МЕЖДУНАРОДНАЯ БОРЬБА С ПРЕСТУПНОСТЬЮ

DOI: https://doi.org/10.24833/0869-0049-2020-4-23-37

Исследовательская статья
Поступила в редакцию: 06.09.2020
Принята к публикации: 26.11.2020

Владимир Михайлович ШУМИЛОВ
Всероссийская академия внешней торговли Министерства экономического развития
Пудовкина ул., 6А, Москва, 119285, Российская Федерация
info@vavt.ru
ORCID: 0000-0002-5247-6284

Ляйсян Маратовна КРАЙНЮКОВА
Астраханский государственный университет
Татищева ул., 20А, Астрахань, 414056, Российская Федерация
5leska5@mail.ru
ORCID: 0000-0002-4411-6510

РОЛЬ ООН В НОРМАТИВНОМ ПРОТИВОДЕЙСТВИИ ПРАКТИКЕ ТРАНСНАЦИОНАЛЬНЫХ ПРЕСТУПЛЕНИЙ ТЕРРОРИСТИЧЕСКОГО ХАРАКТЕРА В ИНФОРМАЦИОННОЙ СФЕРЕ

ВВЕДЕНИЕ. *В современном мире усиливаются угрозы международной информационной безопасности – применение информационно-коммуникационных технологий в преступных целях. Центром разработки мер противодействия такой практике стала Организация Объединенных Наций. В статье раскрывается роль ООН в формировании нового международно-правового института.*

МАТЕРИАЛЫ И МЕТОДЫ. *Материалом для исследования послужили резолюции ГА ООН, Совета Безопасности ООН, тексты соответствующих международных договоров и проекты договоров, научные труды. Методологическую основу исследования составили традиционные для юридических работ общенаучные и частнонаучные методы познания.*

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ. *В результате проведенного исследования авторы скорректировали утверждающийся в правовой науке взгляд на термин «информационный терроризм», выделили положения резолюций ГА ООН и Совета Безопасности ООН, составляющие нормативную основу противодействия государств преступлениям в информационном пространстве, а шире – использованию информационно-коммуникационных технологий в преступных целях.*

ОБСУЖДЕНИЕ И ВЫВОДЫ. *Авторы обращают внимание, что формирование нового международно-правового института происходит в рамках и под эгидой ООН, преимущественно на основе норм «мягкого» права, однако наступает этап, когда международные рекомендательные нормы постепенно становятся международными договорными нормами, обладающими более жесткой юридической силой.*

КЛЮЧЕВЫЕ СЛОВА: *Организация Объединенных Наций, «информационный терроризм»,*

терроризм, экстремизм, кибертерроризм, информационное пространство, международная информационная безопасность, Глобальная контртеррористическая стратегия ООН, преступления международного характера в информационном пространстве в террористических целях, противодействие использованию информационно-коммуникационных технологий в преступных целях.

ДЛЯ ЦИТИРОВАНИЯ: Шумилов В.М., Крайнюкова Л.М. 2020. Роль ООН в нормативном противодействии практике международных преступлений в информационной сфере в террористических и иных преступных целях. – *Московский журнал международного права.* № 4. С. 23–37. DOI: 10.24833 / 0869-0049-2020-4-23-37

INTERNATIONAL LEGAL MEASURES AGAINST CRIMES

DOI: https://doi.org/10.24833/0869-0049-2020-4-23-37

Research article
Received 06.09.2020
Approved 26.11.2020

Vladimir M. SHUMILOV
Russian Foreign Trade Academy of the Ministry of Economic Development of the Russian Federation
6A, ul. Mosfilmovskaya, Moscow, Russian Federation, 117285
info@vavt.ru
ORCID: 0000-0002-5247-6284

Lyasyan M. KRAJNYUKOVA
Astrakhan State University
20A, ul. Tatishcheva, Astrakhan, Russian Federation, 414056
5leska5@mail.ru
ORCID: 0000-0002-4411-6510

THE ROLE OF THE UN IN NORMATIVE COUNTERACTION TO THE TRANSNATIONAL CRIMES OF TERRORISTIC CHARACTER COMMITTED IN THE INFORMATION SPHERE

INTRODUCTION. *In today's world, threats to international information security are increasing. One of them is the use of information and communication technologies for criminal purposes. The United Nations has become the centre for the development of measures to counter such practices. The article discusses the role of the United Nations in the formation of a new international legal institution.*

MATERIALS AND METHODS. *The study was based on resolutions of the United Nations General Assembly, the United Nations Security Council, the texts of relevant international treaties and draft treaties, and academic writings. The methodological basis of the study was the general scientific and private scientific methods of knowledge which are traditional for legal works.*

RESEARCH RESULT. *As a result of the research, the authors corrected the view of the term "information terrorism" that is being approved in legal science, and highlighted the provisions of UN General Assembly and UN Security Council resolutions that form the normative basis for state 'countering crimes in the information space, and more broadly, the use of information and communication technologies for criminal purposes.*

DISCUSSION AND CONCLUSIONS. *The authors note that the formation of a new international legal in-*

stitution takes place within the framework and under the auspices of the United Nations mainly under the basis of soft law norms. But now a new stage of "switching" is beginning. It is the stage in which the method of developing international recommendatory norms turns to the method of developing international Treaty norms that have a more stringent legal force.

KEYWORD: *United Nations, "information terrorism", terrorism, extremism, cyberterrorism, information space, international information security, UN Global Counter-Terrorism Strategy, transnational crimes in the information space for terrorist purposes, countering the use of information and communication technologies for criminal purposes.*

FOR CITATION: Shumilov V.M., Krajnyukova L.M. The Role of the UN in Normative Counteraction to the International Crimes Committed in the Information Sphere for Terrorist and other Criminal Purposes. – *Moscow Journal of International Law.* 2020. No. 4. C. 23–37. DOI: 10.24833 / 0869-0049-2020-4-23-37

К вопросу о терминах

В первые десятилетия XXI века среди различных видов международного терроризма наиболее заметным и опасным становится так называемый «информационный терроризм», который практикуется как частными структурами, экстремистски настроенными лицами, отдельными средствами массовой информации (СМИ), так и государствами в лице соответствующих органов и спецслужб. Сам термин «информационный терроризм» появился в широком научном обороте относительно недавно и зачастую трактуется неоднозначно [Бураева 2016:139–141; Жаворонкова 2015:30–36; Журавлев 2009:157–169]: с одной стороны, как серьезные преступления в *информационной сфере;* с другой стороны, как серьезные преступления, совершаемые с помощью *информационных технологий* в различных сферах общественно-политического бытия. В первом случае преступные намерения направлены на интернет-среду, интернет-инфраструктуру; во втором – интернет-среда выступает как орудие преступления.

В научной правовой литературе ставится вопрос о соотношении понятий «информационный терроризм» и «кибертерроризм» [Роговский 2007:12]. Иногда между ними ставится знак равенства, часто под «кибертерроризмом» понимают хакерские атаки [Denning 2004], и в таком случае предлагается рассматривать «кибертерроризм» как более узкое понятие.

Несмотря на внешнюю привлекательность и яркую иллюстративность термина «информационный терроризм», возникают вопросы о правомерности использования его в юридической практике – как во внутреннем праве, так и в международно-правовой системе. Практически невозможно выделить целостные, системные признаки и состав преступления под условным названием «информационный терроризм».

В Уголовном кодексе РФ содержится статья 205, в которой приводится состав уголовного преступления «террористический акт», характеризующийся предельной конкретикой: взрыв, поджог и т.п. в целях дестабилизации деятельности органов власти или международных организаций. В состав акта «информационного терроризма» следовало бы включить множество слишком разнородных действий. Равным образом обстоит дело и с «информационным терроризмом международного характера».

