Научная статья
УДК 340.69
DOI: 10.37973/KUI.2022.13.69.009

ЭКСПЕРТНОЕ ОБЕСПЕЧЕНИЕ МЕДИАБЕЗОПАСНОСТИ В ЦИФРОВОЙ СРЕДЕ[1]

Константин Михайлович Богатырев,
Московский государственный юридический университет
имени О.Е. Кутафина, Москва, Россия,
kbog@rambler.ru

Аннотация

Введение: целью статьи является рассмотрение предпосылок к формированию системы медиабезопасности в цифровой среде. Предлагается авторский подход к формулированию и научному анализу таких категорий, как медиасреда, цифровая среда и медиабезопасность, анализируется существующее в настоящее время многообразие юридических терминов, связанных с понятием «безопасность», рассматриваемом в публично-правовом ключе (приводится его соотношение с понятиями «национальная безопасность», «информационная безопасность»).

Материалы и методы: методологическую основу исследования составила аналитическая философская традиция наряду с общенаучными (описание, сравнение, обобщение и др.), а также частнонаучными методами (формально-юридическим, сравнительно-историческим, сравнительно-правовым и др.).

Результаты исследования: делается вывод, что информационная безопасность является частью единой системы национальной безопасности и представляет собой безопасность информационного пространства, в то время как ее разновидность (медиабезопасность) связана с той частью информационного пространства (т.н. медиасредой), в которой информация распространяется через средства массовой коммуникации (в т.ч. СМИ). Также рассматривается пересечение медиасреды и цифровой среды, возникшей вследствие процесса цифровизации в результате внедрения электронных технологий и средств коммуникации.

Обсуждение и заключение: обосновывается необходимость разработки теории экспертного обеспечения медиабезопасности (в т.ч. в цифровой среде), выражающегося в использовании специальных знаний путем привлечения сведущих лиц различных экспертных специальностей (в т.ч. тех, которые относятся к классу судебных речеведческих экспертиз) как лиц, участие которых в обеспечении медиабезопасности в цифровой среде наиболее желательно ввиду особенностей информационных медиапродуктов.

Ключевые слова: судебная экспертология; специальные знания; цифровизация; информационная безопасность; медиабезопасность; цифровая среда; информационная угроза; интернет-коммуникация

Для цитирования: Богатырев К.М. Экспертное обеспечение медиабезопасности в цифровой среде // Вестник Казанского юридического института МВД России. 2022. Т. 13. № 4 (50). С. 60 – 70. DOI: 10.37973/KUI.2022.13.69.009

[1] Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований в рамках научного проекта № 20-011-00190.

Scientific article
UDC 340.69
DOI: 10.37973/KUI.2022.13.69.009

FORENSIC ENSURING OF MEDIA SECURITY IN THE DIGITAL ENVIRONMENT[1]

Konstantin Mihailovich Bogatyrev,
Kutafin Moscow State Law University, Moscow, Russia, kbog@rambler.ru

Abstract

Introduction: the goal of the study is consideration of the prerequisites to develop media security systems in the digital environment. The author presents their own approach of formation and academic analysis of the categories “media environment”, “digital environment”, and “media security”. For detailed perception the author analyses the diverse of the legal terms relating to the concept of “safety” under public and legal vein (the author gives the correlation with the concepts of "national security" and "information security").

Materials and Methods: the methodological basis of this work was the analytical philosophical tradition. General scientific methods of cognition were applied in this work: analogy, comparison, generalization, etc. Also private scientific methods of cognition were used: there were legal, comparative-historical, comparative-legal methods, etc.

Results: the author concluded that informational security is a part of the overall system of the national security and represents safety of the information space while its type (media safety) connected to the part of information space (mediaspace) within information is disseminated through the means of mass communication (including mass media). The author also considered confluence of media space and digital space resulting from digitalization resulting from the adoption of electronic technologies and means of communications.

Discussion and Conclusions: the author defines the need to elaborate the theory of expert support for media security (including digital area), of using specific knowledge through various experts participation (including experts of the class of forensic speech experts) as individuals whose involvement in media security in the digital environment is most desirable because of the characteristics of information media products.

