DOI: 10.17803/1994-1471.2022.140.7.136-142

К. М. Богатырев*

Угрозы медиабезопасности в цифровой среде: систематизация и анализ[1]

Аннотация. В статье рассматривается отдельный род информационных угроз, имеющих место в части информационного пространства, образованного пересечением медиасреды и цифровой среды. Такие информационные угрозы обладают спецификой, связанной с особенностями данного модифицированного информационного пространства и подразумевающей высокую степень общественной опасности деяний, посредством которых такие угрозы воплощаются в действительность. Актуальность исследования обусловлена потребностями экспертной практики, нуждающейся в теоретическом анализе и обобщении, разработке на их основе методических рекомендаций с учетом характеристик новой реальности, являющейся следствием цифровизации общественной жизни и заключающейся в повсеместном распространении электронных средств коммуникации. Практическая цель данной работы — систематизация и анализ многообразия угроз медиабезопасности, имеющих место в цифровой среде, для дальнейшей разработки типовых моделей использования специальных речеведческих знаний и обеспечения медиабезопасности в цифровой среде.
Ключевые слова: цифровизация; информационная угроза; информационная безопасность; медиасреда; медиабезопасность; цифровая среда; интернет-коммуникация; судебная экспертология; судебное речеведение; специальные знания.
Для цитирования: *Богатырев К. М.* Угрозы медиабезопасности в цифровой среде: систематизация и анализ // Актуальные проблемы российского права. — 2022. — Т. 17. — № 7. — С. 136–142. — DOI: 10.17803/1994-1471.2022.140.7.136-142.

Threats to Media Security in the Digital Environment: Systematization and Analysis[2]

Konstantin M. Bogatyrev, Postgraduate Student, Department of Forensic Expertise, Kutafin Moscow State Law University (MSAL)
ul. Sadovaya-Kudrinskaya, d. 9, Moscow, Russia, 125993
kbog@rambler.ru

Abstract. The paper considers a separate type of information threats that take place in the part of the information space formed by the intersection of the media environment and the digital environment. Such information threats have specificity, due to the peculiarities of this modified information space and implying a high degree of public danger of acts through which such threats are translated into reality. This study is relevant due to the needs

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-011-00190.
[2] The reported study was funded by RFBR according to the research project No. 20-011-00190.

* *Богатырев Константин Михайлович*, аспирант кафедры судебных экспертиз Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
Садовая-Кудринская ул., д. 9, г. Москва, Россия, 125993
kbog@rambler.ru

of expert practice, which requires theoretical analysis and generalization, methodological recommendations development given the features of a new reality that is a consequence of the digitalization of public life and consists in the widespread dissemination of electronic means of communication. The practical purpose of this work is to bring into the system and analyze the variety of media security threats that occur in the digital environment, for the further development of standard models for the use of special speech knowledge to ensure media security in the digital environment.
Keywords: digitalization; information threat; information security; media environment; media security; digital environment; internet communication; forensic expertise; judicial speech studies; special knowledge.
Cite as: Bogatyrev KM. Ugrozy mediabezopasnosti v tsifrovoy srede: sistematizatsiya i analiz [Threats to Media Security in the Digital Environment: Systematization and Analysis]. *Aktual'nye problemy rossijskogo prava*. 2022;17(7):136-142. DOI: 10.17803/1994-1471.2022.140.7.136-142. (In Russ., abstract in Eng.).

Введение

Одной из основных функций государства является обеспечение безопасности как для себя и общества в целом, так и для отдельной личности. С ней тесно связаны и остальные функции, такие как установление и поддержание общественного порядка, обеспечение социального мира и стабильности, защита личности от произвола, создание нормальных условий жизни и консолидация общества[3].

Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности»[4] содержит понятие и виды безопасности, а также указание на идентичность понятий «безопасность» и «национальная безопасность». Последнее как разновидность безопасности рассматривается в контексте той защитной функции, которая выполняется государством.

Обеспечение национальной безопасности — основная функция правоохранительных органов и одна из основных функций любых других государственных и муниципальных органов (т.е. всех органов публичной власти). Определяет основные направления государственной политики в области обеспечения безопасности и координирует деятельность по ее обеспечению Президент РФ, а также формируемый и возглавляемый им Совет Безопасности.

Эффективное и полноценное обеспечение безопасности во всех сферах общественной жизни невозможно осуществить только силами государства. Граждане и общественные объединения активно участвуют в реализации государственной политики в области обеспечения безопасности. Кроме того, важное место отведено и международному сотрудничеству в данной сфере, ведь многие угрозы (особенно информационные) в настоящее время имеют транснациональный, глобальный характер. В целом же обеспечение национальной безопасности представляет собой совокупность скоординированных и объединенных единым замыслом политических, организационных, социально-экономических, военных, правовых, информационных, специальных и иных мер.