Возьмем для примера события в Белоруссии, которые произошли в августе 2020 г. после выборов президента, – направляемую извне информационную агрессию. Как квалифицировать развернувшиеся в сети или исходящие от финансируемых из-за рубежа общественных оппозиционных структур призывы выходить на несанкционированные митинги и марши, устраивать тотальные забастовки, препятствовать службе милиции, блокировать работу государственных (в том числе силовых) ведомств? И все это дополняется подачей искаженной картины событий в мировых и внутренних «независимых» СМИ, угрозой внешнего военного вторжения, индивидуальными санкциями против руководства государства и должностных лиц страны! Аналогичные явления сопровождают почти каждое крупное общественно-политическое событие и в России. Что из этого набора скоординированных действий является именно актом «информационного терроризма»? Оправдано ли вообще использование слова «терроризм», а если оправдано, то во всех ли указанных случаях? Думается, что правильнее и точнее было бы квалифицировать подобные действия как «информационный экстремизм»: деятельность в информационном

пространстве, направленную на насильственную, антиконституционную смену власти, строя, воспрепятствование работе государственных органов, избирательных комиссий, демонстрацию незаконной атрибутики, распространение соответствующих материалов, разжигание ненависти к тем или иным социальным группам, предоставление для всего этого информационных услуг. В российском законе «О противодействии экстремистской деятельности» (2002) к экстремистской деятельности приравнивается и оправдание терроризма, сама террористическая деятельность, а в Уголовном кодексе имеется статья 282.1, касающаяся организации экстремистского сообщества, то есть создания организованных групп лиц для действий, называемых экстремистскими. Понятия «экстремизма», «экстремистской деятельности» оказывается шире, чем понятия «терроризма» и «террористической деятельности», и целый ряд составов преступлений в информационном пространстве легче «вписать» в понятие «экстремизм», чем в понятие «терроризм».

Можно сделать вывод, что термин «информационный терроризм» не является юридически обоснованным и достаточно точным; правильнее было бы акты подобного рода квалифицировать как «преступления в информационном пространстве в террористических целях»; при этом необходим целый кодекс, в котором были бы собраны все составы таких преступлений [Капитонова 2015].

Международный характер подобные преступления приобретают, если исполнители, организаторы следуют руководящим указаниям из-за рубежа или приезжают из другой страны, получают оттуда помощь в любой форме (в форме услуг, финансирования, идеологического прикрытия) или бегут затем в другую страну, просят там убежища [Шхагапсоев 2018].

Значительная, если не преобладающая, часть «преступлений в информационной сфере в террористических целях» носит международный характер. В этих условиях актуальным становится вопрос: как мировое сообщество государств реагирует на данную проблему, носящую глобальный характер? Что предпринимает главная организация – Организация Объединенных Наций – для решения проблемы или хотя бы для координации усилий заинтересованных государств в противодействии практике организации и проведения подобных актов?

С политической точки зрения трудно определить грань между понятиями «информационный терроризм» и «информационная война»: если «информационный терроризм» – это отдельные акты, то «информационная война» – это целое сетевое явление, системно связанные между собой акты; в международных отношениях они направлены на существенные стороны жизни того или иного государства; их еще можно квалифицировать как «информационную агрессию»[1] [Lee S. Strickland 2015:12–17]. Однако ни в одном международном юридическом документе эти понятия пока не встречаются.

В России проблематике терроризма посвящены: Закон о противодействии терроризму (2006); «Концепция противодействия терроризму в Российской Федерации», утвержденная Президентом (2009); Закон о безопасности критической информационной инфраструктуры Российской Федерации (2017). К «преступлениям в информационном пространстве в террористических целях» имеет отношение Закон об информации, информационных технологиях и защите информации (2006); «Доктрина информационной безопасности Российской Федерации», утвержденная Указом Президента (2016).

«Глобальная контртеррористическая стратегия ООН» и другие акты ООН

В деятельности ООН подготовка и принятие актов, касающихся терроризма, как известно, занимает большое место. Наиболее заметными из актов (резолюций ГА ООН, международных договоров, принятых в рамках или под эгидой ООН в конце XX века и в первые десятилетия XXI века) являются: Международная конвенция о борьбе с бомбовым терроризмом (1998); Международная конвенция о борьбе с финансированием терроризма (1999); Международная конвенция о борьбе с актами ядерного терроризма (2005); Конвенция о взаимной правовой помощи и выдаче в целях борьбы с терроризмом (2008)[2] и многие другие. Однако в этих актах нет поло-

[1] При этом следует помнить, что существует Резолюция ГА ООН «Определение агрессии» (1974), и в этой Резолюции не указаны интересующие нас признаки «информационной агрессии».

[2] Международная Конвенция о борьбе с бомбовым терроризмом 1998 г., принятая Резолюцией Генеральной Ассамблеи ООН от 9 января 1998 г. № 52/164. – Документ ООН A/RES/52/164; Международная Конвенция о борьбе с финан-

жений об «информационном терроризме», или о «преступлениях в информационном пространстве в террористических целях». Можно, однако, представить ситуации, в которых нормы конвенций о терроризме могли бы быть истолкованы – по аналогии – применительно к «преступлениям в информационном пространстве в террористических целях» [Лукацкий 2015].

Содержание многих резолюций Генеральной Ассамблеи и Совета Безопасности ООН подтверждает, что становление международного правосознания и международно-правового института борьбы с преступлениями в информационном пространстве идет в тесной привязке к международным актам, касающимся терроризма. Постепенно, от акта к акту, в тексты резолюций добавляются положения, расширяющие взгляд на специфику преступлений в информационном пространстве вообще и в террористических целях – в частности.

Резолюции ГА ООН о преступном использовании *информационных* технологий стали появляться в 2000 г.; позднее была принята серия резолюций о «создании глобальной структуры кибербезопасности». Тогда были официально провозглашены идеи: интернет как площадка для диалога, управление интернетом на международной основе, обеспечение безопасности интернета, право государств определять свои информационные инфраструктуры и др.[3]

В 2006 г. Генеральная Ассамблея приняла Резолюцию A/RES/60/288 «Глобальная контртеррористическая стратегия ООН»[4], подтвердив Декларацию 1994 г. о мерах по ликвидации международного терроризма и ссылаясь на все предыдущие важнейшие резолюции по вопросам терроризма. В тексте Стратегии государства-члены постановили приложить все усилия, чтобы заключить всеобъемлющую конвенцию о международном терроризме. Стратегия состоит из четырех частей: в первой предусмотрены меры по устранению условий, способствующих распространению терроризма; во второй – меры по предотвращению терроризма и борьбе с ним (речь идет, например, о координации усилий государств в борьбе с терроризмом во всех его формах и проявлениях в сети интернет); в третьей – меры по укреплению роли ООН; в четвертой – меры по обеспечению прав человека как основы для борьбы с терроризмом.

В ряде более поздних резолюций Генеральной Ассамблеи ООН положения, касающиеся интернета и различных аспектов информационной среды, развиваются и дополняются. Так, Резолюция ГА ООН A/RES/60/288 «Глобальная контртеррористическая стратегия ООН» (2006) призывает государства сотрудничать с ООН в изучении путей и средств использования сети интернет в качестве инструмента борьбы с распространением терроризма (п. 12 b).

В Резолюции A/66/282 (2012)[5] Генеральная Ассамблея выразила беспокойство по поводу все более широкого использования исполнителями террористических актов новых информационно-коммуникационных технологий (п. 19). Эта же Резолюция призывает государства заключить всеобъемлющую конвенцию о международном терроризме. Понятно, что если дело дойдет до такой конвенции, в ней должны быть положения, посвященные «преступлениям в информационном пространстве в террористических целях».

