DOI: https://doi.org/10.24833/0869-0049-2024-4-119-131

Исследовательская статья
УДК: 341
Поступила в редакцию: 31.08.2024
Принята к публикации: 13.10.2024

Ирина Григорьевна ЛУКЬЯНЦЕВА
Московский государственный институт международных отношений (университет)
Министерства иностранных дел России
Вернадского п-т, д. 76, Москва, 119454, Российская Федерация
ilukiyantseva1@gmail.com
ORCID: 0009-0003-9940-4645

ПРОБЛЕМА ПРИСВОЕНИЯ ДЕЯНИЙ, СОВЕРШЕННЫХ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

ВВЕДЕНИЕ. *В основе настоящего исследования лежит проблема присвоения ответственности за деяния, совершенные в информационном пространстве. Ее актуальность обуславливается наметившейся в последнее время тенденцией, заключающейся в применении отдельными государствами информационно-коммуникационных технологий (далее – ИКТ) для утверждения своего геополитического превосходства. Вместе с тем остаются открытыми как вопрос присвоения подобных распространенных деяний, так и вопрос дальнейшего реагирования на них. В связи с этим в статье анализируются теоретические аспекты международно-правовой ответственности, в том числе вопросы единообразного применения соответствующей терминологии, особенности присвоения деяния в информационном пространстве. Также рассматривается вопрос эффективности международно-правового регулирования указанной тематики.*

МАТЕРИАЛЫ И МЕТОДЫ. *В научном исследовании рассмотрены международные договоры, международно-правовые обычаи, общепризнанные принципы международного права, а также резолюции, материалы и документы профильных рабочих групп, российская и зарубежная доктрина. При подготовке исследования использовались общенаучные и частнонаучные методы познания (методы анализа и синтеза, дедукции, индукции, диалектический и формально-юридический методы).*

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ. *Результатом проведенного исследования является заключение о невозможности эффективного регулирования вопросов, возникающих в связи с осуществлением атак в информационном пространстве, действующим международным правом и необходимости разработки профильного международного договора с учетом положений концепции Конвенции Организации Объединенных Нация (далее – ООН) об обеспечении международной информационной безопасности. При этом для осуществления эффективного присвоения деяния важно учитывать политический, технический и правовой элементы присвоения ответственности.*

ОБСУЖДЕНИЯ И ВЫВОДЫ. *В статье проведен комплексный анализ подходов к проблеме присвоения атак в информационном пространстве, а также способов реагирования на них в соответствии с действующим международным правом. Рассматриваются конкретные инициативы государств на международных площадках, а также позиции технических специалистов и политологов по данному вопросу. Помимо этого, автор проводит анализ положений концепции Конвенции ООН об обеспечении международной информационной безопасности. Сделан вывод, что вопрос присвоения деяния, совершенного в информационном пространстве, требует разработки дополнительного международно-правового регулирования, которое будет учитывать особенности информационного*

пространства. Также представляется важным развитие международного сотрудничества в данной области, в том числе через создание глобального реестра контактных пунктов.

КЛЮЧЕВЫЕ СЛОВА: *информационное пространство, ответственность, присвоение деяния, ответные меры, реестр контактных пунктов, международное право, Устав ООН, концепция Конвенции ООН об обеспечении международной информационной безопасности*

ДЛЯ ЦИТИРОВАНИЯ: Лукьянцева И.Г. 2024. Проблема присвоения деяний, совершенных в информационном пространстве. – *Московский журнал международного права.* № 4. С. 119–131. DOI: https://doi.org/10.24833/0869-0049-2024-4-119-131

Автор заявляет об отсутствии конфликта интересов.

DOI: https://doi.org/10.24833/0869-0049-2024-4-119-131

Research article
UDC: 341
Received 31 August 2024
Approved 13 October 2024

Irina G. LUKIYANTSEVA
Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation
76, Vernadskogo Ave., Moscow, Russian Federation, 119454
ilukiyantseva1@gmail.com
ORCID: 0009-0003-9940-4645

THE ISSUE OF ATTRIBUTION OF ACTS COMMITTED IN THE INFORMATION SPACE

INTRODUCTION. *Due to the recent trend related to the use of information and communication technologies by certain states with the aim to assert their geopolitical superiority, study of the issue of attribution of responsibility for acts committed in the information space as well as possible of responses to such attacks becomes even more relevant. Therefore, in the article the problems related to international responsibility, particularities of attacks in information space and ways to attribute such attacks, as well as effectiveness of international law are analyzed.*

MATERIALS AND METHODS. *The research examines treaties, international customs, general widely recognized principles of international law, as well as resolutions, materials and documents of specialized working groups, and doctrine. General scientific and specific scientific methods of enquiry (methods of analysis and synthesis, deduction, induction, dialectical and formal legal methods) were used in the preparation of the study.*

RESEARCH RESULTS. *The result of the conducted research is the conclusion that it is impossible to effectively regulate issues arising from the issue of attribution of acts committed in the information space exclusively with the current international law. Therefore, there is a need to develop a relevant international treaty taking into account the provisions of the concept of the UN Convention on International Information Security. At the same time, in order to effectively attribute an act, it is important to take into account the political, technical and legal elements of attribution of responsibility.*

DISCUSSION AND CONCLUSIONS. *The article considers approaches to the issue of attribution of attacks in the information space as well as of possible ways of responding to such attacks within the*

framework of current international law. The problem of possible application of international humanitarian law, especially issue of interpretation of "attack" for the purposes of attacks in information space was also examined. In addition, the author analyzes the provisions of the concept of the UN Convention on International Information Security.
The author concludes that current international law is not sufficient for effective attribution of an act committed in the information space. Elaboration of additional international legal regulation that would take into account the particularities of the information space is required. It is also crucial to develop international cooperation in this area, including through the creation of a global register of contact points.

KEYWORDS: *information space, responsibility, attribution of an act, retaliatory measures, register of contact points, international law, the UN Charter, the concept of the UN Convention on International Information Security*

FOR CITATION: Lukiyantseva I.G. The Issue of Attribution of Acts Committed in the Information Space. – *Moscow Journal of International Law.* 2024. No. 4. P. 119–131. DOI: https://doi.org/10.24833/0869-0049-2024-4-119-131

The author declares the absence of conflict of interest.

