СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ
SIBERIAN FEDERAL UNIVERSITY

ПРОСПЕКТ СВОБОДНЫЙ – 2022

Материалы XVIII Международной конференции
студентов, аспирантов и молодых ученых

Красноярск, 25–30 апреля 2022 г.

Электронное издание

Красноярск
СФУ
2022

СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ
SIBERIAN FEDERAL UNIVERSITY

PROSPECT SVOBODNY – 2022

Materials of the XVIII International Conference students, graduate students and young scientists

Krasnoyarsk, April 25–30, 2022

Electronic publication

Krasnoyarsk
SibFU
2022

Министерство науки и высшего образования Российской Федерации
Сибирский федеральный университет

ПРОСПЕКТ СВОБОДНЫЙ – 2022

Материалы XVIII Международной конференции
студентов, аспирантов и молодых ученых

Красноярск, 25–30 апреля 2022 г.

Электронное издание

Красноярск
СФУ
2022

УДК 001.891(03)
ББК 72.5я21
П827

Ответственный за выпуск Лесняк Татьяна Александровна

П827 **Проспект Свободный – 2022** : материалы XVIII Междунар. конференции студентов, аспирантов и молодых ученых. Красноярск, 25–30 апреля 2022 г. [Электронный ресурс] / отв. за вып. Т. А. Лесняк. – Электрон. дан. (62,4 Mb). – Красноярск : Сиб. федер. ун-т, 2022. – 3002 с. – Систем. требования : PC не ниже класса Pentium I ; 128 Mb RAM ; Windows 98/XP/7/8/10 ; Adobe Reader V8.0 и выше. – Загл. с экрана.

ISBN 978-5-7638-4702-4

Представлены результаты научной работы студентов, аспирантов и молодых ученых.

Предназначены для студентов различных направлений и специальностей, аспирантов, научных работников и преподавателей.

Электронный вариант издания
см.: http://catalog.sfu-kras.ru

УДК 001.891(03)
ББК 72.5я21

ISBN 978-5-7638-4702-4

Электронное научное издание

Подписано в свет 19.08.2022. Заказ № 16577
Тиражируется на машиночитаемых носителях

Библиотечно-издательский комплекс
Сибирского федерального университета
660041, г. Красноярск, пр. Свободный, 82а
Тел. (391) 206-26-16; http://bik.sfu-kras.ru
E-mail: publishing_house@sfu-kras.ru

Ministry of Science and Higher Education of Russian Federation
Siberian Federal University

PROSPECT SVOBODNY – 2022

Materials of the XVIII International Conference
students, graduate students and young scientists

Krasnoyarsk, April 25–30, 2021

Electronic publication

Krasnoyarsk
SibFU
2022

UDC 001.891(03)
LBC 72.5я21
П827

Responsible for edition Tatiana A. Lesnyak

П827 **Prospect Svobodny – 2022** : *materials of the XVIII International Conference students, graduate students and young scientists*. Krasnoyarsk, April 25–30, 2022 [Electronic resource] / edit. S. K. Franchuk. – Electronic data (62,4 Mb). – Krasnoyarsk : SibFU, 2022. – 3002 p. – Hardware requirements : PC Pentium I or higher ; 128 Mb RAM ; Windows 98/XP/7/8/10 ; Adobe Reader V8.0 or higher.

ISBN 978-5-7638-4702-4

The proceedings include results of research by undergraduate, graduate, postgraduate and PhD students.

The edition is aimed at students of difference specializations, PhD students, scholars and university professors.

UDC 001.891(03)
LBC 72.5я21

ISBN 978-5-7638-4702-4

Electronic publication

Signed 19.08.2022. Order 16577

Library and Publishing Center of Siberian Federal University

660041 Krasnoyarsk, Svobodny avenue, 82a
Тел. (391) 206-26-16; http://bik.sfu-kras.ru
E-mail: publishing_house@sfu-kras.ru

УДК 341.1/8

Е. С. Калинина[1],
С. Е. Фомина[2],
В. В. Терешкова[3], канд. юрид. наук., доц. (научный консультант)
[1,2] *Санкт-Петербургский государственный университет*,
[3] *Сибирский федеральный университет*

РАСПРОСТРАНЕНИЕ ДЕЗИНФОРМАЦИИ: ВОЗМОЖНО ЛИ ПРИВЛЕЧЬ ГОСУДАРСТВО К ОТВЕТСТВЕННОСТИ?

Под «дезинформацией» понимается недостоверная или вводящая в заблуждение информация и/или контент, которая распространяется с целью повлиять на действия или выбор граждан [1]. Дезинформация часто составляется таким образом, что при первом прочтении напоминает заслуживающее доверия сообщение. Хотя она уже давно используется в политических целях, стремительное развитие социальных сетей привело к расширению возможности таких операций. Кроме того, благодаря Интернету, дезинформация (в письменной форме, в виде изображений или видео) распространяется быстрее, поскольку пользователи социальных сетей часто пересылают информацию без предварительной фильтрации [2].

Дезинформация принимает множество форм и может варьироваться от историй о том, что Папа Франциск поддержал Дональда Трампа во время выборов 2016 года, до распространения ложной информации о том, что избирательные участки закрыты [3]. В Германии фальшивая новость о том, что беженцы с Ближнего востока изнасиловали 13-летнюю русскую девочку в Берлине, даже вызвала протесты [4].