В Резолюции ГА ООН 68/276 (2014)[6] указывается, что государства не должны позволять неправительственным, некоммерческим и бла-

сированием терроризма 1999 г., принятая Резолюцией Генеральной Ассамблеи ООН от 9 декабря 1999 г. № 54/109. – Документ ООН A/RES/54/109; Международная конвенция о борьбе с актами ядерного терроризма 2005 г., принятая Резолюцией Генеральной Ассамблеи ООН от 13 апреля 2005 г.
№ 59/290. – Документ ООН A/RES/59/290; Конвенция о взаимной правовой помощи и выдаче в целях борьбы с терроризмом 2008 г., принятая на пятой Конференции министров юстиции франкоязычных стран Африки (Рабат, 16 мая 2008 г.). – Документ ООН A/62/939–S/2008/567. Доступ: https://www.un.org/ru/documents/decl_conv/conv_terrorism.shtml (дата обращения: 11.08.2020).

[3] Резолюции Генеральной Ассамблеи ООН. – Информационно-коммуникационные технологии. – Документы ООН. Доступ: https://www.un.org/ru/development/ict/res.shtml (дата обращения 04.09.2020)ю

[4] Глобальная контртеррористическая стратегия ООН / Контртеррористическое Управление – Целевая группа по осуществлению контртеррористических мероприятий. Доступ: https://www.un.org/counterterrorism/ctitf/ru/un-global-counter-terrorism-strategy (дата обращения: 01.09.2019).

[5] Обзор Глобальной контртеррористической стратегии ООН 2012 г., принятой Резолюцией Генеральной Ассамблеи ООН от 29 июня 2012 г. № 66/282. – Документ ООН A/RES/66/282. Доступ: https://undocs.org/ru/A/RES/66/282 (дата обращения 04.09.2020).

[6] Обзор Глобальной контртеррористической стратегии ООН 2014 г., принятой Резолюцией Генеральной Ассамблеи ООН от 13 июня 2014 г. № 68/276. – Документ ООН A/RES/68/276. Доступ: https://undocs.org/ru/A/RES/68/276 (дата обращения 04.09.2020).

готворительным организациям злоупотреблять своим статусом в интересах террористов; именно такие организации зачастую выступают субъектами «преступлений в информационном пространстве в террористических целях». Резолюция призывает государства защищать право неприкосновенности частной жизни в контексте цифровой связи и в условиях борьбы с терроризмом (п. 12), объединить усилия в борьбе с насильственным экстремизмом во всех его формах и проявлениях (п. 24). Ассамблея выразила озабоченность в связи с тем, что террористы и их пособники все шире используют информационно-коммуникационные технологии, прежде всего интернет и другие средства информации, для совершения, подстрекательства, найма исполнителей, финансирования или планирования террористических актов (п. 27).

В Резолюции ГА ООН A/70/291 (2016)[7] отмечено, что практика терроризма создает угрозу территориальной целостности и безопасности государств, дестабилизирует законные правительства. Интересно, что в Резолюции закреплен расширенный взгляд на составы террористической деятельности, в частности указывается, что террористы могут использовать незаконный оборот оружия и наркотиков, незаконную торговлю людьми, культурными ценностями и природными ресурсами, похищение людей, вымогательство, отмывание денег, ограбление банков и другие виды преступлений. Понятие «терроризм» используется наряду с понятием «насильственный экстремизм». Поставлен акцент на цель создания и поддержания в государствах эффективных систем уголовного правосудия. Содержится призыв пересмотреть процедуры и законодательные акты, касающиеся перлюстрации сообщений, их перехвата, сбора личной информации, практики массовой слежки, с тем чтобы обеспечить защиту прав человека. Говорится о необходимости принимать меры, чтобы территории государств не использовались для подготовки или организации террористических актов против других государств или их граждан; изыскивать пути сотрудничества в целях оказания взаимной помощи и привлечения к ответственности лиц, использующих информационно-коммуникационные технологии для террористических целей. Резолюция обращает внимание на то, что террористы с помощью информационно-коммуникационных технологий используют искаженные идеи, в том числе религиозные, для мобилизации ресурсов и сторонников. Генеральная Ассамблея призвала государства принять меры, чтобы законодательно запретить подстрекательство к совершению террористических актов, отказывать в убежище лицам, виновным в таких актах. Все указанные положения Резолюции актуальны и для «преступлений в информационном пространстве в террористических целях», когда происходит использование искаженных идей, подстрекательство к преступным актам, предоставление убежища зачинщикам и подстрекателям.

Кроме того, согласно Резолюции все соответствующие международные организации должны сотрудничать с системой ООН и государствами-членами в том, что касается обмена информацией о физических и юридических лицах, замешанных в террористической деятельности любого рода, в том числе посредством информационных технологий; об их тактике, методах, используемых идеях.

Резолюция ГА ООН A/72/284 (2018)[8] призывает государства к объединению усилий, чтобы «не дать террористам найти безопасные для себя онлайновые зоны», но при этом содействовать функционированию открытого и безопасного интернета. Государствам и соответствующим международным организациям предлагается рассмотреть возможность разработки национальных и региональных планов действий по предупреждению насильственного экстремизма во всех случаях, когда он создает питательную среду для терроризма, а также разработать средства противодействия террористической пропаганде, в том числе через интернет. Контрпропаганда должна утверждать позитивные идеи, давать убедительные альтернативы и освещать вопросы, представляющие интерес для уязвимых групп, являющихся объектами террористической пропаганды. Генеральная Ассамблея

[7] Обзор Глобальной контртеррористической стратегии ООН 2016 г., принятой Резолюцией Генеральной Ассамблеи ООН от 01.06.2016 г. № 70/291. – Документ ООН A/RES/70/291. Доступ: https://undocs.org/ru/A/RES/70/291 (дата обращения 04.09.2020).

[8] Обзор Глобальной контртеррористической стратегии ООН 2012 г., принятой Резолюцией Генеральной Ассамблеи ООН от 26 июня 2018 г. № 72/284. – Документ ООН A/RES/72/284. Доступ: https://undocs.org/ru/A/RES/72/284 (дата обращения 04.09.2020).

обратила внимание на увеличение притока в террористические организации новых членов, завербованных за рубежом. Эта констатация заставляет вспомнить о притоке иностранных граждан с соответствующими намерениями и подготовкой в преддверии и во время «информационной агрессии», в частности и в Белоруссию, в августе 2020 г. после выборов президента страны. Многие положения резолюций ГА ООН повторяются из документа в документ.

В декабре 2019 г. впервые была принята Резолюция ГА ООН о борьбе с киберпреступностью[9], внесенная Россией и рядом государств. За документ проголосовали 79 стран, против – 60, 33 страны воздержались. Против одобрения Резолюции резко выступили Соединенные Штаты Америки, считающие интернет своей «собственностью»; с территории США наиболее интенсивно и агрессивно проводятся кибератаки в отношении информационной инфраструктуры России и многих других стран. Документ предполагает создание Генассамблеей специального межправительственного комитета экспертов, представляющего все регионы, задачей которого станет разработка международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. В МИД России отметили, что предложенная Россией Резолюция фактически закрепляет цифровой суверенитет государств над своим информационным пространством и открывает новую страницу в истории глобального противодействия киберкриминалу. Ранее в Совете Европы была принята кулуарно подготовленная так называемая Будапештская конвенция о преступности в сфере компьютерной информации (2001). Российская Резолюция создает переговорную площадку под эгидой Генеральной Ассамблеи ООН для разработки действительно универсальной конвенции по борьбе с киберпреступностью.[10]

Можно сделать вывод: идет постепенное становление, формирование не только международно-правового института противодействия «преступлениям в информационной сфере в *террористических* целях», но и более широкого института «противодействия использованию информационно-коммуникационных технологий в *преступных* целях». Если первый институт совмещает «киберпространство» и «терроризм», то второй институт – «киберпространство» и все виды международных преступлений (более того, не только «киберпространство», а всё информационное пространство, включая печатные и телевизионные СМИ).

