УДК 342.727:341.1/8
DOI 10.24147/2542-1514.2020.4(4).80-93

СВОБОДА СЛОВА И ПРАВО НА ДОСТУП К ИНФОРМАЦИИ В УСЛОВИЯХ ФОРМИРОВАНИЯ СИСТЕМЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

К.А. Иванова[1,2], М.Ж. Мылтыкбаев[3]
[1] *Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (РАНХиГС), г. Москва, Россия*
[2] *Тюменский государственный университет, г. Тюмень, Россия*
[3] *МГИМО МИД России, г. Москва, Россия*

Информация о статье
Дата поступления –
19 июля 2020 г.
Дата принятия в печать –
16 ноября 2020 г.
Дата онлайн-размещения –
30 декабря 2020 г.

Ключевые слова
Свобода слова, право на доступ к информации, информационно-коммуникационные технологии, международная информационная безопасность, информационная безопасность, информационные технологии, информационные угрозы, киберугрозы, киберпространство

Исследуется влияние информационно-коммуникационных технологий на современное общество, права и свободы человека и гражданина в киберпространстве с учетом концепций России и США в области формирования системы международной информационной безопасности. Предлагается рассмотреть двойной характер информационно-коммуникационных технологий, возможность их использования в качестве оружия, а также возможные угрозы международному сообществу. Сравнение позиций указанных стран показывает принципиальные расхождения в вопросах свободы слова и доступа к информации, причиной которых являются разные трактовки ключевых понятий, разные оценки возможности нанесения ущерба с помощью информации, а также последствий применения норм международного права к конфликтам с применением информационно-коммуникационных технологий. Сделан вывод о необходимости активного международного сотрудничества и последовательной унификации законодательства различных стран с учетом того, что свобода слова и доступ к информации в киберпространстве должны обладать тем же уровнем защиты, что и в физическом мире.

THE FREEDOM OF SPEECH AND RIGHT OF ACCESS TO INFORMATION IN THE EMERGING SYSTEM OF INTERNATIONAL INFORMATION SECURITY**

Ksenia A. Ivanova[1,2], Madi Zh. Myltykbaev[3]
[1] *Russian Presidential Academy of National Economy and Public Administration (RANEPA), Moscow, Russia*
[2] *University of Tyumen, Tyumen, Russia*
[3] *MGIMO University, Moscow, Russia*

Article info
Received –
2020 July 19
Accepted –
2020 November 16
Available online –
2020 December 30

Keywords
Freedom of speech, right to access information, information and communication technologies,

The subject. The article is devoted to the analysis of the freedom of speech and access to information in the context of the emerging system of international information security.
The purpose of the article is to try to predict the positive and negative consequences of changing international relations in the digital age, to determine the role of freedom of speech and access to information in the context of confrontation between Russia and the United States.
The research presented in this article was carried out by combining different disciplinary approaches, including comparative law, comparative politics and international relations, political theory and sociology. Moreover, study includes methods of dialectical logic, analysis and synthesis, as well as formal legal analysis of international legal acts of the UN.
The main results and scope of their application. The rights of freedom of speech and access to information is undoubtedly one of the main in the global digital communication context.

* Статья выполнена при грантовой поддержке РФФИ, номер проекта № 18-29-16204 мк.
** The article was funded by RFBR according to the research project № 18-29-16204 мк.

ISSN 2658-4050 (Online)

international information security, information security, information technologies, information threats, cyber threats, cyber space

Degree of implementation of human and citizen rights to freedom of expression and access to information are indicators of political processes, the pace of building a civil society and legal state in current country. These rights are the foundation of modern democracy.
The authors carry out a systematic analysis of the categories “freedom of speech” and “the right to access information”, identify the features of implementation of these rights in cyberspace, analyze international practice of legal regulation of these rights and assess the place and role of these rights in the emerging system of international information security. A legal analysis of international legal acts shows that the positions of the United States and the Russian Federation in the field of international information security are gradually converging, and the convergence is going in the direction of the Russian position
Conclusions. The limits on the exercise of freedom of speech and access to information do not correspond to the level of development of public relations, because there are no effective legal tools to prevent defamation in the mass media, which in turn can lead to conflict between countries. It is concluded that there is a need for active international cooperation and consistent unification of the legislation of various countries, taking into account that freedom of speech and access to information in cyberspace should have the same level of protection as in the physical world.

1. Введение

Права и свободы, в том числе свобода слова и право на доступ к информации, не являются неизменной категорией. Это продукт исторического развития общества, они представляют собой социокультурное явление, отражают историческую самобытность народов и стран мира, поэтому каждой правовой системе мира присуща своя юридическая концепция прав и свобод.

В условиях глобальной цифровой коммуникации вопрос о свободе слова и доступа к информации, несомненно, является одним из главных. Так, по степени реализации человеком и гражданином прав на свободу слова и доступа к информации можно судить о происходящих в стране политических процессах, оценить темпы построения гражданского общества и правового государства. Данные права являются фундаментом современной демократии.

Особое значение свобода слова и право доступа к информации приобретают в свете стремительно нарастающих вызовов и угроз в информационной среде в условиях формирования биполярной системы международной информационной безопасности, конфронтации, борьбы за безопасный и стабильный мир. В этих условиях указанные права, призванные служить ядром идейного плюрализма, трансформируются в инструмент пропаганды, организующей противоборство, создающей угрозу международной безопасности, культивирующей атмосферу вражды и ненависти между государствами и народами.

Исходя из этого контекста, рассмотрим вопрос о природе и роли свободы слова и права доступа к информации, в формирующейся системе международной информационной безопасности, значении, придаваемом им субъектами международных отношений.

2. Трансформация свободы слова и права на доступ к информации.

История цивилизации неразрывно связана с историей международных отношений. Образование в 1945 году ООН положило начало современной цивилизации, стало точкой отсчета современного международного права, задавшей вектор развития демократическим правовым социальным государствам, ядром которых является гражданское общество – важнейший элемент социального механизма, обеспечивающий реализацию прав человека. Гражданское общество не будет функционировать без свободы слова и доступа к информации, включающих право создавать средства массовой информации в целях выражения мнений, свободный поиск информации [1, с. 9] и дальнейшее ее распространение, запрет цензуры.

Учитывая изложенное, актуальным для исследования трансформации свободы слова и права на доступ к информации представляется период с момента принятия Всеобщей декларации прав человека в 1948 году и до формирования системы международной информационной безопасности в настоящее время.

Данный период можно поделить на три этапа освоения проблемы свободы слова и доступа к информации.