Исследование

Важным элементом национальной безопасности в современном мире является информационная безопасность, имеющая статус стратегического национального приоритета и определяемая как состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз[5]. В Стратегии национальной безопасности Российской Федерации

[3] См.: *Морозова Л. А.* Теория государства и права. М. : Эксмо, 2010. С. 51–52.

[4] СЗ РФ. 2011. № 1. Ст. 2.

[5] См.: Доктрина информационной безопасности Российской Федерации, утв. Указом Президента РФ от 05.12.2016 № 646 // СЗ РФ. 2016. № 50. Ст. 7074.

от 02.07.2021[6] определены национальные интересы, в числе которых развитие безопасного информационного пространства, а также защита российского общества от деструктивного информационно-психологического воздействия.

В перечень задач по обеспечению информационной безопасности России в Доктрине информационной безопасности РФ входят:

— развитие и совершенствование системы обеспечения информационной безопасности Российской Федерации, реализующей единую государственную политику в этой области, включая совершенствование форм, методов и средств выявления, оценки и прогнозирования угроз информационной безопасности Российской Федерации, а также системы противодействия этим угрозам;
— совершенствование нормативной правовой базы обеспечения информационной безопасности Российской Федерации, включая механизмы реализации прав граждан на получение информации и доступ к ней, формы и способы реализации правовых норм, касающихся взаимодействия государства со средствами массовой информации;
— координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, предприятий, учреждений и организаций, независимо от формы собственности, в области обеспечения информационной безопасности Российской Федерации;
— развитие научно-практических основ обеспечения информационной безопасности Российской Федерации с учетом современной геополитической ситуации, условий политического и социально-экономического развития России и реальности угроз применения информационного оружия;
— расширение взаимодействия с международными и зарубежными органами и организациями при решении научно-технических и правовых вопросов обеспечения безопасности информации, передаваемой с помощью международных телекоммуникационных систем и систем связи;
— обеспечение условий для активного развития российской информационной инфраструктуры, участия России в процессах создания и использования глобальных информационных сетей и систем.

В действующей Доктрине угрозы информационной безопасности Российской Федерации, кратко называемые «информационные угрозы», понимаются как совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере. В предыдущей Доктрине информационные угрозы по своей общей направленности подразделялись на следующие виды:

— угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
— угрозы информационному обеспечению государственной политики Российской Федерации;
— угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
— угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

В настоящее же время такой классификации в действующей Доктрине нет; в ней имеются лишь общие указания на то, что информационная инфраструктура может использоваться для подрыва суверенитета, дестабилизации внутриполитической и социальной ситуации, воздействия на индивидуальное, групповое

[6] Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2021. № 27 (ч. II). Ст. 5351.

и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников; а также на то, что на население России в целях размывания традиционных российских духовно-нравственных ценностей наращивается информационное воздействие. Таким образом, единая классификация информационных угроз отсутствует, что формирует социальный запрос на ее разработку.

Перечень информационных угроз обширен и сложен для систематизации как ввиду неоднородности уже существующих угроз, так и вследствие постоянного их изменения, возникновения новых видов. В целях дестабилизации общественно-политической ситуации в Российской Федерации может распространяться недостоверная информация, в информационно-телекоммуникационной сети Интернет могут размещаться материалы террористических и экстремистских организаций, призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, совершению самоубийств, осуществляется пропаганда криминального образа жизни, потребления наркотических средств и психотропных веществ, размещается иная противоправная информация.

Сто́ит отметить, что в настоящее время Интернет понимается не просто как средство коммуникации, а как особая коммуникативная среда (интернет-среда, шире — цифровая среда). Интернет-среда уже не дополнение к реальному бытию человека, а вторая, параллельная (виртуальная) реальность, в которой принимаются и реализуются собственные решения, удовлетворяются потребности, создаются определенные продукты деятельности, а процесс общения трансформируется (становится отличным от аналогичного в ситуации живого общения)[7]. Это создает дополнительные риски, поскольку молодые люди, социализировавшиеся в Интернете, могут не всегда адекватно коммуницировать с окружающими и в целом реализовывать стратегии поведения, возможные в Интернете, но неприемлемые в обществе.