Наряду с Генеральной Ассамблеей, проблематикой терроризма во всех его аспектах занимается и Совет Безопасности ООН. Можно отметить, например, следующие резолюции СБ ООН: № 1373 (2001); 1624 (2005); 2129 (2013); 2178 (2014)[11], в которых содержатся идеи, уже зафиксированные в резолюциях ГА ООН. Вместе с тем можно выделить некоторые положения резолюций СБ ООН, позволяющие увидеть близость понятий «терроризм» и «преступления в информационном пространстве в террористических целях». В ряде резолюций 2015 г. под титулом «Угрозы международному миру и безопасности, создаваемые террористическими актами» (S/RES/2199; S/RES/2249; S/RES/2253; S/RES/2255)[12]

[9] Противодействие использованию информационно-коммуникационных технологий в преступных целях. – Резолюция Генеральной Ассамблеи ООН от 27 декабря 2019 г. № 74/247. – Документ ООН A/RES/74/247. Доступ: https://undocs.org/ru/A/RES/74/247 (дата обращения 04.09.2020).

[10] Зиновьева Е.С. Дипломатическое наступление России в области информационной безопасности. 2018. Доступ: https://mgimo.ru/about/news/experts/diplomaticheskoe-nastuplenie-rossii-v-oblasti-informatsionnoy-bezopasnosti/ (дата обращения: 12.11.2020).

Выступление Министра иностранных дел Российской Федерации С.В. Лаврова в связи с заявлением Президента Российской Федерации В.В. Путина по международной информационной безопасности, Москва, 25.09.2020 [Электронный ресурс Официальный сайт Министерства иностранных дел Российской Федерации]. Доступ: https://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4350560 (дата обращения: 12.11.2020).

[11] Резолюция Совета Безопасности ООН 1373 (2001), принятая на его 4385-м заседании 28 сентября 2001 г. – Документ ООН S/RES/1373 (2001); https://undocs.org/ru/S/RES/1373(2001); Резолюция Совета Безопасности ООН 1624 (2005), принятая Советом Безопасности на его 5261-м заседании 14 сентября 2005 г. – Документ ООН S/RES/1624 (2005); Резолюция 2129 (2013), принятая Советом Безопасности на его 7086-м заседании 17 декабря 2013 г. – Документ ООН S/RES/2129 (2013); Резолюция 2178 (2014), принятая Советом Безопасности на его 7272-м заседании 24 сентября 2014 г. – Документ ООН S/RES/2178 (2014).

[12] «Угрозы международному миру и безопасности, создаваемые террористическими актами» (S/RES/2199; S/RES/2249; S/RES/2253; S/RES/2255). – Документы ООН. Доступ: https://www.un.org/securitycouncil/ru/content/resolutions-adopted-security-council-2015 (дата обращения: 04.09.2020).

говорится об обязанности государств замораживать средства, финансовые активы лиц и соответствующих организаций, которые совершают террористические акты; о том, что государства должны обеспечить, чтобы такие физические лица привлекались к судебной ответственности, а во внутреннем законодательстве – такие террористические акты квалифицировались бы как серьезные уголовные правонарушения. Резолюции с таким же титулом принимались в 2016-2017 гг. и в 2019 г. Ни в одной из них не фигурирует термин «информационный терроризм».

Помимо *нормативной* стороны в деятельности ООН, касающейся противодействия международным преступлениям в информационном пространстве в террористических целях, следует видеть и *институционально-организационную* сторону. Так, в соответствии с Резолюцией Совета Безопасности S/RES/1373 (2001) был учрежден Контртеррористический комитет Совета Безопасности, работу которого направляет Исполнительный директорат[13].

Резолюция была принята на основании главы VII Устава ООН и обязательна для государств – членов ООН. В частности, государства-члены должны:

– ввести уголовную ответственность за финансирование терроризма;

– безотлагательно заблокировать все средства, имеющие отношение к лицам, причастным к актам терроризма;

– не предоставлять ни в какой форме финансовую поддержку террористическим группам;

– запретить предоставление террористам убежища, любых средств или поддержки;

– обмениваться с правительствами других государств информацией о всех группах, осуществляющих или планирующих террористические акты;

– сотрудничать с правительствами других государств в расследовании деятельности, обнаружении, аресте, экстрадиции и уголовном преследовании тех, кто причастен к подобным актам;

– ввести в национальном законодательстве уголовную ответственность за активное и пассивное содействие терроризму и предавать нарушителей суду;

– осуществлять эффективные меры пограничного контроля.

При необходимости все это можно экстраполировать на случаи «преступлений в информационном пространстве в террористических целях». Или еще шире – на все случаи использования информационно-коммуникационных технологий в преступных целях, только, может быть, не в качестве «обязанности», а в качестве «права» государства, реагирующего на информационную агрессию. Из подобных «россыпей» идей и положений постепенно складывается (будет складываться) нормативный массив деклараций и/или конвенций, посвященных противодействию международным преступлениям в информационной сфере.

Резолюцией ГА ООН A/RES/71/291 (2017)[14] учреждено Контртеррористическое управление, которое вобрало в себя полномочия и функции предыдущих структур по осуществлению контртеррористических мероприятий; в состав Управления вошел Контртеррористический центр ООН.

В декабре 2018 г. для сбалансированного осуществления всех частей Глобальной контртеррористической стратегии ООН была создана структура, названная «Глобальным договором ООН по координации контртеррористической деятельности». Участниками Глобального договора стали около 40 подразделений системы ООН, а также Интерпол и Всемирная таможенная организация. Контролирует работу Глобального договора Координационный комитет под председательством заместителя Генерального секретаря ООН и главы Контртеррористического управления. Для связи между структурами Глобального договора создана защищенная онлайновая платформа-портал.

Генеральный секретарь ООН делает регулярные обзоры и доклады[15], касающиеся реализации

[13] Резолюция Совета Безопасности ООН 1373 (2001), принятая на его 4385-м заседании 28 сентября 2001 г. – Документ ООН S/RES/1373 (2001). Доступ: https://undocs.org/ru/S/RES/1373(2001) (дата обращения: 04.09.2020) Контртеррористический комитет и его Исполнительный директорат. Доступ: https://www.un.org/sc/ctc/wp-content/uploads/2015/09/CTED-press-kit-2016-RUSSIAN.pdf (дата обращения: 04.09.2020).

[14] Укрепление потенциала системы Организации Объединенных Наций по оказанию государствам-членам поддержки в осуществлении Глобальной контртеррористической стратегии Организации Объединенных Наций 2017 г., принятой Резолюцией Генеральной Ассамблеи ООН от 15 июня 2017 г. № 71/291. – Документ ООН A/RES/71/291. https://undocs.org/ru/A/RES/71/291 (дата обращения 04.09.2020г.).