Первый этап можно условно назвать декларативным. В этот период определяется содержание,

ISSN 2542-1514 (Print)

уточняются формулировки и понятия, и уже к концу «XX века проблематика свободы слова благодаря скрупулезной работе ученых, дипломатов и чиновников превратилась в глубоко проработанную концепцию, изложенную в десятках Конвенций и Деклараций ООН, действие которых не зависит от государственных границ и является универсальным» [2]. Всеобщая декларация прав человека (далее – ВДПЧ) 1948 года стала первым международным документом, закрепившим рассматриваемые права. Так, статья 19 ВДПЧ провозглашает: «Каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ».

Следующим международным актом по времени, но не по значению становится Конвенция о защите прав человека и основных свобод (далее – ЕКПЧ) 1950 года. Статья 10 ЕКПЧ следует за статьей 19 ВДПЧ и добавляет, что осуществление этих свобод «может быть сопряжено с определенными формальностями, условиями, ограничениями или санкциями, которые предусмотрены законом и необходимы в демократическом обществе в интересах национальной безопасности, территориальной целостности или общественного порядка, в целях предотвращения беспорядков или преступлений, для охраны здоровья и нравственности, защиты репутации или прав других лиц, предотвращения разглашения информации, полученной конфиденциально, или обеспечения авторитета и беспристрастности правосудия». Здесь же прописан механизм, предупреждающий злоупотребление указанными ограничениями. В статье 17 разъясняется, что ничто в ЕКПЧ «не может толковаться как означающее, что какое-либо государство, какая-либо группа лиц или какое-либо лицо имеет право заниматься какой бы то ни было деятельностью или совершать какие бы то ни было действия, направленные на упразднение прав и свобод, признанных [в ЕКПЧ], или на их ограничение в большей мере, чем это предусматривается [в ЕКПЧ]».

Международный пакт о гражданских и политических правах (далее – МПГПП) 1966 года является наглядным примером консенсуса в условиях обострившегося идеологического противостояния на международной арене. Формулировки приобретают широкое толкование в МПГПП в силу отсутствия механизма, предупреждающего злоупотребление ограничениями, образуется Комитет по правам человека. Так статье 19 МПГПП устанавливает следующее:

«1. Каждый человек имеет право беспрепятственно придерживаться своих мнений.

2. Каждый человек имеет право на свободное выражение своего мнения; это право включает свободу искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ, устно, письменно или посредством печати или художественных форм выражения, или иными способами по своему выбору.

3. Пользование предусмотренными в пункте 2 настоящей статьи правами налагает особые обязанности и особую ответственность. Оно может быть, следовательно, сопряжено с некоторыми ограничениями, которые, однако, должны быть установлены законом и являться необходимыми:

a) для уважения прав и репутации других лиц;

b) для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения».

Как подчеркивается в пунктах 18 и 19 замечания общего порядка № 34 Комитета по правам человека, свобода выражения мнений включает в себя право на доступ к информации, находящейся в распоряжении государственных органов[1].

Заключительным международным актом первого этапа можно считать Хартию основных прав Европейского Союза 2000 года, статья 11 которой («Свобода выражения мнений и свобода информации») предусматривает, что каждый человек имеет право на свободу выражения мнений, включая свободу придерживаться своих мнений, получать и распространять информацию и идеи без вмешательства государственных органов и независимо от государственных границ. Дополняется, что свобода и плюрализм средств массовой информации должны уважаться.

Второй этап характеризуется развитием правоприменительной практики. На данном этапе происходит калибровка и уточнение пределов реализации

[1] Human Rights Committee, General Comment no. 34, Article 19, Freedoms of opinion and expression, 12 Sept. 2011, CCPR/C/GC/34, paras. 18-19.

свободы слова и права доступа к информации в практике международных и национальных судов. Несмотря на то, что определение соотношения между правами и свободами, с одной стороны, и другими конкурирующими интересами, с другой, является ежедневной функцией национальных и международных судов, по вопросу о свободе слова и доступа к информации однозначно сформулированного ответа нет. Определить пределы свободы выражения мнений в соответствии со статьей 10 ЕКПЧ, особенно трудно, когда речь заходит о предотвращении насилия.

Отметим, что решения европейских судов являются одними из наиболее мотивированных. Естественным образом наибольшее развитие международные нормы получили в практике Европейского суда по правам человека (далее – ЕСПЧ).

Статья 10 ЕКПЧ («Свобода выражения мнения») расширительно толкуется ЕСПЧ, в чьей практике получили закрепление несколько связанных свобод: свобода слова, свобода доступа к информации, свобода распространения информации. Приведем некоторые актуальные примеры судебных дел по вопросам свободы слова (Ali Gürbüz v. Turkey, 52497/08 et al., 12 March 2019[2]; Margulev v. Russia, 15449/09, 8 October 2019[3]), свободы доступа к информации (Rodionov v. Russia, 9106/09, 11 December 2018[4]; Sedletska v. Ukraine, 42634/18[5]), свободы распространения информации (Szurovecz v. Hungary, 15428/16, 8 October 2019[6]; Brisc v. Romania, 26238/10, 11 December 2018[7]).

Также отметим, что для европейской правовой системы вопрос о свободе выражения мнения всегда занимал особое место. Вот несколько примеров рассмотрения в ЕСПЧ споров, связанных с реализацией этой свободы, за один только 2002 год: Dischand and Others v. Austria, 29271/95, 26.02.2002; McVicar v. United kingdom, 46311/99, 07.05.2002; Nikula v. Finland, 31611/96, 21.03.2002 [3, с. 841–846].

Отметим также и тот факт, что, несмотря на то, что практика ЕСПЧ носит субсидиарный характер для национальных юрисдикций, она является «путеводной звездой» в вопросах соблюдения стандартов в области прав человека.

Так, в апреле 2014 года Конституционный суд Турции постановил, что блокирование доступа к Twitter правительством Турции является нарушением свободы выражения мнений в соответствии со статьей 26 Конституции Турции и судебной практикой ЕСПЧ, предусматривающей, что основные права и свободы могут быть ограничены только законом без ущемления их сущности и при условии, что такие ограничения не должны противоречить демократическому строю общества и принципу пропорциональности. В последующем решении Конституционный суд Турции отменил распоряжение турецких властей о блокировании доступа к YouTube основываясь на тех же самых суждениях ЕСПЧ [4, с. 85].

Третий этап характеризуется проникновением во все сферы жизни сети «Интернет» и, как следствие, стремительным ростом количества вызовов и угроз в информационной сфере. Перед международным сообществом встал вопрос о выработке правил поведения. Свобода слова и право на доступ к информации в цифровую эпоху наиболее актуальны и имеют абсолютный приоритет защиты. В современных условиях право на доступ к информации является первичным, так как без информации реализация большинства других прав и свобод оказывается затруднительной. Право на доступ к информации можно рассматривать как право свободного получения и распространения данных и мыслей самостоятельно, то есть без вмешательства государства. В юриспруденции данное право зачастую обозначается как «право знать». Стоит отметить, что это право должно осуществляться не только без вмешательства властей, но и без учета государственных границ.