1. Введение

Начиная с 80-х гг. XX в. наметилась тенденция использования ИКТ в целях, противоречащих Уставу ООН [Berson, Denning 2011:13-15]. Значительное количество подобных атак наряду с угрозами, которые они представляют, повышает риск милитаризации международного информационного пространства. Это связано с тем, что отдельные государства воспринимают информационное пространство прежде всего в качестве арены для утверждения своего геополитического превосходства, разрабатывая не только оборонительный, но и наступательный информационные потенциалы[1]. Государствами регулярно регистрируются случаи атак с использованием ИКТ на критическую инфраструктуру [Котенко, Хмыров 2022:53]. Именно по поводу подобных транснациональных деяний и возникают разногласия между государствами. Ситуация лишь усугубляется возможностью непропорционального применения средств реагирования на угрозы в информационном пространстве.

Следует отметить, что состояние защищенности в указанном пространстве в российской литературе и в официальных документах обозначается как «международная информационная безопасность», в то время как западные государства указывают на необходимость использования понятия «кибербезопасность» [Крутских, Зиновьева 2021:6]. Предпочтительным для целей данной работы представляется использование термина «международная информационная безопасность» ввиду того, что указанное понятие охватывает весь комплекс угроз – как политических, так и технических, в то время как «кибербезопасность» распространяется скорее на их технологическое измерение.

Далее, важно уточнить, какие именно атаки могут восприниматься государствами в качестве угроз. В контексте данного исследования особый интерес представляют целевые (или таргетированные) атаки – мероприятия, осуществляемые лицами с конкретными мотивами и качественной подготовкой, имеющими определенную структуру [Котенко, Хмыров 2022:53-54]. Некоторые технические специалисты приравнивают таргетированные атаки к так называемым продвинутым постоянным угрозам (advanced persistent threats) [Clark 2017:281]. Однако указанный подход представляется не совсем верным ввиду того, что особенностями «продвинутых постоянных угроз» являются высокий уровень подготовки нарушителей, способность постоянно приспосабливаться к защитным мерам и использовать различные направления

[1] UN: Resolution A/RES/78/237 Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies. URL: https://documents.un.org/doc/undoc/gen/n23/430/64/pdf/n2343064.pdf (accessed date: 20.08.2024).

атаки с единым конечным результатом, наличие значительных ресурсов. Отличается и цель подобных «угроз» – данные мероприятия будут реализовываться непосредственно в отношении критической инфраструктуры. Далеко не все целевые атаки способны достигнуть необходимого «порога» [Edwards, Ford, Szappanos 2015:291-299].

Подобные атаки следует отличать от «традиционных» атак в информационном пространстве, представляющих собой более примитивные мероприятия случайного характера с широким радиусом действия, направленные на компрометацию значительного количества систем и пользователей.

С учетом особенностей атак, совершаемых в информационном пространстве (а именно, их анонимного характера, что приводит к отсутствию единой методологии определения нарушителей, критериев квалификации подобных атак как вооруженных нападений, общих принципов для рассмотрения компьютерных инцидентов), все большую актуальность для обеспечения мира и безопасности приобретает вопрос возложения ответственности за подобные деяния.

2. О применимости международного права к информационному пространству

На данном этапе между государствами имеется консенсус относительно применимости общепризнанных принципов международного права (т. е., принципов суверенного равенства, уважения территориальной целостности государств, неприменения силы или угрозы силой, разрешения международных споров мирными средствами, добросовестного соблюдения международно-правовых обязательств и др.) к информационному пространству. В рамках профильных рабочих групп дополнительно были сформулированы акты рекомендательного характера – добровольные правила ответственного поведения государств, а также меры укрепления доверия, направленные на минимизацию риска возникновения конфликтов в информационном пространстве[2]. Ряд государств (прежде всего, США и государства – члены Европейского союза [O'Connell 2012:206-208]) заявляет о достаточности подобного регулирования, для «верификации» которого предлагаются различные несогласованные под эгидой ООН формы отчетности о соблюдении подобных правил (в частности, речь идет о неких руководствах, контрольных списках, опросниках о выполнении правил)[3].

Однако значительным числом государств (в частности, Россией и Китаем [Кулажников 2019:25]) поддерживается идея неспособности существующих правил поведения государств эффективно регулировать существующие отношения в информационном пространстве; подчеркивается, что подобный пробел в регулировании используется в целях предъявления бездоказательных обвинений и применения ответных мер[4].

При этом у многих государств вызывает разногласия вопрос применимости международного гуманитарного права (далее – МГП) к ИКТ. В настоящее время ни один международно-правовой договор не содержит норм, регулирующих «компьютерные войны» или устанавливающих меры, направленные на защиту гражданского населения. Нет пока и соответствующих решений международных судов [Шинкарецкая 2013:120-126]. В промежуточном докладе Группы правительственных экспертов в 2021 г. было отображено содержащееся в ст. 3 Дополнительного протокола I к Женевским конвенциям от 12 августа 1949 г., касающегося защиты жертв международных вооруженных конфликтов от 8 июня 1977 г.[5] (далее – ДП (I)), положение о применимости МГП исключительно в ходе вооруженных

[2] UN: Resolution A/RES/78/237 Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies. URL: https://documents.un.org/doc/undoc/gen/n23/430/64/pdf/n2343064.pdf (accessed date: 20.08.2024).

[3] Выступление российской межведомственной делегации на пятой сессии Рабочей группы открытого состава ООН по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021-2025. URL: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_OEWG_ICT_security_-_statement_-_norms_25.07.2023_-_RUS.pdf (дата обращения: 20.08.2024).

[4] UN: Resolution A/RES/78/237 Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies. URL: https://documents.un.org/doc/undoc/gen/n23/430/64/pdf/n2343064.pdf (accessed date: 20.08.2024).

