуг.

Для решения вопроса о том, осуществляется ли при данном типе доступа экстратерриториальная исполнительная юрисдикции можно рассмотреть аргументы, используемые в деле, связанном с выдачей властями США в адрес Microsoft ордера на предоставление данных находящимся под контролем Microsoft, но хранящихся на территории Ирландии (Microsoft Corp. v. United, 829 F.3d 197 (2d Cir. 2016)).

В ходе разбирательства в суде апелляционной инстанции Microsoft утверждала, что запрашиваемые данные не могут быть предоставлены, так как хранятся на серверах в Ирландии, в связи с чем выдавая ордер, обязывающий раскрывать данные, власти США осуществляют незаконную исполнительную деятельность на территории другого государства.

В свою очередь правительство США указывало на отсутствие экстратерриториальной исполнительной юрисдикции в данном случае, так как предоставление информации по ордеру не требовало, чтобы должностные лица США входили в помещение адресата для обыска и наложения ареста на имущество, находящееся в его владении, а скорее требовал, чтобы адресат раскрыл властям США имеющиеся в его распоряжении данные. В связи с этим власти США не осуществляли бы никаких действий по физическому принуждению за рубежом, поскольку все шаги, необходимые для обеспечения раскрытия информации, были бы предприняты самой Microsoft.

Суд, анализируя данный вопрос, сосредоточился на определении момента, когда имело бы место вмешательство в права клиента на неприкосновенность частной жизни в случае приведения ордера в исполнение. В случае, если это происходит в том месте, где Microsoft передает данные властям США, т.е. на территории США после того, как Microsoft экспортировала их туда, то вопрос об экстратерриториальной юрисдикции не возникает и предоставление данных по ордеру является допустимым. В случае, если вмешательство происходит в момент, когда Microsoft получает доступ для целей извлечения к данным, хранящимся в дата-центре в Ирландии, то происходит недопустимое экстратерриториальное применение.

В результате суд постановил, что любое вмешательство в права клиента на неприкосновенность частной жизни происходит там, где хранятся защищенные данные. Таким образом, поскольку запрашиваемые данные хранились в дата-центре, расположенном в Ирландии, суд постановил, что исполнение ордера нарушило бы суверенитет Ирландии, если процедуры направления запроса о правовой помощи не были соблюдены.

Решение было обжаловано в Верховный суд, который, однако, не вынес решения, по существу, по причине внесения в закон поправок, явным образом обязывающих поставщиков услуг на территории США предоставлять информацию, находящуюся под их контролем по ордеру или повестке, независимо от фактического местоположения данных (речь идет о ранее упомянутом законе США о разъяснении законного использования данных за рубежом, известном также как « CLOUD Act»).

Решение суда и позиции сторон по данному делу иллюстрируют два взгляда на то, осуществляется ли экстратерриториальная исполнительная юрисдикция в случаях получения косвенного доступа к данным.

Анализируя указанное дело, профессор Дэн Свантессон отметил, что позиции Microsoft и правительства США могут быть одновременно правильными в зависимости от того, каким образом мы понимаем экстратерриториальную юрисдикцию: «как утверждает правительство, и это правда, что на иностранной территории не ведется никакой правоприменительной деятельности. Однако, и это важно, на территории другого государства осуществляются правоохранительные функции. Другими словами, правительство смотрит исключительно на место, из которого осуществляется юрисдикция (Соединенные Штаты). Корпорация Microsoft также учитывает экстратерриториальные последствия, и эти последствия проявляются в Ирландии. Таким образом, правительство США дает экстратерриториальности узкое определение, в то время как Microsoft дает ей широкое определение» [\[13, с. 52\]](#).

В результате профессор приходит к выводу, что международное право не может решить данную проблему, так как в нем не содержится положений, определяющих, где именно имеет место рассматриваемое поведение в ситуациях, подобных делу об ордере Microsoft, то есть в какой момент происходит раскрытие информации и соответственно осуществление исполнительной юрисдикции государств [\[13, с.51\]](#).

Критикуя указанные доводы, другой исследователь - Стивен Аллен, указывает на необходимости системного рассмотрения данного вопроса и предлагает обратиться не только к нормам об юрисдикции, но и об ответственности государств в международном праве [\[14, с.407-408\]](#).

Так, статье 5 Статей об ответственности государств за международно-противоправные деяния, согласно которой поведение лица или образования, не являющегося органом государства в соответствии со статьей 4, но уполномоченного правом этого государства осуществлять элементы государственной власти, рассматривается как деяние этого государства по международному праву, при условии что в данном случае это лицо или образование действует в этом качестве [\[15\]](#).

В свете данных положений, тот факт, что представители правоохранительных органов не будут непосредственно заниматься правоприменительной деятельностью на территории другого государства, не является ключевым критерием для установления ответственности государства с точки зрения международного права.

В результате косвенный доступ становится аналогичным прямому доступу, при котором в качестве агента государства действует не его правоохранительные органы, а частное лицо, уполномоченное на это государством.

Таким образом, осуществление косвенного доступа к данным также может рассматриваться как нарушение международного права, в случае отсутствия согласия государства, на территории которого фактически хранятся данные.