Несомненно, реализация права «знать», обозначенного в середине прошлого столетия, на практике в полной мере стала возможна только в наше время. Причина этого – быстрое развитие современных информационно-коммуникационных технологий (далее – ИКТ), до появления которых названные права носили лишь декларативный характер.

Стоит отметить, что право на доступ к информации в МПГПП охватывает как получение и распространение информации, так на поиск, использование и распространение данных, в том числе устно,

[2] Ali Gürbüz v. Turkey. URL: https://hudoc.echr.coe.int/eng#{"itemid":["002-12386"]}.
[3] Margulev v. Russia. URL: https://hudoc.echr.coe.int/eng#{"itemid":["002-12617"]}.
[4] Rodionov v. Russia. URL: https://hudoc.echr.coe.int/fre#{"itemid":["002-12250"]}.
[5] Sedletska v. Ukraine. URL: https://hudoc.echr.coe.int/eng#{"itemid":["002-12241"]}.
[6] Szurovecz v. Hungary. URL: https://hudoc.echr.coe.int/eng#{"itemid":["002-12615"]}.
[7] Brisc v. Romania. URL: https://hudoc.echr.coe.int/eng#{"display":[2],"itemid":["002-12251"]}.

письменно, с помощью печати, художественных форм выражения или иных методов по выбору лица.

Без нынешних коммуникационных технологий, средств связи и сети «Интернет» сложно вообразить, как человек смог бы самостоятельно получать и распространять и, тем более, добывать любую информацию настолько легко и свободно. Безусловно, только на основе современных ИКТ могут возникать условия, которые позволяют человеку или обществу в целом реализовать право на доступ к информации. Однако одним из негативных проявлений информатизации стало использование цифрового пространства в террористических и экстремистских целях [5, с. 15].

Исходя из вышеуказанного контекста, свобода слова и право на доступ к информации приобретают особое место в системе международной информационной безопасности. Они являются одновременно и краеугольным камнем складывающихся новых международных отношений, и яблоком раздора, становясь инструментом вмешательства во внутренние дела государств, нарушения суверенных прав народов [6, с. 3].

3. Биполярная система международной информационной безопасности.

Впервые в 1998 году на 53-ей сессии Генеральной Ассамблей ООН (далее – ГА ООН) была принята резолюция, призвавшая государства рассмотреть на международном уровне существующие и возможные угрозы в сфере информационной безопасности. По мнения Секретаря Совета Безопасности Российской Федерации Н.П. Патрушева, «это был первый шаг на пути формирования системы международной информационной безопасности, призванной оказать противодействие угрозам для стратегической стабильности и способствовать равноправному стратегическому партнерству в глобальном информационном пространстве» [7, с. 11].

Проблема обеспечения международной информационной безопасности вывела идеологическое противостояние между странами западной демократии и остальным миром на новый уровень, стала импульсом формирования биполярной системы в данной области. Международное сообщество высказывает опасения в отношении продолжающегося наращивания информационного разрыва, «гонки вооружений» в среде информационно-коммуникационных технологий. Именно этот разрыв и является главной причиной нестабильности и конфликта, который с легкостью может трансформироваться в глобальное противостояние. Информационно-коммуникационные технологии носят трансграничный, глобальный характер, потому требуют специального международного регулирования [8, с. 343].

На сегодня в рамках ООН существует два актуальных подхода к вопросу международной информационной безопасности, которые предложены Россией и США. Данные инициативы привели к поляризации международных отношений.

На сегодняшний день выработка консенсуса между Россией и США в построении международной информационной безопасности является залогом безопасного мира. Сравним данные подходы, определим какая роль отводится свободе слова и праву доступа к информации в них.

4. Оценка роли и значения информационно-коммуникационных технологий на современном этапе исторического развития

Сравнение позиций США и РФ по вопросам формирования международной системы информационной безопасности целесообразно начать с международной оценки роли и значения информационно-коммуникационных технологий в развитии мировой экономики, науки и культуры. В этом вопросе международное сообщество демонстрирует полное единство. Анализ резолюций Генеральной Ассамблеи ООН, докладов правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (1-ый Комитет ООН), докладов Генерального Секретаря ООН однозначно указывают на исключительно важную роль информационно-коммуникационных технологий в формировании современного уровня развития цивилизации[8].

В частности, в резолюциях 74/28 и 74/28ГА ООН от 12 декабря 2019 г. после констатации факта интенсивного развертывания новейших информационных технологий и средств телекоммуникации, подтверждается, что в этом процессе заключаются значительные новые возможности для ускоренного прогресса во всех областях экономики, науки и куль-

[8] Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: Доклад A/65/201 - R - A/65/201. 2010. URL: https://undocs.org/ru/A/65/201; доклад A/70/174 - R - A/70/174. 2015. URL: https://undocs.org/ru/A/70/174; доклад A/68/98 - R - A/68/98. 2013. URL: https://undocs.org/ru/A/68/98 (дата обращения: 25.07.2020).

ISSN 2658-4050 (Online)

туры. При этом также растет потенциал взаимодействия между государствами, направленный на их общее благо[9]. Аналогичные оценки роли информационно-коммуникационных технологий присутствуют в документах не только ООН, но и различных региональных международных объединений: ШОС[10], АСЕАН, ОЭСР [9].

Вывод о единодушном признании всеми странами исключительно важной роли информационно-коммуникационных технологий в дальнейшем развитии глобального сообщества не вызывает сомнений, но необходимо отметить, что международное сообщество столь же едино и в признании существования ряда негативных последствий развития таких технологий [10, с. 85]. Речь идет, прежде всего, о таких относительно новых явлениях, как киберпреступность, кибертерроризм, кибератаки и киберугрозы. В распоряжениях президента США киберугрозы критически важной инфраструктуре признаны одной «из самых серьезных проблем национальной безопасности, с которой нам приходится сталкиваться»[11]. Факты, связанные с перечисленными явлениями, стали привлекать внимание международного сообщества относительно недавно – в период 1990–1996 г.г., но масштабы угроз росли так стремительно, что в 1998 году проблема впервые вошла в повестку ООН[12]. Начиная с 2009 года, в составе этой организации уже работала постоянная «Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности».