[5] Дополнительный протокол к Женевским конвенциям от 12 августа 1949 г., касающийся защиты жертв международных вооружённых конфликтов (Протокол I). Женева, 1977. URL: https://www.icrc.org/ru/doc/assets/files/2013/ap_i_rus.pdf (дата обращения: 20.08.2024).

конфликтов, что указывает на невозможность квалификации инцидента в информационном пространстве, произошедшего в мирное время, с точки зрения права вооруженных конфликтов[6].

Однако остается неясным вопрос квалификации вредоносного применения ИКТ как вооруженного нападения в соответствии с МГП и по смыслу ст. 51 Устава ООН. Согласно ст. 51 Устава за государством остается право прибегнуть к военной силе в случае вооруженного нападения до тех пор, пока Совет Безопасности ООН не предпримет шаги по поддержанию мира и безопасности[7], т. е. для активации ст. 51 необходимо выполнение двух условий: 1) наличие вооруженного нападения, 2) достижение атакой порога угрозы миру и безопасности.

Рассмотрим, что может пониматься под нападением. Из содержащегося в ст. 49 ДП (I) определения «нападений» можно сделать вывод о том, что нормы МГП (включая принцип проведения различия и т. д.) применимы только к случаям, которые можно назвать «нападениями» по смыслу этой статьи[8]. В соответствии со ст. 49 ДП (I), «нападения» могут рассматриваться только как «акты насилия в отношении противника»[9]. Нападение во время вооруженного конфликта в его классическом смысле обычно приводит к физическим повреждениям и потерям (физическое разрушение здания, гибель гражданских лиц и т. д.), что далеко не всегда имеет место при проведении операций в информационном пространстве. Таким образом, применимость МГП к операциям, совершаемым в информационном пространстве, равно как и допустимость самообороны, будет во многом зависеть от толкования положений ст. 49 ДП (I).

Здесь можно выделить два подхода к толкованию ст. 49 ДП (I).

1. Согласно широкому толкованию, любая военная операция, которая привела к ущербу (здесь не обязательно будет иметься в виду физический ущерб – достаточно просто прервать бесперебойную работу объекта), может рассматриваться как нападение. Кроме того, Международный Комитет Красного Креста (далее – МККК) в своем толковании вообще не проводит различий по способу проведения нападения. По мнению специалистов МККК, чтобы говорить о наличии нападения в киберпространстве, достаточно установить сам факт такого нападения вне зависимости от характера ущерба[10]. Эту позицию поддерживают некоторые юристы, которые основывают свои рассуждения на положениях ст. 52 Дополнительного протокола (I)[11]. В соответствии со ст. 52 Протокола, одним из способов воздействия на военные цели является «нейтрализация» цели (это не обязательно будут физическое уничтожение или захват цели). Однако подобное толкование с учетом текущей ситуации неопределенности в части возложения ответственности и выбора способа реагирования является неприемлемым, так как в результате ошибочных действий и мер может привести к превращению «жертвы» атаки в информационном пространстве в «агрессора».

2. С другой стороны, согласно узкому толкованию понятия «нападение», операция, чтобы считаться нападением, должна привести к физическому ущербу. Как правило, под физическим ущербом понимается приведение к смерти, причинение вреда лицам либо материальному имуществу [Nicholas 2012:241]. Наиболее очевидным

---

[6] Talking points for the statement by the expert of the Russian Ministry of Defense at the informal intersessional meeting of the UN Open-ended Working Group on Security of and in the Use of Information and Communication Technologies 2021–2025. URL: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Talking_points_for_the_statement_by_the_expert_of_the_Russian_Ministry_of_Defense.pdf (accessed date: 20.08.2024).

[7] ООН: Устав ООН. URL: https://www.un.org/ru/about-us/un-charter/full-text (accessed date: 20.08.2024).

[8] Дополнительный протокол к Женевским конвенциям от 12 августа 1949 г., касающийся защиты жертв международных вооружённых конфликтов (Протокол I). Женева, 1977. URL: https://www.icrc.org/ru/doc/assets/files/2013/ap_i_rus.pdf (дата обращения: 20.08.2024).

[9] Там же.

[10] ICRC: International Humanitarian Law and the Challenges of Contemporary Armed Conflicts. 2011. URL: https://www.icrc.org/en/doc/resources/documents/report/31-international-conference-ihl-challenges-report-2011-10-31.htm?ysclid=likooxoigi770590276 (accessed date: 20.08.2024).

[11] Dörmann K. *Applicability of the additional protocols to computer network attacks. Ed. Byström K. Proceedings of the Conference: Internationsl Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law.* 2004. P. 139-153.

примером такого ущерба, нанесенного операцией в киберпространстве, является смерть пациентов реанимации в больнице в результате нападения на электросеть больницы. Примером может послужить и атака вируса Stuxnet, который вмешался в нормальную работу иранской электростанции и иных промышленных предприятий, что значительно замедлило ядерную программу Ирана [Гаркуша-Божко 2021:67]. Результатом атаки стало именно физическое изменение устройств, в отношении которых осуществлялась атака, вследствие процессов горения и расплавления [Chircop 2019:349, 361]. Подобный случай наглядно демонстрирует, что причиненный атаками в информационном пространстве ущерб может быть сопоставим с ущербом, причиняемым в результате применения оружия[12]. Именно причинение подобного ущерба может быть квалифицировано в качестве угрозы миру и безопасности по смыслу ст. 51 Устава ООН[13]. Данный подход представляется и более гибким, допускающим оценку конкретных обстоятельств (речь идет, в частности, о тяжести наступивших последствий, их направленности, очевидности, а также возможности квалифицировать атаку не *prima facie* как недопустимое применение силы, но также и как просто политическое или экономическое насилие, которое не приветствуется в международном праве, но не запрещено) перед переходом на этап развязывания конфликта [Шинкарецкая 2013:120-126].