[15] Варианты методов оценки воздействия и хода осуществления Глобальной контртеррористической стратегии Организации Объединенных Наций системой Организации Объединенных Наций/ Доклад Генерального секретаря от

Глобальной контртеррористической стратегии и вопросов, связанных с ней. В рамках и под эгидой ООН проводятся разного рода международные мероприятия, конференции: в 2012 г. Целевая группа по осуществлению контртеррористических мероприятий совместно с Управлением ООН по наркотикам и преступности (UNIDOC) выпустила руководство «Использование интернета в террористических целях»[16]; в июле 2015 г. Контртеррористический комитет Совета Безопасности провел специальное совещание с участием государств-членов и соответствующих международных организаций («Мадридское совещание»)[17]; в июне 2018 г. прошла Конференция высокого уровня ООН с участием руководителей контртеррористических ведомств государств-членов.

В связи с этим рождается такое соображение: почему бы дипломатам и специалистам заинтересованных стран постепенно не вести дело к тому, чтобы содержанием деятельности всех названных институциональных органов контртеррористической направленности в ООН (или иных органов/структур) была бы не только борьба с известными мировыми очагами терроризма, но и более отчетливое противодействие практике международных преступлений в информационном пространстве в террористических целях? Возможно, стоит инициировать создание подразделения, которое занималось бы всей проблематикой борьбы с преступлениями экстремистской направленности и уже в этих рамках – организованным противодействием использованию информационно-коммуникационных технологий в преступных целях.

О российском проекте конвенции ООН по борьбе с киберпреступностью

Россия занимает в ООН активную позицию в том, что касается борьбы с терроризмом и с преступлениями в *информационном* пространстве в *террористических* целях, а в более широком плане – с использованием информационно-коммуникационных технологий в *преступных* целях.

В 2011 г. Россия представила в ООН проект Конвенции «Об обеспечении международной информационной безопасности», нацеленный на борьбу с кибертерроризмом, кибермошенничеством и предотвращение конфликтов в киберпространстве[18].

В 2017 г. Министерство связи и массовых коммуникаций РФ разработало проект конвенции ООН по безопасному интернету, учитывающий положения Доктрины информационной безопасности РФ (2016). Проект явился ответом на Будапештскую конвенцию Совета Европы о компьютерных преступлениях (2001), которая во многом устарела: она предусматривает менее десятка составов преступлений, а их на сегодня насчитывается порядка тридцати, считая и кибертерроризм. В российской концепции речь идет о том, чтобы интернет стал частью цифровой экономики, а управление им осуществлялось открыто и демократически всеми государствами на равноправной основе и в соответствии с нормами международного права. Россия стремится закрепить юридически принцип полного контроля государств над их национальными сегментами интернета. Многие положения проекта вошли впоследствии в документы ОДКБ, СНГ, ШОС. Проект был представлен в рамках БРИКС и нашел отражение в одной из деклараций БРИКС [Туронок 2011; Литвинова 2020].

В 2018 г. Генеральная ассамблея ООН приняла Резолюцию «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», содержащую Кодекс ответственного поведения государств в интернете. Проект Резолюции был представлен Российской Федерацией совместно со странами Шанхайской Организации Сотрудничества. Несмотря на ре-

8 мая 2019 г. – Документ ООН A/73/866. Доступ: https://undocs.org/pdf?symbol=ru/A/73/866 (дата обращения 01.09.2020).

[16] Использование интернета в террористических целях. – Руководство ООН / Управление Организации Объединенных Наций по наркотикам и преступности. – Доступ: https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_the_internet_for_terrorist_purposes_Russian.pdf (дата обращения 03.09.2020).

[17] Руководящие принципы в отношении иностранных боевиков-террористов по итогам состоявшегося в Мадриде 27-28 июля 2015 г. специального совещания. – Письмо Председателя Комитета Совета Безопасности, учрежденного резолюцией 1373 (2001) о борьбе с терроризмом, от 15 декабря 2015 года, на имя Председателя Совета Безопасности. – Документ ООН S/2015/939. Доступ: https://www.un.org/sc/ctc/wp-content/uploads/2016/01/N1544887_RU.pdf (дата обращения 04.09.2020).

[18] Конвенция об обеспечении международной информационной безопасности (концепция) от 22.09.2011 г. /Министерство иностранных дел Российской Федерации, официальный сайт. Доступ: https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (дата обращения: 03.09.2020).

комендательный характер данного документа, закрепляемые в нем положения задают общий вектор для разработки универсальной международной конвенции по информационной безопасности. Стоит отметить, что Россия добивалась принятия документа с 1998 г., но активное сопротивление со стороны США и западных коллег фактически препятствовало положительному исходу. Впрочем, консенсус так и не был достигнут, поскольку США и страны Запада выдвинули контррезолюцию с альтернативным сценарием развития международного сотрудничества в данной области [Степанов 2020][19].

В 2019 г., как было указано выше, Генеральная Ассамблея приняла Резолюцию о борьбе с киберпреступностью, инициированную Россией и рядом государств. В 2021 г., как ожидается, начнется работа над будущей конвенцией. Задача осложняется тем, что западные страны преобладают в глобальном информационном пространстве, а США контролируют мировую сеть интернета. Это объясняет те различия в алгоритмах поведения государств и их средств массовой информации, которые наблюдаются при любом крупном событии в любой стране. Запад будет стремиться сохранить свое преимущество в «информационной силе» и продолжит применять ее для достижения геополитических целей, противоречащих международному праву, в частности для вмешательства во внутренние дела других государств и подрыва их публичного порядка.

Нет сомнений, что в проекте будущей конвенции должны быть отражены, судя по текстам указанных выше резолюций и материалов, следующие нормы и принципы, обеспечивающие противодействие киберпреступности в глобальном масштабе:

– признание единства и неделимости глобального информационного пространства, поскольку это общее достояние человечества;

– государства не должны добиваться господства над глобальным информационным пространством;

– информационное пространство государств не должно быть объектом применения информационной силы и вмешательства во внутренние дела;

– государство отвечает за содержание и безопасность своего информационного пространства;

– государства имеют право на защиту своего информационного пространства, информационного суверенитета от вмешательства других государств;

– государства вправе размещать свои информационные средства на территории других государств только на основе добровольных и равноправных договоров;

– государства вправе устанавливать нормы регулирования подконтрольного им сегмента информационного пространства внутренними правовыми актами в соответствии с принципами международного права и взятыми на себя международными обязательствами;

– государство вправе искать и находить баланс между обеспечением (как в глобальном, так и в своем информационном пространстве) соблюдения основных прав и свобод человека и гражданина, с одной стороны, и необходимостью противодействия использованию информационно-коммуникационных технологий в преступных целях, с другой стороны;

– государство вправе ограничивать контент в информационном пространстве, закрывать сайты и при необходимости отключать подконтрольный сегмент интернета в целях противодействия вмешательству во внутренние дела со стороны другого государства и в рамках борьбы с использованием информационно-коммуникационных технологий в преступных целях;

– государства осуществляют международное сотрудничество в деле унификации, гармонизации внутренних норм, касающихся противодействия международным преступлениям в информационном пространстве в *террористических* целях (а в более широком плане – противодействия использованию информационно-коммуникационных технологий в *преступных* целях) [Darrel C. Menthe 1998; Heim M. 1993; Петухов 2008].

Для развития этих и некоторых иных положений, ставших частью международного правосознания общественности многих стран, можно предложить еще несколько идей, которые, возможно, найдут отражение в тексте будущих конвенций по проблематике противодействия использованию информационно-коммуникационных технологий в преступных целях:

[19] Резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности 2018 г.», принятая Генеральной Ассамблеей ООН 5 декабря 2018 г. № 73/27. – Документ ООН A/RES/73/27. Доступ: https://undocs.org/ru/A/RES/73/27 (дата обращения 04.09.2020).