С другой стороны, подобный подход явно не способствует эффективному и оперативному сбору электронных доказательств и делает привлекательным для поставщиков услуг поиск благоприятных правовых режимов, характеризующийся низкой степенью международного сотрудничества.

В связи с этим выводы профессора Дэн Свантессона о том, что решение

проблемы косвенного доступа к данным, требует создания юридической фикции, направленной на определение момента раскрытия данных и разработки условий подобного раскрытия, являются достаточно разумными [\[13, с.51\]](#).

Вывод.

На основании вышеизложенного можно прийти к выводу, что прямой трансграничный доступ к данным, хранящимся на территории иностранного государства, является одним из способов осуществления экстратерриториальной исполнительной юрисдикции и соответственно должен осуществляться в соответствии с требованиями международного права, а именно наличия разрешительной нормы или согласия государства.

Бесспорным в международном праве является подход, согласно которому государства могут получать удаленный доступ к данным, хранящимся на территории другого государства в случае, если такие данные являются общедоступными, либо получено согласие государства на доступ к данным.

Более сложной является ситуация, когда доступ был получен на основании законного и добровольного согласия лица, имеющего законные полномочия предоставить доступ. В частности, разногласия могут возникнуть, как в связи с общей правомерность осуществления подобного доступа без согласия государства, на территории которого данные хранятся, так и в связи с толкованием терминов «законные полномочия» и «законное и добровольное согласие».

Косвенный трансграничный доступ к информации, осуществляемый посредством направления поставщику информационных услуг запроса, обязывающего согласно национальному законодательству раскрыть информацию о своих абонентах вне зависимости от ее фактического местоположения, также можно расцениваться в качестве противоречащего международному праву. Поставщик услуг в таком случае рассматривается в качестве агента государства и осуществляет неправомерный, с точки зрения международного права, доступ к данным, находящимся под юрисдикцией иностранного государства.

Указанные сложности приводят к тому, что государства продолжают руководствоваться запросами о взаимной правовой помощи в целях получения электронных данных несмотря на то, что вопрос об эффективности использования подобных способов для борьбы с киберпреступностью остается открытым.

Более продвинуты механизмы сотрудничества, как например, возможность направления прямых запросов поставщикам услуг, развиваются в рамках региональных объединений, что, по справедливому мнению межправительственной группы экспертов по киберпреступности ООН увеличивает риск образования страновых кластеров, в рамках которых существуют необходимые полномочия и процедуры для сотрудничества между входящими в их состав странами, но которые по отношению ко всем другим странам ограничиваются «традиционными» видами международного сотрудничества, не учитывающими особенности электронных доказательств [\[16, с.220\]](#).

В связи с этим в целях повышения эффективности борьбы с киберпреступностью и получения электронных доказательств требуется разработка общих стандартов удаленного доступа к данным, находящимся на серверах и устройствах, расположенных на территории другого государства. Подобные стандарты должны регулировать следующие направления:

- определять процедуры и правила получения согласия лица, обладающего полномочиями на трансграничное раскрытие данных;
- расширять универсальное международное сотрудничество, в том числе путем признания возможности направления прямых запросов о предоставлении определенной информации об абонентах поставщикам услуг;
- устанавливать механизмы раскрытия поставщиками услуг данных, находящихся под контролем поставщика, но хранящихся на серверах, расположенных на территории иностранных государств.

Библиография

1. Ryngaert C. *Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts* // *German Law Journal*. 2023. № 24(3). Pp. 537–550.
2. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности № A/76/135, 14 июля 2021 // URL: <https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=A/76/135&Lang=R> (дата обращения: 14.10.2023).
3. Документ A/61/10. Доклад Комиссии международного права о работе её пятьдесят восьмой сессии (1 мая – 9 июня и 3 июля – 11 августа 2006 года) // URL: https://legal.un.org/ilc/publications/yearbooks/russian/ilc_2006_v2_p2.pdf (дата обращения: 14.10.2023).
4. Черниченко О.С. Международно-правовые аспекты юрисдикции государств: дис. ... канд. юрид. наук. – М., 2003.
5. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) // URL: <https://rm.coe.int/1680081580> (дата обращения: 14.10.2023).
6. Конвенции Лиги арабских государств о борьбе с преступлениями в области информационных технологий 2010 года // URL: <https://www.asianlaws.org/gclid/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf> (дата обращения 14.10.2023).
7. Проект текста конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях № A/AC.291/22, 29 Мая 2023 // URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/V23/039/53/PDF/V2303953.pdf?OpenElement> (дата обращения 14.10.2023).
8. Cedric R. *Jurisdiction in international law – Second Edition*. – Oxford: Oxford University Press, 2015.
9. Сводный переговорный документ, содержащий преамбулу, положения о международном сотрудничестве, мерах по предупреждению, технической помощи и механизме осуществления и заключительные положения проекта всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях № A/AC.291/19, 19 December 2022 // URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/V22/188/35/PDF/V2218835.pdf?OpenElement> (дата обращения: 14.10.2023).
10. Сводный переговорный документ по преамбуле, положениям о международном сотрудничестве, превентивных мерах, технической помощи и механизме осуществления и заключительным положениям всеобъемлющей международной

конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях от 21 апреля 2023 // URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Document/s/CND_2_-_21.04.2023.pdf (дата обращения: 14.10.2023).