Другим аспектом, также вызывающим разногласия, является непосредственно вопрос присвоения деяния в информационном пространстве государству в целом. В международном праве институт международно-правовой ответственности образуется из обычных норм (содержащихся в значительной степени в Статьях Комиссии международного права (далее – КМП) об ответственности государств за международно-противоправные деяния от 2001 г.[14]), а также в отдельных международных договорах. Несмотря на то что Статьи КМП так и не легли в основу международно-правового договора, их значение является крайне важным в связи с отсутствием какого-либо иного универсального соглашения по данному вопросу. Применимость положений Статей в качестве обычных норм подтверждает и практика Международного суда ООН и международных трибуналов[15]. В соответствии со Статьями, деяние:

во-первых, присваивается государству (в частности, за действия органов как механизма, любые действия которого контролируются и подчинены его структуре [Колосов 2014:97]);

во-вторых, является нарушением государством его международно-правового обязательства[16].

Иначе говоря, для получения возможности требовать привлечения государства-«нарушителя» к политической либо материальной ответственности пострадавшему государству будет необходимо установить наличие непосредственной связи между государством и лицом, что, учитывая неприспособленность действующего международного права к реалиям информационного пространства (прежде всего, элементу анонимности) практически невозможно [Красиков 2018:240-241].

Очевидно, что безопасный прогресс в области ИКТ возможно эффективно обеспечить исключительно через формирование полноценного, специального международно-правового режима в информационном пространстве, а не через

[12] Neger G. *Cyberdéfense et droit international: qui veut la paix…préparer la guerre hybride. Village de la justice.* 2024.

[13] Talking points for the statement by the expert of the Russian Ministry of Defense at the informal intersessional meeting of the UN Open-ended Working Group on Security of and in the Use of Information and Communication Technologies 2021–2025. URL: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Talking_points_for_the_statement_by_the_expert_of_the_Russian_Ministry_of_Defense.pdf (accessed date: 20.08.2024).

[14] Статьи КМП об ответственности государств за международно-противоправные деяния. 2001. URL: https://base.garant.ru/2565571/?ysclid=likqpo55v9927953807 (дата обращения: 20.08.2024).

[15] Gabčíkovo-Nagymaros Project (Hungary v. Slovakia). – *International Court of Justice.* URL: https://www.icj-cij.org/case/92 (accessed date: 20.08.2024); Air Service Agreement Case (France v. USA). – *Ad hoc Arbitration.* URL: https://jusmundi.com/en/document/decision/en-air-service-agreement-of-27-march-1946-between-the-united-states-of-america-and-france-decision-saturday-9th-december-1978 (accessed date: 20.08.2024).

[16] ООН. Генеральная Ассамблея: Официальные отчеты пятьдесят шестой сессии. Дополнение No10 (A/ 56/10). Доклад Комиссии международного права. Пятьдесят третья сессия (23 апреля – 1 июня и 2 июля – 10 августа 2001 г.). URL: https://www.un.org/ru/documents/decl_conv/conventions/pdf/responsibility.pdf (дата обращения: 20.08.2024); Статьи КМП об ответственности государств за международно-противоправные деяния. 2001.

простую экстраполяцию норм международного права. Обязательства государств (в том числе касающиеся вопросов ответственности) могут основываться исключительно на нормах международного права, а не на добровольных правилах поведения и тем более не на мерах доверия. Понимание необходимости развития международного права в направлении разработки соответствующих специальных норм юридически обязывающего характера было зафиксировано государствами в профильной резолюции Генеральной Ассамблеи ООН[17], а также в докладах групп правительственных экспертов[18].

Это побуждает государства искать способы применения международного права к информационному пространству в целом, а также пути присвоения вредоносных деяний конкретным государствам.

3. Процедура присвоения деяния в информационном пространстве

В целом, присвоение деяния можно понимать как совокупность мероприятий по поиску виновника нападения для его привлечения к ответственности. Как уже было указано, присвоение деяний в информационном пространстве будет иметь ряд особенностей в связи с особой природой ИКТ, которая может влиять на корректность применения существующих международно-правовых норм к сфере использования ИКТ. Как показывают результаты дискуссий в профильных форматах, не все государства готовы принять это во внимание, что влияет на процесс присвоение деяния на практике.

Процесс присвоения ответственности можно разделить на несколько категорий: речь идет о политическом, техническом и правовом способах [Марков, Ромашкина 2022:59-60]. Идеальной, позволяющей осуществить действительно объективное и всеобъемлющее присвоение деяния, представляется синергия всех трех подходов. Однако в инфополе часто появляются новости о присвоении ответственности и следующих за этим односторонних ограничительных мерах на основе политических мотивов без проведения достаточно глубокого юридического и технического анализа[19]. Более того, отдельные зарубежные специалисты выступают за введение подобных мер в отношении «государств-нарушителей» в информационном пространстве, мотивируя это «невозможностью призвать к ответственности страны с правом вето по ст. 41 Устава ООН»[20].

Для подхода отдельных государств (прежде всего западного блока) характерен некоторый перекос в сторону именно политического метода присвоения деяния. В СМИ и на международных площадках регулярно появляются «вбросы», касающиеся «российской киберагрессии»[21]. Проблема же присвоения деяния как комплексного установления источника атаки обходится стороной. Для подобного декларативного способа присвоения деяния характерна также концепция так называемого коллективного присвоения деяния, согласно которой группа государств получает возможность выносить коллективный вердикт о виновности любого государства в совершении атаки без предъявления каких-либо конкретных доказательств [Крутских, Зиновьева 2021:42].

Аналогичная идея заложена и в американской концепции «выяви и пристыди», заключающейся в «уполномочивании» группы государств автономно определять источник атаки и без предъявления доказательств наносить ответные удары в информационном пространстве [Schmitt 2017:30]. В определенном смысле свое воплощение данная концепция получила в ст. 6 Таллинского руководства, в соответствии с которой государствам вменяется в обязанность проявлять должную степень осмотрительности в целях сохранения своей территории и инфраструктуры таким образом, чтобы она не использовалась для

---

[17] Resolution A/RES/78/237 Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies. URL: https://documents.un.org/doc/undoc/gen/n23/430/64/pdf/n2343064.pdf (accessed date: 20.08.2024);

[18] Report of the open-ended working group on security of and in the use of information and communications technologies 2021-2025. URL: https://documents.un.org/doc/undoc/gen/n22/454/03/pdf/n2245403.pdf (accessed date: 20.08.2024).

[19] Там же.