В первом же докладе группы зафиксировано, что имеющиеся и возможные угрозы в сфере информационной безопасности следует считать наиболее серьезными проблемами XXI века. Перечень источников таких угроз не поддается определению, их проявлением становится подрывная деятельность против физических и юридических лиц, национальных правительств и инфраструктур. В случае реализации угроз возникает значительный ущерб безопасности и стабильности не только отдельных стран, но и международного сообщества в целом вследствие реакций в глобальной сети. Распространение информационно-коммуникационных технологий неизбежно приводит к появлению новых уязвимостей в критической инфраструктуре и неожиданных вариантов подрывных действий [11, с. 129]. В силу специфики современных телекоммуникаций и сети «Интернет» каждый элемент информационно-коммуникационных технологий может являться источником или объектом высокотехнологичных атак. Более того, специфика этих технологий такова, что не только средства хранения, обработки и передачи информации могут иметь двойное назначение, но средства защиты могут создавать угрозы международному миру и безопасности как в глобальном, так и в национальном масштабе [12, с. 18].

Тезисы о двойном назначении и значительной опасности угроз, возникающих при злонамеренном применении информационно-коммуникационных технологий, уточнялись в каждом докладе Группы правительственных экспертов. В целом, после 2010 года ни одна сессия Генеральной Ассамблеи ООН не завершала свою работу без принятия резолюций, содержащих пункты об угрозах, связанных с применением таких технологий. Если к этому добавить присутствие аналогичных формулировок в документах регионального уровня: постановлениях Совета Европы и Европарламента, Агентства Европейского союза по кибербезопасности и по сертификации кибербезопасности, решениях Варшавского саммита НАТО, документах Межамериканского комитета ОАГ, а также ответах государств – приведенных в Докладе Генерального секретаря ООН[13], то полностью подтверждается вывод о международном признании двойного характера информационно-коммуникационных техноло-

[9] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности A/RES/74/29 - R - A/RES/74/29. 2019. URL: https://undocs.org/ru/A/RES/74/29 (дата обращения: 25.07.2020).

[10] Соглашение между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности». 2009. URL: http://rus.sectsco.org/documents/ (дата обращения: 26.03.2020).

[11] Executive Order - Improving Critical Infrastructure Cybersecurity. URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (дата обращения: 25.07.2020).

[12] О принятии Генассамблеей ООН российской резолюции по международной информационной безопасности – Международная информационная безопасность – Министерство иностранных дел Российской Федерации. URL: https://www.mid.ru/ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/3437775 (дата обращения: 25.07.2020).

[13] Доклад Генерального секретаря Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности A/74/120 - R - A/74/120 [Электронный ресурс]. 2019. URL: https://undocs.org/ru/A/74/120 (дата обращения: 25.07.2020).

гий и значительной опасности связанных с ними угроз [13, с. 127]. Этот вывод, несмотря на его кажущуюся простоту и очевидность, имеет фундаментальное значение для процессов формирования международной правовой системы обеспечения информационной безопасности. Без признания двойного назначения информационно-коммуникационных технологий не может быть поставлен вопрос о правомерности их использования в качестве оружия и квалификации такого применения с позиций соответствующих норм международного права.

Резюмируя все сказанное выше, следует подчеркнуть, что по вопросам роли и значения информационно-коммуникационных технологий, их двойного характера, возможности использования в качестве оружия, связанных с этим угроз в международном сообществе нет сколь-нибудь существенных разногласий. Соответственно, позиции США и России здесь также совпадают, что объясняет наличие идентичных пунктов в проектах резолюций ГА ООН, предлагаемых США и Россией[14]. Разногласия и противоречия появляются на уровне концепций по обеспечению международной и национальной безопасности в условиях глобального применения информационно-коммуникационных технологий.

5. Противоречия в определениях информационной и кибербезопасности, их последствия.

Противоречия между РФ и США в определениях безопасности, связанной с применением информационно-коммуникационных технологий, не имеют отношения к contradictio in adjecto – классической логической ошибке, заключающейся в противоречии между определяемым и определением. Напротив, каждая из сторон предлагает свои достаточно логичные формулировки, но, тем не менее, разница между ними существенна и ведет к далеко идущим последствиям [14, с. 8].

США определяют феномен, известный в РФ как «информационная безопасность», в виде безопасности структур по хранению, обработке и передаче информации (данных) [15]. Соответственно, в федеральном законодательстве США для обозначения данного понятия используется термин «кибербезопасность», относящийся к защите информационных систем от несанкционированного доступа, использования, разрушения, а также защите информации от раскрытия, разрушения, изменения или уничтожения. В федеральном законодательстве США термин «информационная безопасность» (Information Security) также используется, но имеет совершенно другой смысл. Под ним понимается безопасность граждан, обеспечиваемая достаточным уровнем информирования обо всех действиях исполнительной власти[15]. Контроль в этой области обеспечивается специально созданным для этих целей агентством – Information Security Oversight Office (ISOO), тогда как кибербезопасностью занимается Национальный консультативный совет по инфраструктуре (National Infrastructure Advisory Council, NIAC)[16]. Таким образом, в правовой системе США термины «информационная безопасность» и «кибербезопасность» не являются синонимами и относятся к разным явлениям.

Подобный подход имеет важную особенность. Понятие «кибербезопасность» значительно уже «информационной безопасности». Оно охватывает только аспекты работоспособности технической инфраструктуры и целостности передаваемых, хранимых и обрабатываемых данных. Что касается непосредственно данных, то считается, что они не могут быть угрозой, если не наносят ущерба киберструктурам и не приводят к нарушению целостности и установленному порядку обработки других данных. Другими словами, если информация из глобального киберпространства не наносит какого-либо физического или финансового ущерба, то ее распространение не является вредоносным воздействием, а источник такого раскрытия не может быть обвинен в злонамеренных действиях, что соответственно избавляет от риска стать объектом для ответных мер, имеющихся в распоряжении ООН.

Необходимо признать, что аналогичное содержание в понятие «информационная безопасность» вкладывается не только США, но еще целым рядом преимущественно европейских стран. При этом в пользу такой трактовки высказываются доводы, не обусловленные союзническими или политическими соображениями. В частности, в ответе Франции Генеральному секретарю ООН содержатся следующие разъяснения: «Франция не использует термин «информационная безопасность», отдавая предпочтение термину «безопасность информационных си-

[14] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности A/RES/73/27 - R - A/RES/73/27. 2018. URL: https://undocs.org/ru/A/RES/73/27 (дата обращения: 25.07.2020).

[15] About ISOO / National Archives. URL: https://www.archives.gov/isoo/about (дата обращения: 25.07.2020).

[16] National Infrastructure Advisory Council / CISA. URL: https://www.cisa.gov/niac (дата обращения: 25.07.2020).