11. Заявление делегации Российской Федерации на пятой сессии Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях (Вена, 11-21 апреля 2023 года) // URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Document/s/Member_States/RU_RF_Statement_5_session_RU_PDF.pdf (дата обращения: 14.10.2023).
12. Второй дополнительный протокол к Конвенции о киберпреступности о расширении сотрудничества и раскрытии электронных доказательств (CETS № 224) // URL: <https://rm.coe.int/1680a49dab> (дата обращения: 14.10.2023).
13. Svantesson. D. Solving the Internet Jurisdiction Puzzle. – Oxford: Oxford University Press, 2017.
14. The Oxford Handbook of Jurisdiction in International Law / Ed. by S. Allen, D. Costelloe, M. Fitzmaurice, P. Gragl, and Ed. Guntrip. — Oxford : Oxford University Press, 2019.
15. Резолюция Генеральной Ассамблеи ООН A/RES/56/83 «Ответственность государств за международно-противоправные деяния» от 28 января 2002 // URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/477/99/PDF/N0147799.pdf?OpenElement> (accessed: 14.10.2023).
16. Проект всестороннего исследования проблемы киберпреступности, февраль 2013 года // URL: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf (дата обращения: 14.10.2023).

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.

Со списком рецензентов издательства можно ознакомиться [здесь](#).

Предмет исследования. Рецензируемая статья "Отдельные проблемы экстратерриториальной исполнительной юрисдикции государств в киберпространстве" в качестве предмета исследования исследования имеет нормы международного права об оказании правовой помощи. Автор предпринял попытку показать, что "...запросы о правовой помощи могут быть неэффективны в ситуации, когда данные находятся на устройствах и серверах, расположенных по всему земному шару. Более того, данные могут быть оперативно перемещены из одной юрисдикции в другую, изменены или удалены, могут храниться в разных юрисдикциях одновременно, что делает механизмы взаимной правовой помощи устаревшими и часто неосуществимыми".

Методология исследования. Исходя из содержания статьи можно заключить, что в ходе ее написания автором использовались многие современные методы научного познания, как общенаучные, так и частные (специальные). Можно отметить применение такие приемов и способов научного познания, как: анализ, абстрагирование, индукция, дедукция, гипотеза, аналогия, синтез, типология, классификация, систематизация, обобщение и др.

Актуальность исследования. Глобальная цифровизация всех сфер жизнедеятельности порождает необходимость совершенствования правового регулирования общественных

отношений нового формата, складывающихся между членами информационного общества. Как отмечает автор данной статьи, "Данная проблема является особенно актуальной в свете увеличения числа и территориального охвата киберпреступлений, доказательства по которым нередко существуют только в электронной форме и могут быть расположены по всему земному шару". Экстратерриториальность - это один из признаков информационного общества. Государства на международном и национальных уровнях должны искать пути решения проблем правового регулирования, а также правоприменения в современных условиях. Представляется, что актуальность тематики этой статьи очевидна.

Научная новизна. Процесс цифровизации и становления информационного общества требует новых научных разработок, в том числе и по различным аспектам юриспруденции. Автор этой статьи, пожалуй, впервые в отечественной юридической науке обратился к проблеме экстратерриториальной исполнительной юрисдикции государств в киберпространстве. Выводы и предложения автора по разрешению существующих проблем в этой сфере общественных отношений аргументированы и заслуживают внимания, например: "...прямой трансграничный доступ к данным, хранящимся на территории иностранного государства, является одним из способов осуществления экстратерриториальной исполнительной юрисдикции и соответственно должен осуществляться в соответствии с требованиями международного права, а именно наличия разрешительной нормы или согласия государства".

Стиль, структура, содержание. Статья написана научным стилем, с применением специальной юридической терминологии. Применение отдельных терминов (их понятия) разъясняются автором, что может свидетельствовать о наличии понятийного аппарата, используемого при написании статьи. Материал изложен последовательно, грамотно и ясно. Статья структурирована. Тема раскрыта. Статья по содержанию соответствует своему названию.

Библиография. В качестве устранимого замечания можно отметить, что автором использовано недостаточное количество доктринальных источников (для научной статьи - не менее 10), включая публикации последних лет. Представляется, что статья "выиграла" бы в научном плане, если был бы актуализирован список библиографии (и соответственно содержание статьи). Исходя из тематики статьи допустимо использование иностранных публикаций в качестве источников библиографии.

Апелляция к оппонентам. В статье имеет место научная дискуссия. Обращения к оппонентам корректное.

Выводы, интерес читательской аудитории. Статья "Отдельные проблемы экстратерриториальной исполнительной юрисдикции государств в киберпространстве" рекомендуется к опубликованию. Статья отвечает установленным требованиям, отличается актуальностью, имеет практическую значимость и содержит элементы научной новизны. Данная публикация может представлять интерес для ученых, практиков, а также преподавателей и студентов юридических вузов и факультетов.