[20] Etievant C.S. Les sanctions européennes relatives au cyber espace : un arsenal juridique à parfaire? – *Kaufhold and Reveillaud avocats.* 2021.

[21] Выступление российской межведомственной делегации на пятой сессии Рабочей группы открытого состава ООН по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025. Право на ответ. URL: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_OEWG_ICT_security_-__statement_-_right_of_reply_-_RUS.pdf (дата обращения: 20.08.2024).

атак в информационном пространстве, которые могли бы затронуть права иных государств либо приводили бы к «серьезным последствиям» для указанных государств (без указания на то, что может пониматься под «серьезными последствиями») [Schmitt 2017:30]. Ряд исследователей указывает на то, что подобные формулировки, будучи даже нормами общего международного права [Krasikov, Lipkina 2022:362], дают государствам широкие возможности для их толкования применительно к информационному пространству и фактически предоставляют им дополнительные полномочия по применению любых контрмер на основе достаточно субъективного анализа инцидента [Jensen, Watts 2017:1555-1577].

Фокус на политической стороне при присвоении деяния просматривается и в научной литературе. Так, американский исследователь Д.Э. Льюис подчеркивает необходимость «деятельной» реакции на атаку в информационном пространстве, указывая на то, что бездействие со стороны пострадавшего государства позволит нарушителю ощутить свою безнаказанность[22]. Процесс же присвоения деяния он предлагает осуществлять через поиск ответов на такие вопросы, как: чьи интересы преследуются атакой, каковы были публичные заявления субъектов, осуществлял ли потенциальный нападающий уже такие действия ранее. Подобные вопросы характерны именно для «политического» элемента присвоения[23].

Предложенная П.С. Стокбургером концепция по присвоению ответственности также во многом опирается на установление мотивации государства, взаимосвязи между потенциальным государством-нарушителем и совершившим атаку лицом[24].

Подобный однобокий подход может легко привести к эскалации ситуации и способствует не обеспечению принципа мирного урегулирования межгосударственных споров, а, напротив, закреплению «права сильного» в информационном пространстве.

Следует рассмотреть техническую сторону присвоения деяния более предметно.

После инцидента первым шагом является именно технический (криминалистический) элемент присвоения деяния, включающий в себя сбор и оценку технических артефактов (следов) для получения первичного «портрета» злоумышленника и доказательство цели технического элемента присвоения деяния – сбор информации о действиях злоумышленника («знание злоумышленника»).

Технический элемент присвоения деяния осуществляется на основе совокупности признаков, таких как возможная мотивация, интерес к определенным данным, географические признаки (часовые пояса активных действий), сетевые следы (например, IP-адреса), лексика кода (в нем могут содержаться слова либо ошибки в словах, косвенно указывающие на языковую или национальную принадлежность авторов), особенности его написания (нередко национальную принадлежность лиц специалисты определяют на основе качества написанного кода), выбора конкретного алгоритма шифрования и сжатия[25]. В частности, считается, что русскоязычные пишут качественный код со сложными навесными защитами, однако при этом часто делают типичные для носителей русского языка ошибки в английских словах, в то время как китайцы обычно не задумываются о качестве кода и пользуются уже готовыми системными программами. Географический же параметр определяется, как правило, через часовые пояса активных действий нарушителя.

С одной стороны, установить технический элемент присвоения деяния на основе подобных повсеместно известных признаков кажется несложной задачей, способной дать объективный результат. С другой стороны, при присвоении деяния для возложения ответственности на основе артефактов следует учитывать и легкость их имитации не просто для создания поддельного профиля, а с целью именно выступить

[22] Lewis J.A. Creating accountability for global cyber norms. – CSIS. 2022. URL: https://www.csis.org/analysis/creating-accountability-global-cyber-norms (accessed date: 20.08.2024).

[23] Ibid.

[24] Stockburger P.Z. From Grey Zone to Customary International Law: How Adopting the Precautionary Principle May Help Crystallize the Due Diligence Principle in Cyberspace. – *10th International Conference on Cyber Conflict: CyCon X: Maximising Effects*. 2018. P. 245-263.

[25] Гостев А. Основная сложность сейчас – достоверная идентификация источника и организатора атаки. – Коммерсантъ. 2017. URL: https://www.kommersant.ru/doc/3331544?ysclid=m04b7y0mzo998181660 (дата обращения: 20.08.2024).

«под чужим флагом» для имитации атаки другим субъектом. Например, в ходе атаки Duqu 2.0 верхние слои кода были намеренно представлены в виде меток, характерных как для русскоговорящих, так и для китайцев[26].

Безусловно, помимо технического элемента присвоения деяния важно учитывать и политическую, а также правовую. Важным представляется также «публичный» характер присвоения ответственности [Merz 2019:3]. Как уже было указано выше, указанные способы присвоения ответственности имеют целью выявить мотивацию, а также нарушенные нормы.

Однако игнорирование именно «технического» элемента присвоения деяния может, помимо финансового и репутационного ущерба для государства, также привести к эскалации ситуации (когда ошибка в присвоении деяния, повлекшая за собой акт возмездия, приведет, к примеру, к столкновению между государствами, в том числе потенциально обладающими оружием массового уничтожения.

4. О перспективах разработки специальных международно-правовых норм для информационного пространства

Наконец, представляется, что для успешной реализации правового аспекта присвоения деяния (на основе политического и технического элементов) необходимо создание соответствующей, отвечающей специфике информационного пространства международно-правовой основы.

В начале 2023 г. Российская Федерация совместно с группой стран представила обновленную концепцию Конвенции ООН об обеспечении международной информационной безопасности[27]. Будущий договор во многом основывается на положениях из уже одобренных международным большинством профильных резолюций[28].

Новый вариант концепции носит сбалансированный характер, учитывая как подходы государств-сторонников мер доверия, так и стран, выступающих за разработку профильного международного договора.