Keywords: forensic expertology; special knowledge; digitalization; information security; media security; digital environment; information threat; internet communications

For citation: Bogatyrev K.M. Forensic Ensuring of Media Security in the Digital Environment // Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2022. Vol. 13. № 4 (50). P. 60 – 70. DOI: 10.37973/KUI.2022.13.69.009

Введение

Одной из основных функций государства как особого общественного института является обеспечение безопасности (состояния защищенности от угроз природного и антропогенного характера) для общества в целом и для отдельных его членов. С ней тесно связаны и остальные функции, такие как установление в обществе определенного порядка, обеспечение социального мира и стабильности, защита личности от произвола, создание нормальных условий жизни для всех членов общества и его консолидация [1, с. 51-52].

Информационная безопасность как часть единой системы национальной безопасности

Сама по себе **безопасность** – категория максимально общая, и применительно к деятельности государства необходимо определиться с ее пониманием более основательно. В этом нам помогает Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности»[2], где, во-первых, перечисляются виды безопасности (безопасность государства, общественная безопасность, экологическая безопасность, безопасность личности и иные предусмотренные законодательством Россий-

[1] Acknowledgments: The reported study was funded by RFBR according to the research project No. 20-011-00190.

[2] О безопасности: Федеральный закон от 28.12.2010 № 390-ФЗ // Собрание законодательства Российской Федерации. 2011. № 1. Ст. 2.

ской Федерации виды безопасности), во-вторых, указывается на синонимичность понятий «**безопасность**» и «**национальная безопасность**» в контексте той защитной функции, которая выполняется государством.

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

Однако эффективное и полноценное обеспечение безопасности во всех сферах общественной жизни было бы невозможно обеспечить только лишь силами государства. Граждане и общественные объединения также активно участвуют в реализации государственной политики в области обеспечения безопасности. Кроме того, важное место отведено и международному сотрудничеству в данной сфере, поскольку 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.

Таким образом, основными принципами обеспечения безопасности являются:

- соблюдение и защита прав и свобод человека и гражданина;

- законность;

- системность и комплексность применения политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности;

- приоритет предупредительных мер;

- взаимодействие государственных органов с общественными объединениями, международными организациями и гражданами в целях обеспечения безопасности.

Нормативно-правовую основу деятельности по обеспечению безопасности, помимо Конституции Российской Федерации, федерального и регионального законодательства, составляют также подзаконные нормативные акты. Например, в Стратегии национальной безопасности Российской Федерации от 2 июля 2021 г.[1] определены национальные интересы, в число которых входит развитие безопасного информационного пространства, защита российского общества от деструктивного информационно-психологического воздействия. Для обеспечения и защиты национальных интересов концентрируются, в том числе, на таком стратегическом национальном приоритете, как **информационная безопасность**, определяемая как состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз[2].

Информационная безопасность – часть единой системы национальной безопасности (безопасность в информационном пространстве). Ее правовую основу составляют (помимо упомянутого Федерального закона «О безопасности») Федеральный закон «Об информации, информационных технологиях и о защите информации»[3], Закон «О средствах массовой информации»[4], Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию»[5], Стратегия национальной безопасности[6], Доктрина информационной безопасности[7], кодексы, в которых закреплена ответственность за нарушения информационной безопасности, и т.д.

Информационная безопасность имеет технический и содержательный компоненты. Технический компонент связан с защитой информационной, в т.ч. критической, инфраструктуры (технологий, оборудования и состоящих из них сетей, а также функционирующих на их основе систем и программ, программно-аппаратных

[1] О Стратегии национальной безопасности Российской Федерации: указ Президента Российской Федерации от 02.07.2021 № 400 // Собрание законодательства Российской Федерации. 2021. № 27 (ч. II). Ст. 5351.

[2] Доктрина информационной безопасности Российской Федерации, утв. указом Президента Российской Федерации от 05.12.2016 № 646 // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

[3] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ // Собрание законодательства Российской Федерации. 2006. № 31 (ч. I). Ст. 3448.

[4] О средствах массовой информации: Закон Российской Федерации от 27.12.1991 № 2124-I // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1992. № 7. Ст. 300.

[5] О защите детей от информации, причиняющей вред их здоровью и развитию: Федеральный закон от 29.12.2010 № 436-ФЗ // Собрание законодательства Российской Федерации. 2011. № 1. Ст. 48.

[6] О Стратегии национальной безопасности Российской Федерации: указ Президента Российской Федерации от 02.07.2021 № 400 // Собрание законодательства Российской Федерации. 2021. № 27 (ч. II). Ст. 5351.