ISSN 2658-4050 (Online)

стем», или «кибербезопасность». Такой выбор обусловлен тем, что Франция, будучи активной сторонницей свободы выражения мнений в сети «Интернет» (о чем свидетельствует тот факт, что в 2018 году она была соавтором резолюции 38/7 Совета по правам человека[17]), не считает, что сама по себе информация может быть фактором уязвимости, от которого необходимо защищать себя, без ущерба для мер, которые могут быть приняты на пропорциональной и транспарентной основе в условиях, строго определенных правовыми рамками, в соответствии со статьей 19 МПГПП. Кратко смысл такого подхода можно выразить следующим образом: даже непопулярные или разобщающие речи должны защищаться правом на свободу слова [16, с. 294].

Термин «кибербезопасность» является более точным, поскольку он означает способность информационной системы противостоять явлениям из киберпространства, которые ставят под угрозу доступность, целостность и конфиденциальность хранящихся, обрабатывающихся или передающихся данных и связанных с ними услуг, которые имеются в этих системах или к которым эти системы обеспечивают доступ. Кибербезопасность основывается на методах обеспечения безопасности информационных систем и поддерживается за счет борьбы с киберпреступностью и создания системы киберзащиты [17, с. 64].

Такая позиция типична для стран Северной Америки и европейских стран, входящих в Евросоюз. Она не лишена оснований из области международного права, но в то же время дает достаточно аргументов для критики также с позиций международного права. В частности, обращение к пункту b) части 3 той же 19 статьи МПГПП показывает целый набор случаев, когда информация вредна и опасна сама по себе, а ее распространение должно быть ограничено законом. Наглядным примером служит то, что анонимность, предоставляемая системе TOR (The Onion Router), созданной для приватного пользования сетью «Интернет», позволила некоторым преступным группировкам создавать сайты незаконного содержания, предлагающие запрещенные услуги и продукты для продажи. Новое программное обеспечение взаимодействует с сайтами даркнета, такими как Silk Road («Шелковый путь» – анонимная торговая интернет-площадка, большинство продаваемых на ней товаров нелегальны. Наиболее известна как площадка по торговле запрещенными психотропными веществами, которые составляли 70 % от общей массы предлагаемых товаров) [4, с. 86].

Сторонники позиции США настойчиво продвигают свою точку зрения в масштабах международного сообщества. Примером может служить подпункт b) пункта 1 проекта резолюции 74 сессии ГА ООН. В ней государства призываются: «поддерживать осуществление совместных мер, определенных в докладах Группы правительственных экспертов, для рассмотрения угроз, возникающих в этой сфере, и обеспечения открытой, интероперабельной, надежной и безопасной информационно-коммуникационной среды, исходя из необходимости сохранить свободный поток информации»[18].

Конечно, не стоит забывать о том, что сеть «Интернет» изначально и создавалась именно для свободного, трансграничного обмена информацией, а само право свободного выражения идей и мнений является одними из базовых, основополагающих и общепризнанных прав человека и гражданина. Право свободно выражать свое мнение включает право получать и распространять информацию и идеи без какого-либо вмешательства со стороны публичных властей и независимо от государственных границ, а также предполагает возможность выразить свое мнение и сообщить его, как совокупность информации, другому субъекту, у которого, в свою очередь, возникает право эту информацию получить [18, с. 141]. 9 марта 2015 года Парламентское Управление по науке и технике (The Parliamentary Office of Science and Technology – POST), консультирующее Парламент Великобритании, опубликовало доклад под названием «Даркнет и онлайн-анонимность», в котором говорится, что запрет на онлайн анонимность сети будет «технологически неосуществимым» и контрпродуктивным. Если бы запрет был наложен, анонимная сеть, такая, как Tor Hidden Services (THS), просто добавила бы секретные узлы входа или «мосты», которые «очень трудно заблокировать». В докладе также сказано, что анонимная сеть используется не только в преступных целях, но и в целях защиты общественных

[17] Резолюция, принятая Советом по правам человека 5 июля 2018 г. «Поощрение, защита и осуществление прав человека в Интернете». URL: https://undocs.org/pdf?symbol=ru/A/HRC/RES/38/7.

[18] Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности. Проект резолюции A/C.1/74/L.49/Rev.1 - R - A/C.1/74/L.49/Rev.1. 2019. URL: https://undocs.org/ru/A/C.1/74/L.49/Rev.1 (дата обращения: 25.07.2020).

ISSN 2542-1514 (Print)

интересов, таких, как информирование, журналистика, правоохранительные расследования и обход цензуры в сети Интернет [4, с. 86].

В контексте данной статьи представляется важным отметить использование в проекте резолюции термина «информационно-коммуникационная среда» вместо традиционного для позиции США термина «киберпространство». Такое изменение вполне может трактоваться как «дрейф» в сторону более соответствующей современной реальности позиции РФ. Однако ключевым элементом данного пункта проекта резолюции является не изменение терминологии, а требование сохранения свободного потока информации. Именно эта часть гарантирует защиту любого контента, отправляемого государством в суверенную часть информационно-коммуникационной среды другого государства. Присутствие такого положения в Резолюциях ГА ООН позволит США не поддерживать меры против государств, транслирующих с помощью информационно-коммуникационных технологий контент, направленный на дестабилизацию обстановки в других государствах. Кроме того, и это представляется крайне важным, такой подход избавляет США в дальнейшем не только от осуждения, но даже от рассмотрения действий, предпринимаемых против других государств в информационно-коммуникационной среде. Позиция, при которой главным является свободный поток информации, в правовом смысле «развязывает руки» для ведения в информационной среде действий, не совместимых с поддержанием мира и стабильности [19, с. 191]. Единственным условием легитимности таких действий (опять же, по мнению США и их союзников) остается отсутствие ущерба киберструктурам. В отношении этого условия необходимо отметить, что оно не является сколь-нибудь сложным и непреодолимым препятствием. Во-первых, ущерб сложно доказать (Россия последовательно требует не допускать бездоказательных обвинений), а во-вторых, нанесение такого ущерба особенно в отношении критической инфраструктуры целесообразно только в случае открытого конфликта с применением силы. В других случаях, как свидетельствует международный опыт, для дестабилизации достаточно специально подготовленного контента, направляемого в информационную среду с помощью информационно-коммуникационных технологий [20].

Позиция РФ также в значительной мере обусловлена содержанием, вкладываемым в понятие «информационная безопасность». В соответствии с принятой Доктриной информационной безопасности Российской Федерации это понятие определяется как «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие» [21]. В соответствии с таким определением любые действия в суверенной части информационного пространства, ведущие к перечисленным последствиям, следует считать направленными против информационной безопасности страны. Это в свою очередь дает государству право на ответные меры адекватного характера, поскольку суверенитет и следующие из него международные нормы и принципы распространяются на деятельность, связанную с информационно-коммуникационными технологиями, и на соответствующую инфраструктуру, расположенную на территории государства, а значит, на них распространяется и юрисдикция государства[19]. Более того, в таких случаях теоретически возможно обращение в Совет безопасности ООН, поскольку современные угрозы международному миру и безопасности не обязательно связаны с применением вооруженных сил. В соответствии со статьей 39 Устава Организации Объединенных Наций определение любой угрозы миру находится в пределах полномочий Совета Безопасности ООН. СБ ООН уже признал, что угрозы в «экономических, социальных, гуманитарных и экологических областях» могут рассматриваться как угрозы международному миру и безопасности [22].