Среди прочего предлагается включить в Конвенцию положения о:

1) недопущении использования ИКТ в целях подрыва и ущемления суверенитета, нарушения территориальной целостности и независимости государств;

2) интенсификации сотрудничества государств в области международной информационной безопасности для преодоления возникшей в результате инцидентов напряженности (в том числе через создание специальных механизмов);

3) недопустимости бездоказательных обвинений других государств в совершении противоправных деяний с применением ИКТ с последующим принятием различного рода ограничений в виде односторонних мер экономического воздействия и иных способов реагирования;

4) запрете на включение в технологический продукт недекларируемых возможностей;

5) полном и добросовестном исполнении государствами своих обязательств по обеспечению международной информационной безопасности, включая обязательство по добросовестному недопущению совершения негосударственными субъектами международно-противоправных действий в информационном пространстве;

6) недопустимости присвоения деяния в информационном пространстве исключительно по территориальному признаку и необходимости изучения всех артефактов, связанных с инцидентом, особенностей установления ответственности;

7) запрете на использование государствами их территорий для совершения международно-противоправных деяний с использованием ИКТ;

[26] Гостев А. Основная сложность сейчас – достоверная идентификация источника и организатора атаки..

[27] Выступление представителя Российской Федерации на четвертой сессии Рабочей группы открытого состава ООН по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021-2025. 2021. URL: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_OEWG_ICT_security_-_statement_-_norms_25.07.2023_-_RUS.pdf (дата обращения: 20.08.2024).

[28] Обновленная концепция Конвенции ООН об обеспечении международной информационной безопасности. 2023. URL: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/RUS_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian__Federation_0.pdf (дата обращения: 20.08.2024).

8) указании на суверенное право государств самостоятельно обеспечивать безопасность национального информационного пространства, в том числе через принятие соответствующего внутреннего законодательства;

9) обязательстве не наносить ущерб информационным системам групп реагирования на компьютерные инциденты другого государства;

В Концепции особое место уделяется основным принципам международного права в преломлении к вопросам безопасности в информационном пространстве; в частности, подчеркивается суверенное равенство государств, разрешение международных споров мирными средствами, воздержание в международных отношениях от угрозы силой или ее применения.

В будущем договоре планируется закрепить и эффективные механизмы контроля за выполнением участниками его положений.

В существующих же условиях отсутствия профильного международного юридически обязывающего инструмента особое значение приобретает сотрудничество между государствами по данному вопросу [Ивлюшкин 2023:38]. Проблема присвоения атак в информационном пространстве заключается в том, что процесс присвоения деяния является, по сути, комплексом оперативно-разыскных мероприятий. Учитывая трансграничный характер инцидентов в информационном пространстве, успешный поиск истинного организатора и исполнителя атаки возможен исключительно при условии привлечения правоохранительных органов, причем в условиях международной кооперации в расследовании. Именно отсутствие подобного сотрудничества в настоящий момент значительно осложняет расследование, которое может затянуться на годы [Banks 2021:1051].

В данном контексте особую роль в координации между компетентными ведомствами государств в случае инцидентов в информационном пространстве играет наличие постоянно действующих каналов связи и взаимодействия.

Так, в мае 2024 г. по предложению России был произведен официальный запуск глобального межправительственного реестра контактных пунктов (далее – РКП) для обмена информацией о компьютерных атаках/инцидентах[29]. Данная инициатива была согласована консенсусом всеми государствами – членами ООН в рамках Рабочей группы открытого состава по международной информационной безопасности. Указанная мера доверия предполагает создание «службы единого окна», через которую будут осуществляться прямые контакты между уполномоченными ведомствами, а именно, через контактные пункты (дипломатический – Министерство иностранных дел и технический – национальная организация либо группа, ответственная за предотвращение, обнаружение, реагирование и ликвидацию последствий инцидентов в информационном пространстве). Взаимодействие будет выстраиваться на постоянной двусторонней основе по телефонной связи, электронной почте, дипломатическим каналам либо иными желаемыми способами связи, что позволит предотвратить любую возможную эскалацию в результате инцидентов в информационном пространстве, а также обеспечит, при желании сторон, конфиденциальность передаваемых данных. Сотрудничество будет осуществляться в деполитизированном ключе с учетом суверенного решения государств предоставлять данные для реестра; реагировать или нет на соответствующие запросы партнеров; участвовать в учениях; получать адресную помощь в области реагирования на инциденты[30].

Запуск РКП фактически позволил формализовать уже существующие механизмы «джентльменского» взаимодействия между национальными группами реагирования на компьютерные инциденты (CERT и CSIRT), основная проблема которых заключается в отсутствии установленных уполномоченных национальных органов, что нередко приводило к тому, что у запрашивающей стороны не было данных о конкретном адресате, а у стороны-получателя запроса –

[29] Выступления представителя российской делегации А.А. Радовицкого на восьмой сессии Рабочей группы открытого состава ООН по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021-2025. 2024. URL: https://russiaun.ru/ru/news/oewg_0907241 (дата обращения: 20.08.2024).

[30] Выступление представителя Российской Федерации на четвертой сессии Рабочей группы открытого состава ООН по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021-2025. 2023. Реестр контактных пунктов. URL: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/RUS_Russian_statement_PoCs_Directory.pdf (дата обращения: 20.08.2024).

необходимых полномочий для его обработки[31]. Кроме того, учитывая, что национальные группы CERT объединены, например, в международную некоммерческую организацию FIRST, контроль за членством в которой осуществляет США, и региональную сеть групп CSIRT ЕС, сложно говорить о возможности участия в них действительно всех государств[32].

Существуют также региональные инициативы. Речь идет, в частности, о Сети связи Организации по безопасности и сотрудничеству в Европе, Консультативном координационном центре Организации Договора о коллективной безопасности (далее – ОДКБ). Очевидно, что, несмотря на значительный опыт работы у подобных реестров и высокий уровень структурированности функций, их деятельность направлена на конкретный регион и, соответственно, не предоставляет возможность присоединиться всем государствам, заинтересованным в подобном сотрудничестве. Кроме того, со временем стали известны и негативные стороны деятельности указанных реестров. В частности, речь идет о значительной политизации работы реестра ОДКБ, отсутствии взаимодействия между уполномоченными национальными пунктами, а также невозможности обеспечить конфиденциальность передаваемых в его рамках данных[33]. Реестр контактных пунктов же призван стать каналом для непрерывного взаимодействия и оперативной передачи необходимой технической информации об инцидентах действительно для всех желающих государств, что позволит выявлять истинные источники атак и эффективно предотвращать конфликты в информационном пространстве.