[7] Доктрина информационной безопасности Российской Федерации, утв. указом Президента Российской Федерации от 05.12.2016 № 646 // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

комплексов) от атак, направленных на их уничтожение, повреждение или перехват контроля над ними. Содержательный же компонент имеет отношение к информации, которая распространяется посредством таких информационных систем. И хотя в настоящее время, говоря об информационной безопасности, подразумевают в первую очередь борьбу с несанкционированным доступом к информационной инфраструктуре и ее содержимому, в последнее время на первый план вышел вопрос борьбы с преступлениями, связанными с запрещенным законом созданием и распространением информации определенной направленности или содержания.

Распространение определенной информации (согласно официальной государственной позиции, изложенной в Стратегии) несет угрозу для российского суверенитета, приводит к дестабилизации общественно-политической ситуации в стране. Как правило, речь идет о недостоверной (в т.ч. общественно значимой) информации, материалах террористической и экстремистской направленности, запрещенной законом пропаганды (например, криминального образа жизни, наркотиков) и т.д. Также делается акцент на том, что основным объектом деструктивного воздействия посредством такой информационной продукции является молодежь.

Однако серьезные риски деструктивного влияния такого рода информации следуют не только из ее смысловой направленности, но и из массового характера распространения. Внедрение результатов научно-технического прогресса порождало преобразование всех сфер общественной жизни – от экономической и политической до культурной. Общество вступило в эпоху высоких технологий, связанных с дистанционной коммуникацией, передачей данных. По мере внедрения средств, расширявших возможности передачи информации, часть из них начала приобретать массовый характер – направленность на максимально широкую аудиторию. Однако роль одних и тех же средств коммуникации со временем изменялась: в настоящее время значение ставших традиционными средств массовой информации (таких как печатные издания, радио, телевидение), ранее являвшихся основными источниками сведений о мире и в силу этого определявших мышление большей части общества, сохранилось, однако девальвировалось. Основными средствами передачи данных, наряду с традиционными, являются информационно-телекоммуникационные сети (Интернет). Поэтому особенно важно разработать научно обоснованную теорию обеспечения информационной безопасности в той части информационного пространства, связанную с массовым распространением информации, т.е. с медиасредой.

Медиабезопасность
как вид информационной безопасности

Обратимся к анализу термина «медиасреда». Так, А.М. Кузьмин определяет ее как «пространство, в котором формируется, распространяется и воспроизводится с помощью массовых коммуникаций и СМИ культура информационного общества» [2]. По мнению М.В. Шкондина, «медиасфера (медиасистема) – часть инфосферы», имеющая отношение главным образом к информации массовой, и в ее структуру входят, прежде всего, средства массовой информации [3, с. 337]. Как можно заметить, в приведенных определениях значительную смысловую нагрузку несут термины «средства массовой информации», «инфосфера», «информационное сообщество», «массовые коммуникации». Данные термины входят в понятийное поле, изучаемое в рамках информационного права как юридической дисциплины.

В нашем понимании **медиасреда** – это часть информационного пространства, в которой информация вне зависимости от формы распространяется при помощи *средств массовой коммуникации* (в т.ч. средств массовой информации как их особого вида, имеющего при этом нормативное определение). Понятие «информационное пространство», фигурирующее в данном определении, активно используется в той же Стратегии, однако ни в ней, ни в каком-либо другом нормативном правовом акте его содержание не раскрывается. Попытки его рассмотрения были в науке; например, С.А. Проскурин определяет информационное пространство как «пространство, в котором создается, перемещается и потребляется информация» [4].

В контексте рассматриваемой темы также важно установить соотношение понятий «массовая информация» и «массовая коммуникация», «средства массовой информации» (СМИ) и «средства массовой коммуникации» (СМК). Мы сформулируем две возможных гипотезы их соотношения:

1. Они не являются понятиями-синонимами (СМК – шире СМИ и включают их в себя);

2. Эти понятия – тождественны. Необходимо отметить, что в науке отсутствует однозначный подход к определению термина «средство массовой информации»; также не определено его соотношение с терминами «средства массовой коммуникации», «медиа» и «масс-медиа», кото-

Таблица 1. Медиасреда (система средств массовой коммуникации)
Table 1. Media environment (mass communication media system)