Сам Интернет является компонентом *медиасреды* — части информационного пространства, в которой информация вне зависимости от формы распространяется при помощи *средств массовой коммуникации* (СМК), в том числе средств массовой информации (СМИ) как их особого вида, имеющего при этом нормативное определение. Это подводит нас к определению *медиабезопасности*: она понимается нами как состояние защищенности отдельной личности от любых существующих в медиасреде информационных угроз (выраженных в информационных продуктах, оборот которых ограничен или запрещен действующими нормативными правовыми актами), а также вытекающее из него состояние защищенности государства и общества. Важно заметить, что поскольку медиасреда понимается как часть информационного пространства, то и медиабезопасность следует понимать как составную часть информационной безопасности, безопасность СМК, в том числе СМИ.

Система медиабезопасности включает в себя следующие элементы:

— безопасность аналоговых (нецифровых) СМК, не являющихся СМИ;
— безопасность аналоговых (нецифровых) СМИ;
— безопасность цифровых СМК, не являющихся СМИ;
— безопасность цифровых СМИ.

Последние два компонента формируют подсистему *медиабезопасности в цифровой среде*.

Для того чтобы полноценно рассмотреть все многообразие угроз медиабезопасности, необходимо осуществить классификацию этих информационных угроз. Основания такой классификации могут быть различными, от наличия

[7] Привод. по: *Галяшина Е. И.*, *Никишин В. Д.* Деструктивное речевое поведение в цифровой среде: факторы, детерминирующие негативное воздействие на мировоззрение пользователя // Lex russica (Русский закон). 2021. № 6 (175). С. 79–94.

соответствующих юридических составов в законодательстве до степени распространенности. Специалисты факультета психологии МГУ имени М. В. Ломоносова приводят следующую классификацию онлайн-рисков: контентные, коммуникационные, потребительские, технические риски, а также интернет-зависимость[8].

В контексте обеспечения медиабезопасности целесообразно использование концептов «контент-риски» и «коммуникационные риски». Контент-риски (контентные риски) — угрозы, связанные с ознакомлением пользователей с уже размещенной в Интернете информацией. Коммуникационные риски возникают в процессе общения интернет-пользователей ввиду использования одним из коммуникантов деструктивных речевых стратегий[9].

Приведенная ниже классификация угроз медиабезопасности основана на коммуникативной сущности (смысловой направленности) информационных продуктов, в которых находят выражение соответствующие угрозы (по умолчанию они будут относиться к категории коммуникационных рисков).

Угрозы экстремистского характера:

1) терроризм;
2) политический экстремизм (в том числе незаконные акции):
— правые (национал-социалисты, выстраивание жестких иерархий и т.д.);
— левые (примеры: анархисты (инцелы), коммунисты, феминистки);
— сепаратисты;
3) контркультура преступников (АУЕ);
4) религиозный экстремизм:
— радикальные религиозные течения;
— оскорбление чувств верующих;
5) этнический экстремизм;
6) ненависть (вражда, унижение человеческого достоинства) по признакам принадлежности к какой-либо демографической/социальной группе, например:
— женоненавистничество;
— эйблизм (ненависть к инвалидам);
— хулиганы, в том числе футбольные.

Угрозы оккультного характера:

1) тоталитарные секты;
2) деструктивные религиозные культы.

Угрозы антивиталистского характера:

1) культ смерти;
2) культ насилия и жестокости:
— дегуманизация жертв;
— скулшутинг/колумбайн;
— прославление/героизация убийц (тру-крайм комьюнити);
— каннибализм;
— жестокое обращение с животными;
3) продвижение аутодеструктивного поведения:
— суицид (в том числе посредством групп смерти);
— опасные хобби, связанные с риском для жизни (челленджи (вызовы), зацеперы, руферы, диггеры и т.д.);
— цифровое самоповреждение (селфхарм);
— нетипичное пищевое поведение (анорексия, булимия);
4) популяризация наркотиков и психоактивных веществ, романтизация наркоторговли.

Угрозы личной безопасности:

1) кибersталкинг (слежка);
2) доксинг (несанкционированный сбор информации, в том числе в виде цифровых файлов);
3) деанон (публичное распространение персональных данных / иных личных сведений);
4) киберагрессия, в том числе:
— диффамация (унижение чести и достоинства, умаление деловой репутации), клевета, оскорбление;
— троллинг;
— травля (буллинг);
5) домогательство (нарушение половой неприкосновенности и половой свободы):
— кибергруминг;
— секстинг;
— секс-шантаж;
6) фейкинг (распространение не соответствующих действительности сведений), манипуляция общественным сознанием.