5. Заключение

Итак, вопрос присвоения деяния в информационном пространстве не теряет своей актуальности ввиду значительных рисков, которые может нести некорректное определение нарушителя, совершившего атаку. Для всеобъемлющего и объективного присвоения деяния представляется важным учитывать все три элемента – политический, технический и правовой. Необходимо также учитывать особенности информационного пространства, которые могут значительно затруднить присвоение деяния – в частности, речь идет о его анонимности. Между тем, как показывает практика, процесс присвоения деяния остается затруднен ввиду отсутствия на данный момент эффективного международно-правового регулирования указанного вопроса. Подобное регулирование возможно обеспечить через разработку профильного международного договора. Основа для этого имеется – внесенная Российской Федерацией концепция Конвенции ООН об обеспечении международной информационной безопасности. С учетом же отсутствия на данный момент действенного международно-правового регулирования, особое значение приобретают акты рекомендательного характера (в частности, согласуемые профильной РГОС меры доверия), способные обеспечить, в частности, координацию между государствами. Однако единственным способом заполнить пробелы, связанные, в том числе, с вопросами присвоения деяния, остается разработка специальных норм (не исключающая, при этом, параллельное существование добровольных мер по укреплению доверия) [Яникеева 2022:25].

Список литературы

1. Гаркуша-Божко С.Ю. 2021. Международное гуманитарное право в киберпространстве: Ratione materiae, ratione temporis и проблема квалификации кибератак. – *Цифровое право.* Т. 2. № 1. С. 64-82. DOI: 10.38044/2686-9136-2021-2-1-64-82
2. Ивлюшкин А.С. 2023. Применимость норм международного публичного права к обеспечению безопасности в киберпространстве: позиция НАТО. – *Международное сотрудничество евразийских государств: политика, экономика, право.* № 4. С. 32-39.
3. Колосов Ю.М. 2014. Ответственность в международном праве. 2-е изд. Москва: Статут. 222 с.

[31] Разъяснение позиции Российской Федерации по инициативе о создании глобального реестра контактных пунктов. 2022. URL: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/2022_12_04_Explanation_of_position_on_POCs_Directory_-_Russian_Federation_-_Rus.pdf (дата обращения: 20.08.2024).

[32] Выступление представителя Российской Федерации на четвертой сессии Рабочей группы открытого состава ООН по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021-2025. 2023. Реестр контактных пунктов. URL: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/RUS_Russian_statement_PoCs_Directory.pdf (дата обращения: 20.08.2024).

[33] Разъяснение позиции Российской Федерации по инициативе о создании глобального реестра контактных пунктов. 2022.

4. Котенко И.В., Хмыров С.С. 2022. Анализ моделей и методик, используемых для атрибуции нарушителей кибербезопасности при реализации целевых атак. – *Вопросы кибербезопасности.* № 4 (50). С. 52-79. DOI: 10.21681/2311-3456-2022-4-52-79.
5. Красиков Д.В. 2018. Международно-правовая ответственность государств в киберпространстве. – *Государство и право в новой информационной реальности*. Отв. ред. Е.В. Алферова, Д.А. Ловцов. Москва. С. 235-247. DOI: 10.31249/pras/2018.01.11.
6. Крутских А.В., Зиновьева Е.С. 2021. Международная информационная безопасность: подходы России. Москва: МГИМО-Университет. 48 с.
7. Кулажников В.В. 2019. Нормативно-правовое и технологическое обеспечение информационной безопасности КНР. – *Образование и право.* № 7. С. 24-30.
8. Марков А.С., Ромашкина Н.П. 2022. Проблема выявления источника (атрибуции) кибератак – фактор международной безопасности. – *Мировая экономика и международные отношения.* Т. 66. № 12. С. 58-68. DOI: 10.20542/0131-2227-2022-66-12-58-68.
9. Шинкарецкая Г.Г. 2013. Международное право и война в киберпространстве. – *Современное право.* № 8. С. 120-126.
10. Яникеева И.О. 2022. Перспективные направления развития и углубления международного взаимодействия по проблематике международной информационной безопасности. – *Мировая политика*. № 1. С. 23-34. DOI: 10.25136/2409-8671.2022.1.37532.
11. Banks W. 2021. Cyber attribution and State responsibility. – *International law studies.* Vol. 97. P. 1039-1072.
12. Berson T., Denning D. 2011. Cyber warfare. – *Taylon and Francis Journal.* № 9 (5). P. 13-15. DOI:10.1109/MSP.2011.132.
13. Chircop L. 2019. Territorial sovereignty in cyberspace after "Tallinn Manual 2.0". – *Melbourne journal of international law.* Vol. 20. P. 349-377.
14. Clark R. M. 2017. Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level. – *Publ. Springer Cham.* Vol. 3. P. 1-17. DOI:10.1007/978-3-319-32824-9.
15. Edwards S., Ford R., Szappanos G. 2015. Effectively Testing APT Defences: Defining threats, addressing objections to testing and suggesting some practical approaches. – *Virus bulletin conference September.* P. 291-299.
16. Jensen E.T., Watts S.A. 2017. Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer? – *Texas law review.* Vol. 95. P. 1555-1577.
17. O'Connell M. 2012. Cyber security without cyber war. – *Journal of conflict and security law.* № 17 (2). P. 187-209.
18. Merz F. 2019. L'attribution publique d'incidents cybernétiques. – *Politique de securité.* № 244. P.1-4. DOI: 10.3929/ethz-b-000340840.
19. Nicholas T. 2012. Cyber-attacks, self-defense and the problem of attribution. – *Journal of conflict and security law.* Vol. 17. № 2. P. 229-244.
20. Schmitt M.N. 2017. Tallin Manual 2.0. On the International Law Applicable to Cyber Operations. 2nd ed. Cambridge: Publ. Cambridge University Press. P. 1-30. DOI: 10.1017/9781316822524.