<table>
<tr><td colspan="2">Аналоговая форма представления данных</td><td colspan="2">Цифровая форма представления данных</td></tr>
<tr><td>СМК, не являющиеся СМИ</td><td colspan="2">СМИ</td><td>СМК, не являющиеся СМИ</td></tr>
<tr><td rowspan="2">Средства массовой коммуникации, имеющие аналоговую форму представления данных и не зарегистрированные как СМИ (например, коротковолновые радиостанции, частные периодические издания и т.д.)</td><td>Традиционные СМИ: телевидение; радио; периодические издания; и т.п.</td><td>Средства массовой коммуникации, имеющие цифровую форму и зарегистрированные как СМИ: сайты традиционных СМИ, интернет-издания.</td><td rowspan="2">Сайты:
социальные сети; хостинги;
стриминг-сервисы;
мессенджеры;
почтовые сервисы; форумы;
тематические сайты;
сервисы объявлений;
облачные хранилища;
поисковые сервисы и т.д.</td></tr>
<tr><td colspan="2">Закон РФ от 27.12.1991 № 2124-I «О средствах массовой информации»</td></tr>
<tr><td colspan="4">ФЗ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и ФЗ от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»</td></tr>
</table>

рые одни ученые считают синонимами, другие же различают данные понятия.

В Большой актуальной политической энциклопедии понятие «средство массовой информации» приравнивается к масс-медиа. СМИ (средства массовой информации, massmedia) – в совокупности газеты, журналы, радио, телевидение, интернет-издания и т.п.[1]. Подобный подход наблюдается и в словаре бизнес-терминов: масс-медиа – средства массовой информации[2].

В энциклопедии культурологии же тождественными понятиями являются «масс-медиа» и «средства массовой коммуникации»: технологии и институты, через которые централизованно распространяются информация и другие формы символической коммуникации крупным, гетерогенным и географически рассеянным аудиториям; одна из форм распространения и бытия массовой культуры[3].

М.М. Лукина и И.Д. Фомичева разграничивают средства массовой информации и средства массовой коммуникации, считая, что одно является частью другого. Интернет (как одно из средств массовой коммуникации) является носителем, с помощью которого СМИ распространяют свои публикации. Различные сайты, порталы и т.п. могут стать средствами массовой информации (получить статус сетевого издания) и использовать те или иные средства массовой коммуникации для осуществления своей деятельности [5, с. 22].

С ними согласен и М.А. Ющенко, утверждая, что «необходимо различать средства массовой информации (СМИ) и средства массовой коммуникации (СМК). <…> …Можно выделить как минимум три основные причины использования СМК в более широком понимании, чем СМИ. Во-первых, потому что СМК появились раньше. Когда не существовали СМИ в принятом сегодня понимании (печать, телерадиовещание), их функцию выполняли рукописные книги. Во-вторых, сегодня СМК, помимо СМИ, включают в себя кинематограф, шоу-бизнес, Интернет, новые средства массовой информации, рекламу, PR, оказывающие значительное влияние на массовое сознание. В-третьих, СМИ – это преимущественно однонаправленная система, в то время как СМК являются системой, обладающей обратной связью, почему в последние годы все активнее обсуждается необходимость преобразования СМИ в СМК, т.е. в инструмент социального взаимодействия. Обратная связь обеспечивается посредством дополнительных специальных исследовательских организаций» [6].

Таким образом, термины «медиа» и СМК мы считаем синонимичными, в то время как отождествление термина «медиа» со СМИ («масс-ме-

[1] Большая актуальная политическая энциклопедия. URL: http://greater_political.academic.ru/ (дата обращения: 26.08.2021).
[2] Словарь бизнес-терминов. URL: http://dic.academic.ru/dic.nsf/business/7613 (дата обращения: 26.08.2021).
[3] Энциклопедия культурологии. URL: http://dic.academic.ru/dic.nsf/enc_culture/ (дата обращения: 26.08.2021).

диа») следует оценивать как неоправданное сужение. Однако существует еще одно серьезное основание для обособления СМИ как особой разновидности СМК. Существует их нормативное определение – это «периодическое печатное издание, сетевое издание, телеканал, радиоканал, телепрограмма, радиопрограмма, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации под постоянным наименованием (названием)»[1]. Из этого следует, что главной характеристикой СМИ является их периодичность. Кроме того, это еще и особый правовой статус, получить который можно только путем регистрации. Таким образом, СМК делятся на зарегистрированные в качестве СМИ и не получившие такого статуса. При этом позиция, в рамках которой любой сайт, а также вся сеть Интернет в целом рассматриваются как СМИ, некорректна как в силу рассмотренных выше обстоятельств, так и в силу прямого указания закона (сайт в информационно-телекоммуникационной сети «Интернет», не зарегистрированный в качестве средства массовой информации, средством массовой информации не является[2]).