Далее обозначим важный момент, в значительной мере раскрывающий сущность российской позиции в области международной информационной безопасности. Информационные атаки и ответные меры означают наличие конфликта, и вероятность таких конфликтов нарастает[20]. Предотвращение подобных конфликтов – важнейшая задача международного сообщества. Для ее решения необходимы

[19] Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности A/RES/73/266 - R - A/RES/73/266. 2018. URL: https://undocs.org/ru/A/RES/73/266 (дата обращения: 25.07.2020).

[20] Доклад Первого комитета Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности A/74/363 - R - A/74/363. 2019. URL: https://undocs.org/ru/A/74/363 (дата обращения: 25.07.2020).

обоснованные меры по предупреждению конфликтных ситуаций в информационном пространстве. Российская трактовка понятия «международная информационная безопасность» дает ясный ответ на данный вопрос. В частности, государства, применяя информационно-коммуникационные технологии, должны не допускать ущерба информационным системам других государств, вмешательства во внутренние дела других государств путем генерации и трансляции контента, несущего угрозы, содержащего враждебную пропаганду и оскорбления[21]. В целом же, государства должны соблюдать ряд правил ответственного поведения в информационном пространстве. Такие требования и правила уже созданы и закреплены в Резолюции ГА ООН RES/73/27от 5 декабря 2018 г. Любое государство может присоединиться к ним на добровольной основе. С тем, что соблюдение таких правил снижает риск возникновения конфликтов, согласны даже противники российской позиции, что подтверждается Резолюцией ГА ООН RES/74/27 от 12.12.2019.

В настоящий момент соблюдение Правил ответственного поведения государств в сфере использования информационно-коммуникационных технологий (далее – Правила) не является международной правовой нормой, в связи с чем представляют интерес перспективы изменения их статуса и реакция экспертного сообщества на такие изменения. С целью ознакомления гражданского общества с мнениями экспертного сообщества Управление ООН по вопросам разоружения (United Nations Office for Disarmament Affairs, UNODA) подготовило материал «Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology A Commentary», содержащий комментарии более чем 40 экспертов по всем тринадцати пунктам Правил. Анализ комментариев показывает, что возражения касаются, главным образом, неясно сформулированного статуса Правил. В настоящий момент их положения могут выполнить роль добровольных стандартов поведения государств, но при некоторой доработке, сопровождаемой изменениями в национальных законодательствах, они могут быть восприняты как правовая норма [22].

Позиции России и США допускают применение ответных мер на информационные угрозы. В этой связи сразу же встает вопрос об отношении международного сообщества к таким действиям и ответным мерам. Разумеется, международное сообщество в лице ООН должно в таких случаях руководствоваться положениями соответствующих разделов международного права, поэтому остается актуальным вопрос о применимости существующего международного права к обеспечению информационной безопасности. Данный вопрос представляет не только академический интерес, но и имеет важнейшее практическое значение. В случае положительного ответа – к конфликтам в информационной среде становятся применимы существующие конвенции, действующие в отношении случаев применения вооруженной силы. Нарушение их требований будет являться нарушением международного права, а при некоторых обстоятельствах – и военным преступлением со всеми вытекающими последствиями. В связи с этим вопрос применимости существующих норм международного гуманитарного права к действиям в информационном пространстве представляется исключительно важным в целом и представляет интерес в контексте данной статьи. Последнее обусловлено тем, что именно трактовка информационной безопасности и формулировки ее основных положений будут служить основой для квалификации действий с применением информационно-коммуникационных технологий.

6. Применимость существующего международного права к обеспечению информационной безопасности

После продолжительного периода дискуссий, следуя рекомендациям Группы правительственных экспертов, международное сообщество признало применимость существующего международного права к обеспечению международной информационной безопасности. Между тем до его практического применения еще далеко, поскольку требуется доработка существующих норм и создание ряда новых положений. Создаваемая система международного правового обеспечения информационной безопасности в условиях глобального трансграничного информационного пространства (киберпространства) должна опираться на базовые принципы, заложенные в Уставе ООН. Это может быть реализовано различными способами, поэтому в научной литературе, посвященной этому вопросу, предлагаются различные подходы. Так, крупнейший специалист в области развития Интернета, руководитель и создатель «Дипло Фоундейшн» Йован Курбалийа, описывая част-

[21] Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности A/RES/74/28 - R - A/RES/74/28. 2019. URL: https://undocs.org/ru/A/RES/74/28 (дата обращения: 25.07.2020).

ISSN 2542-1514 (Print)

ный случай взаимодействия отдельных граждан в киберпространстве, говорит о «реальном» праве, в котором «Интернет» следует считать техническим явлением, развитием предшествующих технологий коммуникации. Безусловно, сеть «Интернет» быстрее и масштабнее, но это, по-прежнему, один из способов общения между людьми. Следовательно, любые существующие правовые нормы могут применяться и по отношению к сети «Интернет».

Интернет обладает огромным потенциалом для развития. Он обеспечивает беспрецедентный объем ресурсов для информации и обмена знаниями, что открывает новые возможности для выражения гражданами своего мнения и участия в управлении государственными делами [23, с. 471]. При этом возникает следующее противоречие. С одной стороны, принцип свободы выражения мнений в контексте развития прав человека должен применяться к развитию демократии, в том числе посредством Интернет-среды. С другой стороны, свободный поток информации ведет к угрозе свободного оборота потенциально опасной информации, в том числе экстремистской, а также к возможности влияния на общественное мнение путем внедрения в сеть пропаганды [24].

7. Заключение

Исследование документов ООН показывает, что позиции США и РФ в области международной информационной безопасности постепенно сближаются, причем сближение идет в сторону российской позиции. В настоящий момент резолюции ГА ООН, инициируемые США концептуально совпадают по многим пунктам с резолюциями, вносимыми Россией. Однако при этом остаются принципиальные расхождения, вытекающее из разных трактовок понятий «информационная безопасность», «информационная угроза», следовательно, возникают разные подходы к смысловому наполнению свободы слова и доступа к информации. США и ряд иных стран на уровне международных документов не признают того факта, что информация сама по себе может нести угрозу государствам и международному миру даже без нанесения физического ущерба киберструктурам и целостности данных. Вследствие этого США критикуют или одобряют меры безопасности в зависимости от их влияния на свободу распространения потоков информации. Тем не менее, принятие резолюции ГА ООН RES/73/27 с пунктом против распространения фальшивых или искаженных сообщений показывает, что у российской позиции становится все больше сторонников.