– признать в качестве критически важных объектов инфраструктуры – по аналогии с таким же термином в борьбе с терроризмом[20] – органы власти, управления, силовые ведомства, поддерживающие порядок, крупные государственные информационные центры – СМИ, телевидение. В 2018 г. возглавляемая Интерполом Целевая группа по осуществлению контртеррористических мероприятий приняла Сборник передового опыта по защите критически важных объектов инфраструктуры от террористических атак[21]. От идей и положений этого Сборника можно было бы отталкиваться применительно к «критически важным объектам информационной инфраструктуры». В случае «информационной агрессии» они подлежат особо жесткой защите, что должно быть оформлено нормами внутреннего права (возможно, в рамках противодействия как терроризму, так и экстремизму), а также нормами договорного международного права, например на региональным уровне;

– государства должны стремиться к недопущению и устранению в компьютерных программах «онлайновых темных и серых зон», которые могут быть использованы при организации и осуществлении международных преступлений и преступлений международного характера;

– государства вправе запрещать сбор персональных данных на своей территории (в своем информационном пространстве) госструктурами и частными информационными операторами других стран; государства не будут осуществлять сбор персональных данных в других странах с использованием национальной государственной инфраструктуры;

– при современном состоянии договорных правоотношений, касающихся противодействия использованию информационно-коммуникационных технологий в преступных целях, государства вправе самостоятельно констатировать/квалифицировать факты информационной агрессии или применения двойных стандартов, а также принимать самые жесткие меры в соответствии с внутренним правом (вплоть до ограничения деятельности СМИ, прекращения регистрации неправительственных, некоммерческих организаций, управляемых извне, несущих антигосударственную пропаганду, распространяющих инструкции по дезорганизации общественной жизни);

– следует скорректировать некоторые внутренние материальные и процессуальные нормы, например, возможность признать допустимыми доказательства, собранные с помощью информационно-коммуникационных технологий и социальных сетей; также необходимо внести в уголовные и административные кодексы все составы правонарушений, касающиеся информационных технологий, не забывая и о правонарушениях против отдельных граждан (вымогательство, шантаж и т.п.);

– следует создавать международные организации (в том числе межведомственные, частные профессиональные), которые могли бы осуществлять совместные расследования, вести базы данных, обмениваться доказательствами, отслеживать зачинщиков и подстрекателей, включая тех, кто бежал за рубеж; применять скоординированные меры на территории заинтересованных государств;

– можно и целесообразно использовать метод аналогии при разработке норм, касающихся противодействия использованию информационно-коммуникационных технологий в преступных целях: формулировать новые нормы, отталкиваясь от аналогичных, создававшихся применительно к международному терроризму и международному экстремизму;

– возможно, следовало бы проработать вопрос о начале работы над проектом конвенции против экстремизма в информационном пространстве, или же необходимо усиление этой составляющей в предложенном Россией проекте конвенции о международной информационной безопасности.

---

[20] Резолюция Совета Безопасности ООН 2341 (2017), принятая на его 7882-м заседании 13 февраля 2017 г. – Документ ООН S/RES/2341 (2017). Доступ: https://undocs.org/ru/S/RES/2341(2017) (дата обращения: 04.09.2020)

[21] Защита критически важных объектов инфраструктур от террористических атак: сборник передового опыта. – Руководство ООН/ Контртеррористическое управление ООН (КТУ ООН) Исполнительный директорат Контртеррористического комитета Совета Безопасности ООН (ИДКТК) 2018. Доступ: https://www.un.org/sc/ctc/wp-content/uploads/2019/07/RUS-compendium-final.pdf (дата обращения 03.09.2020)

В сборнике содержатся рекомендации для государств-членов. Несмотря на теоретический характер источника, нельзя не отметить его ключевое значение в обобщении существующих практических стратегий, разрабатываемых и реализуемых государствами в сфере защиты критически важных объектов инфраструктуры от террористических атак и предотвращении актов кибертерроризма.

Заключение и выводы

Как видим, сотрудничество государств в информационном пространстве, и в частности, в противодействии преступлениям террористической, экстремистской направленности (а шире – использованию информационно-коммуникационных технологий в преступных целях), расширяется и развивается, испытывая при этом серьезные противоречия. Угрозы в информационном пространстве нарастают – как на глобальном, так и на региональном уровнях. Можно было бы наряду с термином «информационное пространство» использовать термины: «киберпространство», «цифровое пространство».

Основная работа по формированию общей позиции государств в том, что касается международно-правового регулирования информационной сферы, сосредоточилась в рамках ООН и ее структур. ООН здесь играет центральную, координирующую роль. До настоящего времени в разработке нормативного массива на этом направлении преобладали нормы мягкого права. Вместе с тем следует обратить внимание на нормы актов Совета Безопасности ООН, носящие обязательный характер, а также на факт постепенной трансформации ряда рекомендательных норм резолюций ГА ООН в зачатки международно-правовых обычаев, получающих подкрепление в нормах внутреннего права государств и международных договорных нормах регионального уровня.

Кроме того, можно констатировать, что начался этап «переключения» в международном нормативном регулировании рассматриваемой проблематики с регулирования посредством преимущественно нормами мягкого права на регулирование посредством норм полноценных международных конвенций, тексты которых разрабатываются или подлежат разработке. Идет процесс формирования нового международно-правового института или даже подотрасли права.

Список литературы

1. Борисов Д.А. 2018. Экстремизм и контртеррористическая повестка ООН в XXI веке. – *Мировая политика*. № 1. С. 48–57.
2. Бочарников И.В. 2013. Информационное противодействие терроризму в современных условиях. – *Электронный научный журнал проблем безопасности*. № 3 (21). С. 2-3. Доступ: https://elibrary.ru/item.asp?id=21292041 (дата обращения: 25.09.2020).
3. Бураева Л.А. 2016. Информационный терроризм как угроза национальной безопасности Российской Федерации. – *Пробелы в российском законодательстве*. № 6. С. 139–141.
4. Бураева Л.А. 2017. Кибертерроризм как новая и наиболее опасная форма терроризма. – *Пробелы в российском законодательстве*. № 3. С. 35–37.
5. Дремлюга Р.И. 2017. Кибертерроризм в Китае: уголовно-правовые и криминологические аспекты. – *Всероссийский криминологический журнал*. № 3. С. 607–614.
6. Жаворонкова Т.В. 2015. Использование сети Интернет террористическими и экстремистскими организациями. – *Вестник Оренбургского государственного университета*. № 3 (178). С. 30–36.
7. Журавлев Д.А. 2009. Международный терроризм и СМИ: эволюция коммуникационного взаимодействия. – *Вестник РГГУ. Серия: политология, история, международные отношения. Зарубежное регионоведение, востоковедение*. № 14. С. 157–169.
8. Зиновьева Е.С. 2018. *Дипломатическое наступление России в области информационной безопасности*. – Официальный портал МГИМО. Доступ: https://mgimo.ru/about/news/experts/diplomaticheskoe-nastuplenie-rossii-v-oblasti-informatsionnoy-bezopasnosti/ (дата обращения: 12.11.2020).
9. Капитонова Е.А. 2015. Особенности кибертерроризма как новой разновидности террористического акта. – *Известия ВУЗов. Поволжский регион. Общественные науки. Право*. № 2 (34). С. 29–41.
10. Литвинова Т.Н. 2020. Европейская и российская политики противодействия кибертерроризму (на примере борьбы с «кибер-джихадом»). – *Национальная безопасность*. № 3. С. 32–47. Доступ: https://elibrary.ru/item.asp?id=43863837 (дата обращения: 04.09.2020).
11. Лукацкий А.В. 2015. Кибербезопасность ядерных объектов. – *Индекс безопасности*. № 4 (115). С. 117–130.
12. Петухов В.Б. 2008. Интернет и «информационный терроризм». – *Россия и мусульманский мир*. № 5. С. 176–190.
13. Роговский Е.А. 2007. Россия в борьбе с международным терроризмом: грани повышения позитивного образа страны. – *Россия и Америка в XXI веке. Электронный научный журнал*. № 3. Доступ: http://www.rusus.ru/?act=read&id=66 (дата обращения: 01.09.2020).
14. Степанов О.А. 2020. *Противодействие кибертерроризму в цифровую эпоху. Монография*. М.: Юрайт. 104 с.
15. Тропина Т.Л. 2012. Киберпреступность как новая криминальная угроза. – *Криминология: вчера, сегодня, завтра*. № 1 (24). С. 45–55.
16. Туронок С.Г. 2011. Информационный терроризм: выработка стратегии противодействия. – *Общественные науки и современность*. № 4. С. 131–140.
17. Шхагапсоев З.Л. 2018. Об актуальных вопросах международного сотрудничества в противодействии проявлениям экстремизма и терроризма в Интернет-пространстве. – *Пробелы в российском законодательстве*. № 5. Доступ: https://cyberleninka.ru/article/n/ob-aktualnyh-voprosah-mezhdunarodnogo-sotrudnichestva-v-protivodeystvii-proyavleniyam-ekstremizma-i-terrorizma-v-internet (дата обращения: 03.09.2020).