[8] *Солдатова Г. У.*, *Рассказова Е. И.*, *Нестик Т. А.* Цифровое поколение России: компетентность и безопасность : монография. М. : Смысл, 2017. С. 90–99.

[9] См.: *Галяшина Е. И.*, *Никишин В. Д.* Указ. соч. С. 85.

Угрозы российской исторической памяти:

1) фальсификация истории;
2) реабилитация нацизма;
3) оскорбление дней воинской славы и памятных дат, осквернение символов воинской славы России;
4) оскорбление памяти защитников Отечества, унижение чести и достоинства ветеранов.

Угрозы аморального характера:

1) нецензурная брань (обсценная лексика);
2) антисемейные ценности;
3) социально-паразитарное поведение;
4) культура андерграунда;
5) продвижение нетрадиционных сексуальных отношений:

— ЛГБТ (яой, юри, смена пола и т.д.);
— зоофилия (фурри);

6) порнография, в том числе детская порнография.

Необходимо различать угрозы медиабезопасности и типы той информационной продукции, в которой такие угрозы находят выражение. Например, шок-контент, треш-контент, фанфикшн и аниме — не отдельные виды деструктива, а лишь возможные формы контента — проявления отдельных информационных угроз экстремистского, антивиталистского, аморального характера. Кроме того, не все информационные продукты, относящиеся к данным жанрам, представляют собой информационные угрозы; например, в контексте того же аниме содержащая деструктив информационная продукция является лишь его маргинальной частью.

Результаты и выводы

Так или иначе, анализ контент-рисков (т.е. конкретных информационных материалов деструктивного характера), корреспондирующих перечисленным выше угрозам медиабезопасности, представляется эффективным проводить посредством специальных исследований, посвященных отдельным видам угроз. Целью же настоящей работы была разработка приведенной выше классификации.

Анализ представленного многообразия угроз медиабезопасности, имеющих место в цифровой среде, в последующих исследованиях необходим для дальнейшей разработки типовых моделей использования специальных речеведческих знаний в целях обеспечения медиабезопасности в цифровой среде в рамках разработки соответствующей частной экспертной теории в русле учения о цифровизации судебно-экспертной деятельности, разрабатываемой представителями кафедры судебных экспертиз Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)[10].

БИБЛИОГРАФИЯ

1. *Галяшина Е. И.*, *Никишин В. Д.* Деструктивное речевое поведение в цифровой среде: факторы, детерминирующие негативное воздействие на мировоззрение пользователя // Lex russica (Русский закон). — 2021. — № 6 (175). — С. 79–94.
2. *Морозова Л. А.* Теория государства и права. — М. : Эксмо, 2010. — 384 с.
3. *Носов Н. А.* Виртуальная психология. — М., 2000. — 432 с.
4. *Россинская Е. Р.* Учение о цифровизации судебно-экспертной деятельности и проблемы судебно-экспертной дидактики // Правовое государство: теория и практика. — 2020. — № 4-1 (62). — С. 88–101.
5. *Солдатова Г. У.*, *Рассказова Е. И.*, *Нестик Т. А.* Цифровое поколение России: компетентность и безопасность : монография. — М. : Смысл, 2017. — 375 с.

Материал поступил в редакцию 31 декабря 2021 г.

[10] См.: *Россинская Е. Р.* Учение о цифровизации судебно-экспертной деятельности и проблемы судебно-экспертной дидактики // Правовое государство: теория и практика. 2020. № 4-1 (62). С. 88–101.

REFERENCES (TRANSLITERATION)

1. Galyashina E. I., Nikishin V. D. Destruktivnoe rechevoe povedenie v cifrovoj srede: faktory, determiniruyushchie negativnoe vozdejstvie na mirovozzrenie polzovatelya // Lex russica (Russkij zakon). — 2021. — № 1 (175). — S. 79–94.
2. Morozova L. A. Teoriya gosudarstva i prava. — M.: Eksmo, 2010. — 384 s.
3. Nosov N. A. Virtualnaya psihologiya. — M., 2000. — 432 s.
4. Rossinskaya E. R. Uchenie o cifrovizacii sudebno-ekspertnoj deyatelnosti i problemy sudebno-ekspertnoj didaktiki // Pravovoe gosudarstvo: teoriya i praktika. — 2020. — № 4-1 (62). — S. 88–101.
5. Soldatova G. U., Rasskazova E. I., Nestik T. A. Cifrovoe pokolenie Rossii: kompetentnost i bezopasnost: monografiya. — M.: Smysl, 2017. — 375 s.