Таким образом, сеть «Интернет» имеет существенное влияние на общественную сферу, следовательно, свобода слова и доступ к информации в киберпространстве должны обладать тем же уровнем защиты, что и в физическом мире. Пределы реализации свободы слова и права доступа к информации, на наш взгляд, не соответствует уровню развития общественных отношений, так как присутствует возможность развязывания войны в информационном поле под предлогом защиты свободы слова и свободного доступа к информации. Невозможно также администрировать запрещенную информацию, например, Google признал, что «невозможно отфильтровать весь контент, связанный с терроризмом, поскольку примерно каждую минуту около 300 часов видеоматериалов загружается в YouTube»[22]. За скобками остается вопрос, кто должен давать правовую оценку спорным материалам? Если это будут делать компетентные органы, это автоматически приведет к необоснованному росту бюрократических барьеров, что в любом обществе вызывает раздражение и недопонимание.

Отсутствие эффективных правовых инструментов, позволяющих не допускать диффамации в массмедиа, является серьезным индикатором проблем в области обеспечения полноценной реализации гражданами в полном объеме свободы слова и права на доступ к информации, построения стабильной и равноправной системы международной информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Литвак Н.В. Информационные процессы в современной дипломатической службе: опыт Франции / Н.В. Литвак. – М.: МГИМО-Университет, 2016. – 486 с.

2. Дзялошинский И.М. Особенности коммуникативного поведения в киберпространстве / И.М. Дзялошинский // Проблемы взаимодействия языка и мышления. – М.: Интеллект-Центр, 2010. URL: http://www.dzyalosh.ru/02-01-Auditoriya-Media/Kiberprostranstvo.pdf (дата обращения: 10.07.2020).

[22] Google: Impossible to filter all YouTube 'terror' // Al Jazeera, 28 Jan. 2015.

3. Путеводитель по прецедентной практике Европейского Суда по правам человека. 2002–2016 / науч. ред. и сост. Ю.Ю. Берестнев. – М.: Развитие правовых систем, 2016. – 1288 с.

4. Kittichaisaree K. Public International Law of Cyberspace / K. Kittichaisaree. – Springer International Publishing, 2017. – 376 p. – DOI: 10.1007/978-3-319-54657-5.

5. Судиев И.Ю. Теория и практика информационного противодействия экстремистской и террористической деятельности: монография / И.Ю. Судиев, А.А. Смирнов, А.И. Кундетов, В.П. Федотов. – М.: Полиграф-Книга, 2014. – 240 с.

6. Колосов Ю.М. Массовая информация и международное право / Ю.М. Колосов. – М.: Статут, 2014. – 160 с.

7. Международная информационная безопасность: Теория и практика: В трех томах. Том 1: Учебник для вузов / под общ. ред. А.В. Крутских. – М.: Аспект Пресс, 2019. – 384 с.

8. Роговский Е.А. Кибер-Вашингтон: глобальные амбиции / Е.А. Роговский. – М.: Международные отношения, 2014. – 848 с.

9. Болгов Р.В. Деятельность ООН в области информации и международные аспекты информационной безопасности России / Р. Болгов // Сравнительная политика. – 2018. – Т. 10, № 1. – С. 59–69.

10. Смирнов А.И. Современные информационные технологии в международных отношениях: монография / А.И. Смирнов. – М.: МГИМО-Университет, 2017. – 334 с.

11. Floridi L. The 4-th revolution: how the infosphere is reshaping human reality / L. Floridi. – New York, Oxford University Press, 2014. – 248 p.

12. Саликов М.С. Права человека в сети Интернет: коллективная монография / М.С. Саликов, С.Э. Несмеянова, А.Н. Молчанов, Н.Е. Колобаева, К.А. Иванова. – Екатеринбург: Изд-во УМЦ УПИ, 2019. – 148 с.

13. Стратегия коммуникации в цифровую эпоху. Новые технологии: учебное пособие / под. ред. Л.С. Сальниковой. – М.: Издательский дом «Научная библиотека», 2019. – 300 с.

14. Грошиков К.К. Социально значимая информация и ее уголовно-правовая охрана: монография / К.К. Грошиков. – М.: Юрлитинформ, 2011. – 144 с.

15. Карасев П. Стратегия информационной (кибер) безопасности США в XXI веке / П. Карасев // Вестник Московского университета. Серия 12. Политические науки. – 2013. – № 3. – С. 89–102.

16. Как принести права человека домой: защита человека в национальных и международных инстанциях / под ред. А.Л. Буркова. – М.: Известия, 2018. – 400 с.

17. Информационно-коммуникационные технологии третьего тысячелетия: учебное пособие / под ред. П.В. Меньшикова. – М.: МГИМО-Университет, 2020. – 460 с.

18. Mounk Y. The people vs. democracy. Why our freedom is in danger and how to save it / Y. Mounk. – Cambridge: Harvard University Press, 2018. – 393 p.

19. Democracy at Large - NGOs, Political Foundations, Think Tanks, and International Organizations / ed. by B. Petric. – New York, Palgrave Macmillan, 2012. – 280 p.

20. Лебедева М. «Мягкая сила»: понятие и подходы / М. Лебедева // Вестник МГИМО-Университета. – 2017. – Т. 3(54). – С. 212–223.

21. Молчанов Н.А. Доктрина информационной безопасности Российской Федерации (новелла законодательства) / Н.А. Молчанов, Е.К. Матевосова // Актуальные проблемы российского права. – 2017. – С. 159–165. – DOI: 10.17803/1994-1471.2017.75.2.159-165.

22. Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology A Commentary / ed. by E. Tikk. – New York, United Nations Publication, 2017. – 280 p.

23. The handbook of Global Security Policy / ed. by M. Kaldor, I. Randelov. – Chichester, Wiley Blackwell, 2014. – 541 p.

24. Hoffman B. Inside terrorism / B. Hoffman. – New York, Columbia University Press, 2017. – 494 p.

REFERENCES

1. Litvak N.V. Information processes in the modern diplomatic service: the experience of France. Moscow, MGIMO-University Publ., 2016. 486 p. (In Russ.).

2. Dzyaloshinsky I.M. Features of communicative behavior in cyberspace, in: Problems of interaction of language and thinking. Moscow, Intellect Center Publ., 2010. Available at: http://www.dzyalosh.ru/02-01-Auditoriya-Media/Kiberprostranstvo.pdf (accessed on 10.07.2020). (In Russ.).