References

1. Banks W. Cyber attribution and State responsibility. – *International law studies.* 2021. Vol. 97. P. 1039-1072.
2. Berson T., Denning D. Cyber warfare. – *Taylon and Francis Journal.* 2011. № 9 (5). P. 13-15. DOI:10.1109/MSP.2011.132.
3. Chircop L. Territorial sovereignty in cyberspace after "Tallinn Manual 2.0". – *Melbourne journal of international law.* 2019. Vol. 20. P. 349-377.
4. Clark R. M. Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level. – *Publ. Springer Cham.* 2017.Vol. 3. P. 1-17. DOI:10.1007/978-3-319-32824-9.
5. Edwards S., Ford R., Szappanos G. Effectively Testing APT Defences: Defining threats, addressing objections to testing and suggesting some practical approaches. – *Virus bulletin conference September.* 2015. P. 291-299.
6. Garkusha-Bozhko S.U. Mezhdunarodnoe gumanitarnoe pravo v kiberprostranstve: Ratione materiae, ratione temporis i problema kvalifikacii kiberatak [International humanitarian law in cyberspace: Ratione materiae, ratione temporis and the issue of qualification of cyberattacks]. – *Zifrovoe parvo [Digital law].* 2021. V. 2. № 1. P. 64-82. DOI: 10.38044/2686-9136-2021-2-1-64-82. (In Russ.)
7. Ivlyushkin A.S. Primenimost' norm mezhdunarodnogo publichnogo prava k obespecheniyu bezopasnosti v kiberprostranstve: poziciya NATO. [Application of public international law norms to cybersecurity: NATO position] – *Mezhdunarodnoe sotrudnichestvo evrazijskih gosudarstv: politika, ekonomika, pravo [International cooperation of the Eurasian states: politics, economics, law].* 2023. № 4. P. 32-39. (In Russ.)
8. Jensen E.T., Watts S.A. Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer? – *Texas law review.* 2017. Vol. 95. P. 1555-1577.
9. Kolosov U.M. *Otvetstvennost' v mezhdunarodnom prave [Responsibility in international law].* 2-e izd. Moscow: Statut. 2014. (In Russ.)
10. Kotenko I.V., Hmyrov S.S. Analiz modelej i metodik, ispol'zuemyh dlja atribucii narushitelej kiberbezopasnosti pri realizacii celevyh atak [Analysis of models and techniques used to attribute cybersecurity violators in the implementation of targeted attacks]. – *Voprosy kiberbezopasnosti [Cybersecurity issues].* 2022. № 4 (50). P. 52-79. DOI: 10.21681/2311-3456-2022-4-52-79. (In Russ.)
11. Krasikov D.V. Mezhdunarodno-pravovaya otvetstvennost` gosudarstv v kiberprostranstve. [International responsibility of States in cyberspace]. – *Gosudarstvo i pravo v novoj informacionnoj real`nosti [The state and law in the new information reality].* Ed. E.V. Alferova, D.A. Lovtsov. Moscow. 2018. P. 235-247. DOI: 10.31249/pras/2018.01.11. (In Russ.)
12. Krutskih A.V., Zinov'eva E.S. Mezhdunarodnaja informacionnaja bezopasnost': podhody Rossii [International information security: Russia's approaches]. Moscow: MGIMO-Universitet. 2021. 48 p. (In Russ.)
13. Kulazhnikov V.V. Normativno-pravovoe i tekhnologicheskoe obespechenie informacionnoj bezopasnosti KNR [Regulatory and technological support of information security of the People's Republic of China] – Obrazovanie i pravo [Education and law]. 2019. № 7. P. 24-30. (In Russ.)
14. Markov A.S., Romashkina N.P. Problema vyjavlenija istochnika (atribucii) kiberatak – faktor mezhdunarodnoj bezopasnosti [The problem of identifying the source

(attribution) of cyber-attacks is a factor of international security]. – *Mirovaja jekonomika i mezhdunarodnye otnoshenija [World economy and international relations]*. 2022. Vol. 66. № 12. P. 58-68. DOI: 10.20542/0131-2227-2022-66-12-58-68. (In Russ.)
15. Merz F. L'attribution publique d'incidents cybernétiques. – *Politique de securité*. 2019. № 244. P.1-4. DOI: 10.3929/ethz-b-000340840.
16. Nicholas T. Cyber-attacks, self-defense and the problem of attribution. – *Journal of conflict and security law*. 2012. Vol. 17. № 2. P. 229-244.
17. O'Connell M. Cyber security without cyber war. – *Journal of conflict and security law*. 2012. № 17 (2). P. 187-209.
18. Schmitt M.N. Tallin Manual 2.0. On the International Law Applicable to Cyber Operations. 2nd ed. Cambridge: Publ. Cambridge University Press. 2017. P. 1-30. DOI: 10.1017/9781316822524.
19. Shinkareckaja G.G. Mezhdunarodnoe pravo i vojna v kiberprostranstve [International law and the war in cyberspace]. – *Sovremennoe parvo [Modern law]*. 2013. № 8. P. 120-126. (In Russ.)
20. Yanikeeva I.O. Perspektivnye napravleniya razvitiya i uglubleniya mezhdunarodnogo vzaimodejstviya po problematike mezhdunarodnoj informacionnoj bezopasnosti. [Promising directions for the development and deepening of international cooperation on the issues of international information security]. – *Mirovaya politika [World politics]*. 2022. № 1. P. 23-34. DOI: 10.25136/2409-8671.2022.1.37532. (In Russ.)

Информация об авторе

Ирина Григорьевна ЛУКЬЯНЦЕВА,
соискатель кафедры международного права, Московский государственный институт международных отношений (университет) Министерства иностранных дел России

Вернадского пр-т, д. 76, Москва, 119454, Российская Федерация

ilukiyantseva1@gmail.com
ORCID: 0009-0003-9940-4645

About the Author

Irina G. LUKIYANTSEVA,
Postgraduate student of the International Law Department, Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation

76, Vernadskogo Ave., Moscow, Russian Federation, 119454

ilukiyantseva1@gmail.com
ORCID: 0009-0003-9940-4645