Можно ли «дезинформационные операции», осуществляемые другими государствами, квалифицировать как международно-противоправное деяние. Международно-противоправное деяние состоит из двух элементов: (1) должно быть нарушено правовое обязательство государства; (2) деяние должно присваиваться соответствующему государству [5].

Первый элемент имеет место – дезинформационные операции нарушают принцип невмешательства во внутренние или внешние дела другого государства. Некоторые авторы приводят в пример выборы в США в 2016 году, полагая, что имело место вмешательство России посредством «fakenews» [6]. Однако большинство экспертов придерживаются строгого доктринального толкования термина «принудительный».

Обычный характер обязанности невмешательства во внутренние дела государства является нормой обычного права подтвердил Международный суд ООН в деле «Никарагуа против США», подчеркнув, что вмешательство является незаконным, если оно удовлетворяет двум условиям.

Во-первых, вмешательство касается вопросов, в которых «каждому государству разрешено свободно принимать решения в соответствии

с принципом государственного суверенитета» [7]. Например, выбор политической, экономической и культурной системы является неотъемлемым правом государства. Представляется, что любая дезинформация, направленная на лишение свободного выбора в отношении данных вопросов, будет удовлетворять данному условию.

Во-вторых, вмешательство является незаконным, «когда используются методы принуждения» [7], однако данное условие является дискуссионным. Под принуждением понимаются действия, «направленные на то, чтобы лишить другое государство его свободы выбора, то есть заставить это государство действовать недобровольно» [8]. При таком определении распространение дезинформации, нам представляется, выходит за рамки принуждения, поскольку их целью является воздействие, а не принуждение к принятию определенных действий.

Тем не менее, ряд ученых полагают, что по крайней мере некоторые формы кибероперации представляют собой запрещенное вмешательство в соответствии с международным правом. По мнению специалистов *Таллинского руководства,* запрещенные формы вмешательства включают «манипулирование выборами или общественным мнением с помощью кибернетических средств накануне выборов. Например, публикация ложной информации» будет представлять вмешательство во внутренние дела государства [8].

Таким образом, только серьезные операции по дезинформации с определенными оговорками могут признаваться как нарушающие принцип невмешательства.

Для наступления ответственности должен быть второй элемент – международно-противоправное деяние должно присваиваться государству. Однако на практике присвоение кибероперацией государствам зачастую оказывается весьма сложным. Относительно технических и политических аспектов присвоения, государства столкнулись с проблемой определения не только местоположения и идентификации киберинфраструктуры, из которой исходит операция, но и лица, которое управляло инфраструктурой [9]. В киберпространстве сложность присвоения усугубляется рядом факторов, в том числе возможностью проведения кибероперацией с использованием нескольких компьютерных систем в разных государствах, или использованием специальных механизмов для сокрытия происхождения кибероперации [9].

Зачастую государства используют в своих целях негосударственных субъектов, чтобы избежать ответственности. Государство будет нести ответственность за кибероперации негосударственного субъекта только в ситуации, если действия предпринимаются в соответствии с инструкциями или под руководством или контролем государства, или когда государство признает и принимает операции как свои собственные постфактум [10]. Вероятность того, что государство может признать и принять ответственность за кибервмешательство негосударственного субъекта, ничтожно мала. В каждом случае нужно будет доказать «эффективный контроль» государства над таким негосударственным субъектом.

Таким образом, распространение дезинформации находится в так называемой «серой зоне» международного права [10]. С одной стороны, данные действия не являются разрешенными с точки зрения международного права, а с другой стороны – нет прямого запрета. Общие нормы международного права также не дают полного ответа. Отсутствие правовой определенности создает заманчивые условия для государств, поскольку государства могут избежать ответственности за свои действия. В случае распространения дезинформации потерпевшее государство не может применить контрмеры или получить возмещение вреда.

Список источников

1. Manuel Rodriguez, “Disinformation Operations Aimed at (Democratic) Elections in the Context of Public International Law: The Conduct of the Internet Research Agency During the 2016 US Presidential Election” // 47 International Journal of Legal Information. 2019. P. 154.

2. Isabelle Hansen and Darren J. Lim, “Doxing Democracy: Influencing Elections Via Cyber Voter Interference”// Contemporary Politics. 2018. P. 413.

3. Van De Velde, Jacqueline, “The Law of Cyber Interference in Elections’, Social Science Research Network”. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3043828 (дата обращения: 12.04.2022).

4. Damien McGuinness, “Russia Steps into Berlin ‘Rape” Storm Claiming German Cover-up, BBC News” (Jan. 27, 2016). URL: http://www.bbc.com/news/blogs-eu-35413134 (дата обращения: 12.04.2022).

5. International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts with commentaries, Yearbook of the ILC (2001).

6. Steven Barela, “Zero Shades of Grey: Russian-Ops Violate International Law”. URL: https://www.justsecurity.org/54340/shades-grey-russian-ops-violate-international-law/ (дата обращения: 12.04.2022).

7. International Court of Justice, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Jurisdiction and Admissibility) [1984] ICJ Reports 391.

8. Michael N. Schmitt, “Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations” //Cambridge University Press. 2017. P. 317.

9. Barrie Sander, “Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections” // Chinese Journal of International Law. Volume 18. March 2019. P. 24-27.

10. Michael N. Schmitt, “Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law” // Chicago Journal of International Law. 2018. P. 49.