18. Banks W. 2017. State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0. – *Texas Law Review*. Vol 95 (7). P. 1487–1513. URL: https://texaslawreview.org/state-responsibility-attribution-cyber-intrusions-tallinn-2-0/ (accessed: 02.09.2020).
19. Choi K., Lee C.S. 2018. The Present and Future of Cybercrime, Cyberterrorism and Cybersecurity. – *International journal of Cybersecurity Intelligence and Cybercrime*. P. 1-4. URL: https://www.researchgate.net/publication/328433593_The_Present_and_Future_of_Cybercrime_Cyberterrorism_and_Cybersecurity (accessed: 20.09.2020).
20. Darrel C. Menthe. 1998. Jurisdiction in Cyberspace: A Theory of International Spaces. – n *Michigan Telecommunications and Technology Law Review*. URL: https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1163&context=mttlr (accessed: 02.09.2020).
21. Denning Dorothy E. 2004. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. Georgetown University // Активизм, хактивизм и кибертерроризм: Интернет как средство воздействия на внешнюю политику / перевод Т.Л. Тропиной/ Владивостокский центр исследования организованной преступности. – Владивосток. URL: https://avtonom.org/pub/hacktivism.html (accessed: 05.09.2020)
22. Denning Dorothy E. 2015. *The Rise of Hacktivism*. – Georgetown Journal of International Affairs. Vol. 16 (1). URL: http://journal.georgetown.edu/the-rise-of-hacktivism/ (accessed: 05.09.2020)
23. He Qinglian. 2005. The hijacked potential of China`s Internet. – *Special book preview*. Vol. 2. Issue 2. P. 31–47.
24. Heim M. 1993. *The metaphysics of virtual reality*. Oxford University Press: New York. 175 p.
25. Huey L., Winter E. 2016. #IS_Fangirl: Exploring a New Role for Women in Terrorism. – *Journal of Terrorism Research*. Vol. 7(1). URL: https://www.researchgate.net/profile/Laura_Huey (accessed: 01.09.2020).
26. Lee J., Macdonald S. 2015. What Is Cyberterrorism? Findings from a Survey of Researchers. – *Terrorism and Political Violence*. Vol. 27 (4). P. 657–678.
27. Klein A.G. 2015. Vigilante Media: Unveiling Anonymous and the Hacktivist Persona in the Global Press. – *Communication Monographs*. Vol. 82 (3). P. 379–401.
28. Lee S. 2005. Strickland Information and the War Against Terrorism. – *Bulletin of the American Society for Information Science and Technology*. Vol. 28(2). P. 12–17.
29. Lessig L. 1998. The laws of Cyberspace. Draft. 16 p. URL: http://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf (accessed: 02.09.2020)
30. Morgan S. 2018. Fake news, disinformation, manipulation and online tactics to undermine democracy. – *Journal of Cyber Policy*. Vol. 3(1). P. 39–43.
31. Popham J.F. 2018. Microdeviation: Observations on the Significance of Lesser Harms in Shaping the Nature of Cyberspace. – *Deviant Behavior*. Vol. 29 (2). P. 159–169.

References

1. Borisov D.A. Ekstremizm i kontrterroristicheskaya povestka OON v XXI veke [Extremism and the UN counterterrorism agenda in the 21st century]. – *Mirovaya politika* [World policy]. 2018. No. 1. P. 48–57. (in Russ.).
2. Bocharnikov I.V. Informatsionnoe protivodeistvie terrorizmu v sovremennykh usloviyakh. [Information counteraction to terrorism in modern conditions]. – *Elektronnyi nauchnyi zhurnal problem bezopasnosti [Electronic scientific journal of security problems]*. 2013. No. 3 (21). P. 2-3. URL: https://elibrary.ru/item.asp?id=21292041 (accessed: 25.09.2020) (in Russ.).
3. Buraeva L.A. Informatsionnyi terrorizm kak ugroza natsional'noi bezopasnosti Rossiiskoi Federatsii [Information terrorism as a threat to the national security of the Russian Federation]. – *Probely v rossiiskom zakonodatel'stve [Gaps in Russian legislation]*. 2016. No. 6. P. 139-141 (in Russ.).
4. Buraeva L.A. Kiberterrorizm kak novaya i naibolee opasnaya forma terrorizma [Cyberterrorism as a new and most dangerous form of terrorism]. *Probely v rossiiskom zakonodatel'stve [The gaps in the Russian legislation]*. 2017. No. 3. P. 35–37 (in Russ.).
5. Dremlyuga R.I. Kiberterrorizm v Kitae: ugolovno-pravovye i kriminologicheskie aspekty. – [Cyberterrorism in China: criminal law and criminological aspects]. – *Vserossiiskii kriminologicheskii zhurnal [Russian Journal of Criminology]*. 2017. No. 3. P. 607–614. (in Russ.)
6. Zhavoronkova T.V. Ispol'zovanie seti Internet terroristicheskimi i ekstremistskimi organizatsiyami [Use of the Internet by terrorist and extremist organizations]. – *Vestnik Orenburgskogo gosudarstvennogo universiteta [Bulletin of the Orenburg State University]*. 2015. No. 3 (178). P. 30–36. (in Russ.)
7. Zhuravlev D.A. Mezhdunarodnyi terrorizm i SMI: evolyutsiya kommunikatsionnogo vzaimodeistviya [International terrorism and the media: the evolution of communication interaction.]. – Vestnik RGGU. Seriya: politologiya, istoriya, mezhdunarodnye otnosheniya. Zarubezhnoe regionovedenie, vostokovedenie [RSUH Bulletin. Series: political science, history, international relations. Foreign regional studies, Oriental studies]. 2009. No. 14. P. 157–169 (in Russ.)
8. Zinov'eva E.S. *Diplomaticheskoe nastuplenie Rossii v oblasti informatsionnoi bezopasnosti*. [Russia's diplomatic offensive in the field of information security]. – MGIMO web-site. 2018. URL: https://mgimo.ru/about/news/experts/diplomaticheskoe-nastuplenie-rossii-v-oblasti-informatsionnoy-bezopasnosti/ (accessed: 12.09.2020) (in Russ.)
9. Kapitonova E.A. Osobennosti kiberterrorizma kak novoi raznovidnosti terroristicheskogo akta [Features of cyberterrorism as a new type of terrorist act]. – *Izvestiya VUZov. Povolzhskii region. Obshchestvennyi nauki. [Proceedings of the Universities of the Volga region. Social Sciences. Law]*. 2015. No. 2 (34). (in Russ.)
10. Litvinova T.N. Evropeiskaya i rossiiskaya politiki protivodeistviya kiberterrorizmu (na primere bor'by s «kiber-dzhikhadom»). [European and Russian policies to counter cyberterrorism (on the example of the fight against «cyber-Jihad»)]. – *Natsional'naya bezopasnost' [National security]*. 2020. No. 3. P. 32–47. URL: https://elibrary.ru/item.asp?id=43863837 (accessed: 04.09.2020) (in Russ.)
11. Lukatskii A.V. Kiberbezopasnost' yadernykh ob"ektov [Cybersecurity of nuclear facilities]. – *Indeks bezopasnosti [Security index]*. 2015. No. 4 (115). P. 117–130 (in Russ.)
12. Petukhov V.B. Internet i «Informatsionnyi terrorizm» [Internet and «Information terrorism»]. – *Rossiya i musul'manskii mir [Russia and the Muslim world]*. 2008. No. 5. P. 176–190 (in Russ.)