3. Berestnev Yu. Yu. Guide to the case law of the European Court of Human Rights. 2002-2016. Moscow, Razvitie pravovykh system Publ., 2016. 1288 p. (In Russ.).

4. Kittichaisaree K. Public International Law of Cyberspace. Springer International Publishing, 2017. 376 p. DOI: 10.1007/978-3-319-54657-5.

5. Sudiev I. Yu., Smirnov A. A., Kundetov A. I., Fedotov V. P. Theory and practice of information counteraction to extremist and terrorist activities. Moscow, Polygraph-Book Publ., 2014. 240 p. (In Russ.).

6. Kolosov Yu.M. Mass information and international law. Moscow, Statut Publ., 2014. 160 p. (In Russ.).

7. Krutskikh A.V. (ed.). International information security: Theory and practice. Volume 1. Moscow, Aspect Press, 2019. 384 p. (In Russ.).

8. Rogovskiy E.A. Cyber-Washington: global ambitions. Moscow: Mezhdunarodnye otnosheniya Publ., 2014. 848 p. (In Russ.).

9. Bolgov R. UN Activities in the field of information and international aspects of information security in Russia. *Sravnitel'naya politika = Comparative politics*, 2018, vol. 10, no. 1, pp. 59-69. (In Russ.).

10. Smirnov A.I. Modern information technologies in international relations. Moscow, MGIMO-University Publ., 2017. 334 p. (In Russ.).

11. Floridi L. The 4-th revolution: how the infosphere is reshaping human reality. New York, Oxford University Press, 2014. 248 p.

12. Salikov M.S., Nesmeyanova S.E., Molchanov A.N., Kolobaeva N.E., Ivanova K.A. Human Rights in the Internet. Yekaterinburg: UPI Publishing house, 2019. 148 p. (In Russ.).

13. Salnikova L.S. (ed.). The communication strategy in the digital age. New technologies. Moscow, Scientific library Publ., 2019. 300 p. (In Russ.).

14. Groshikov K.K. Socially significant information and its criminal-legal protection. Moscow, Yurlitinform Publ., 2011. 144 p. (In Russ.).

15. Karasev P. Strategy of information (cyber) security of the USA in the XXI century. *Vestnik Moskovskogo universiteta. Seriya 12. Politicheskie nauki = Moscow University Bulletin. Series 12. Political Science,* 2013, no. 3, pp. 89-102. (In Russ.).

16. Burkov A.L. (ed.). How to bring human rights home: human protection in national and international institutions. Moscow, Izvestiya Publ., 2018. 400 p. (In Russ.).

17. Menshikov P.V. (ed.). Information and communication technologies of the third Millennium. Moscow, MGIMO-University Publ., 2020. 460 p. (In Russ.).

18. Mounk Y. The people vs. democracy. Why our freedom is in danger and how to save it. Harvard University Press, 2018. 393 p.

19. Petric B. (ed.). Democracy at Large - NGOs, Political Foundations, Think Tanks, and International Organizations. New York, Palgrave Macmillan, 2012. 280 p.

20. Lebedeva M. "Soft power": the concept and approaches. *Vestnik MGIMO-Universiteta = MGIMO Review of International Relations,* 2017, vol. 3, pp. 212-223. (In Russ.).

21. Molchanov N.A., Matevosova E.K. Information Security Doctrine of the Russian Federation (new legislation). *Aktual'nye problemy rossiiskogo prava = Actual problems of the Russian law,* 2017, pp. 159-165. DOI: 10.17803/1994-1471.2017.75.2.159-165. (In Russ.).

22. Tikk E. (ed.). Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary. New York, United Nations Publication, 2017. 280 p.

23. Kaldor M., Randelov I. The handbook of Global Security Policy. Chichester, Wiley Blackwell, 2014. 541 p.

24. Hoffman B. Inside terrorism. New York, Columbia University Press, 2017. 494 p.

ISSN 2658-4050 (Online)

ИНФОРМАЦИЯ ОБ АВТОРАХ

Иванова Ксения Алексеевна – кандидат юридических наук, [1]директор научно-образовательного Центра местного самоуправления, [2]доцент кафедры конституционного и муниципального права
[1] *Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (РАНХиГС)*
[2] *Тюменский государственный университет*
[1] 119571, Россия, г. Москва, пр. Вернадского, 84
[2] 625003, Россия, г. Тюмень, ул. Володарского, 6
E-mail: ivanova-ka@ranepa.ru
SPIN-код РИНЦ: 6610-9218; AuthorID: 695216

Мылтыкбаев Мади Женискалиевич – аспирант кафедры международного права
МГИМО МИД России
119454, Россия, г. Москва, пр. Вернадского, 76
E-mail: myltykbaev@my.mgimo.ru
ORCID: 0000-0003-3261-9927
ResearcherID: AAA-3864-2019
SPIN-код РИНЦ: 6952-1510; AuthorID: 1028441

INFORMATION ABOUT AUTHORS

Ksenia A. Ivanova – PhD in Law; [1] Director of the Center of Local Authorities of the Institute of Management and Regional Development; [2] Associate Professor, Department of Constitutional and Municipal Law
[1] *Russian Presidential Academy of National Economy and Public Administration (RANEPA)*
[2] *University of Tyumen*
[1] 84, Vernadskogo pr., Moscow, 119571, Russia
[2] 6, Volodarskogo ul., Tyumen, 625003, Russia
E-mail: ivanova-ka@ranepa.ru
RSCI SPIN-code: 6610-9218; AuthorID: 695216

Madi Zh. Myltykbaev – post-graduate student, International Law Department
MGIMO University
76, Vernadskogo pr., Moscow, 119454, Russia
E-mail: myltykbaev@my.mgimo.ru
ORCID: 0000-0003-3261-9927
ResearcherID: AAA-3864-2019
RSCI SPIN-code: 6952-1510; AuthorID: 1028441

БИБЛИОГРАФИЧЕСКОЕ ОПИСАНИЕ СТАТЬИ

Иванова К.А. Свобода слова и право на доступ к информации в условиях формирования системы международной информационной безопасности / К.А. Иванова, М.Ж. Мылтыкбаев // Правоприменение. – 2020. – Т. 4, № 4. – С. 80–93. – DOI: 10.24147/2542-1514.2020.4(4).80-93.

BIBLIOGRAPHIC DESCRIPTION

Ivanova K.A., Myltykbaev M.Zh. The freedom of speech and right of access to information in the emerging system of international information security. *Pravoprimenenie = Law Enforcement Review*, 2020, vol. 4, no. 4, pp. 80–93. DOI: 10.24147/2542-1514.2020.4(4).80-93. (In Russ.).