13. Rogovskij E.A. Rossiya v bor'be s mezhdunarodnym terrorizmom: grani povysheniya pozitivnogo obraza strany [Russia in the fight against international terrorism: the facets of raising the positive image of the country]. – *Rossiya i Amerika v XXI veke. – Elektronnyi nauchnyi zhurnal [Russia and America in the XXI century. – Electronic scientific journal].* 2007. No. 3. URL: http://www.rusus.ru/?act=read&id=66 (accessed: 01.09.2020) (in Russ.)
14. Stepanov O.A. *Protivodeistvie kiberterrorizmu v tsifrovuyu epokhu. Monografiya [Countering cyberterrorism in the digital age. Monograph].* M.: Yurait Publ. 2020. 104 p. (in Russ.);
15. Tropina T.L. Kiberprestupnost' kak novaya kriminal'naya ugroza [Cybercrime as a new criminal threat]. – *Kriminologiya: vchera, segodnya, zavtra [Criminology: yesterday, today, tomorrow].* 2012. No. 1 (24). P. 45–55. (in Russ.)
16. Turonok S.G. Informatsionnyi terrorizm: vyrabotka strategii protivodeistviya sovremennost' [Information terrorism: development of a counteraction strategy]. – Obshchestvennyi nauki i sovremennost' [Social Sciences and modernity]. 2011. No. 4. P. 131–140 (in Russ.)
17. Shkhagapsoev Z.L. Ob aktual'nykh voprosakh mezhdunarodnogo sotrudnichestva v protivodeistvii proyavleniyam ekstremizma i terrorizma v Internet-prostranstve [On topical issues of international cooperation in countering the manifestations of extremism and terrorism in the Internet space]. – *Probely v rossiiskom zakonodatel'stve [The gaps in the Russian legislation].* 2018. No. 5. URL: https://cyberleninka.ru/article/n/ob-aktualnyh-voprosah-mezhdunarodnogo-sotrudnichestva-v-protivodeystvii-proyavleniyam-ekstremizma-i-terrorizma-v-internet (accessed: 03.09.2020) (in Russ.)
18. Banks W. State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0. – *Texas Law Review.* 2017. Vol 95 (7). P. 1487–1513. URL: https://texaslawreview.org/state-responsibility-attribution-cyber-intrusions-tallinn-2-0/ (accessed: 02.09.2020)
19. Choi K., Lee C.S. The Present and Future of Cybercrime, Cyberterrorism and Cybersecurity. – *International journal of Cybersecurity Intelligence and Cybercrime.* 2018. P. 1–4. URL: https://www.researchgate.net/publication/328433593_The_Present_and_Future_of_Cybercrime_Cyberterrorism_and_Cybersecurity (accessed: 20.09.2020).
20. Darrel C. Menthe. Jurisdiction in Cyberspace: A Theory of International Spaces. – n *Michigan Telecommunications and Technology Law Review.* 1998. URL: https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1163&context=mttlr (accessed: 02.09.2020).
21. Denning Dorothy E. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. Georgetown University // Активизм, хактивизм и кибертерроризм: Интернет как средство воздействия на внешнюю политику / перевод Т.Л. Тропиной/ Владивостокский центр исследования организованной преступности. – Владивосток. 2004. URL: https://avtonom.org/pub/hacktivism.html (accessed: 05.09.2020).
22. Denning Dorothy E. The Rise of Hacktivism. – *Georgetown Journal of International Affairs.* 2015. Vol. 16 (1). URL: http://journal.georgetown.edu/the-rise-of-hacktivism/ (accessed: 05.09.2020).
23. He Qinglian. The hijacked potential of China`s Internet. – *Special book preview.* 2005. Vol. 2. Issue 2. P. 31–47.
24. Heim M. *The metaphysics of virtual reality.* Oxford University Press: New York. 1993. 175 p.
25. Huey L., Winter E. #IS_Fangirl: Exploring a New Role for Women in Terrorism. – *Journal of Terrorism Research.* 2016. Vol. 7(1). URL: https://www.researchgate.net/profile/Laura_Huey (accessed: 01.09.2020).
26. Lee J., Macdonald S. What Is Cyberterrorism? Findings from a Survey of Researchers. – *Terrorism and Political Violence.* 2015. Vol. 27 (4). P. 657–678.
27. Klein A.G. Vigilante Media: Unveiling Anonymous and the Hacktivist Persona in the Global Press. – *Communication Monographs*. 2015. Vol. 82 (3). P. 379–401.
28. Lee S. Strickland Information and the War Against Terrorism. – *Bulletin of the American Society for Information Science and Technology.* 2005. Vol. 28(2). P. 12–17.
29. Lessig L. The laws of Cyberspace. Draft. 1998. 16 p. URL: http://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf (accessed: 02.09.2020).
30. Morgan S. Fake news, disinformation, manipulation and online tactics to undermine democracy. – *Journal of Cyber Policy.* 2018. Vol. 3(1). P. 39–43.
31. Popham J.F. Microdeviation: Observations on the Significance of Lesser Harms in Shaping the Nature of Cyberspace. – *Deviant Behavior.* 2018. Vol. 29 (2). P. 159–169.

Информация об авторах

Владимир Михайлович Шумилов,
Заслуженный юрист Российской Федерации, доктор юридических наук, профессор кафедры международного права, Всероссийская академия внешней торговли Министерства экономического развития Российской Федерации

119285, Российская Федерация, г. Москва, ул. Пудовкина, д. 6А.

VShumilov@vavt.ru
ORCID: 0000-0002-5247-6284

About the Authors

Vladimir M. Shumilov,
Honoured Lawyer of the Russian Federation, Doctor of laws, Professor, at the Department of International Law, the All-Russian Academy of Foreign Trade of the Ministry of Economic Development of the Russian Federation

6A, Pudovkin str., Moscow, Russian Federation, 119285

VShumilov@vavt.ru
ORCID: 0000-0002-5247-6284

Ляйсян Маратовна Крайнюкова,
Аспирант, ассистент кафедры международного права, Астраханский государственный университет

414056, Российская Федерация, г. Астрахань, ул. Татищева, 20А

5leska5@mail.ru
ORCID: 0000-0002-4411-6510

Lyasyan M. Krajnyukova,
Postgraduate, Assistant at the Department of International Law, Astrakhan State University

20A, Tatishcheva str., Astrakhan, Russian Federation, 414056

5leska5@mail.ru
ORCID: 0000-0002-4411-6510