Развитие инфраструктуры, в рамках которой осуществляется оборот информации в любой (в т.ч. цифровой) форме, привело к многообразию способов и каналов передачи информации. Однако этой инфраструктурой, представляющей собой совокупность средств массовой коммуникации, передающих информацию в т.ч. в цифровой форме, могут пользоваться и правонарушители. В связи с этим возникает необходимость выстраивания соответствующей системы безопасности, позволяющей эффективно осуществлять выявление правонарушений, собирание, исследование и использование криминалистически значимой информации, привлечение правонарушителей к ответственности. Такая система кратко может быть обозначена термином «медиабезопасность».

Исследователи указывают, что в настоящее время возник социальный запрос на создание системы обеспечения медиабезопасности (в т.ч. в цифровой среде). Поэтому, в том числе, делаются попытки по формулированию самого термина «медиабезопасность». Так, по мнению А.А. Морозовой, «медиабезопасность – это состояние защищенности каждого индивида от недостоверной или опасной информации, причиняющей вред здоровью человека, его нравственности и личностному развитию» [7]. И.А. Фатеева, проанализировав имеющиеся труды по данной тематике, дала следующее определение: «медиабезопасность – это состояние защищенности индивида от некачественной информации, поступающей из медиасферы, то есть из системы средств массовой информации и коммуникации» [8].

Мы же предлагаем следующее определение **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. Угрозы информационной безопасности определяются в соответствии с перечнем запрещенных деяний, приведенном в различных кодифицированных нормативных правовых актах (таких как УПК РФ, КоАП РФ, ГК РФ). Важно заметить, что раз медиасреда понимается как часть информационного пространства, то и медиабезопасность следует понимать как составную часть информационной безопасности, безопасности СМК, в т.ч. СМИ. Однако сама медиабезопасность также имеет в себе подразделения, формирующие ее внутреннюю структуру. Исходя из наших научных изысканий (в т.ч. из нашего понимания структуры медиасреды, представленной выше), **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.

Как мы видим, в основе данного разделения медиабезопасности лежат два компонента – форма представления данных и правовой статус СМК (зарегистрировано оно в качестве СМИ или же нет). Последние два компонента формируют подсистему **медиабезопасности в цифровой среде.**

Цифровизация всех сфер общественной жизни, ставшая главным трендом последнего десятилетия, привела к качественному скачку в развитии инфраструктуры передачи данных.

[1] О средствах массовой информации: Закон Российской Федерации от 27.12.1991 № 2124-I // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1992. № 7. Ст. 300.

[2] Ст. 8 Закона Российской Федерации от 27.12.1991 № 2124-I «О средствах массовой информации».

Многообразие способов и каналов передачи информации вкупе с ростом цифровой грамотности населения привело к тому, что цифровые технологии в настоящее время играют ведущую роль в развитии всех сфер жизнедеятельности общества (некоторые ученые даже видят в такой зависимости от высоких технологий угрозу [9]). Научно-техническими изысканиями в данной области активно занимаются государственные учреждения (заинтересованные в обеспечении государственной безопасности в данной сфере) и негосударственные коммерческие организации (заинтересованные в разработке новых информационных продуктов с последующим получением выгоды).

Массовая коммуникация также преобразуется за счет внедрения новых технологий. Информационно-телекоммуникационные сети (в т.ч. Интернет), относящиеся к числу т.н. «новых медиа», характеризуются тем, что у значительного объема информационных потоков отсутствует государственный контроль (в отличие от тех же традиционных СМИ). Это можно объяснить тем, что цифровая среда (частью которой является Интернет) – новое и динамичное явление, некоторое время находившееся на периферии или же за пределами внимания законодателя. Более того, сама возможность государственного контроля Интернета представляется ограниченной ввиду его децентрализованной природы и сложного технического устройства. Поэтому отечественному законодателю необходимо корректно определить границу возможного нормативно-правового регулирования.

Мы же для этих целей специально выделяем подсистему **медиабезопасности в цифровой среде** (как особую часть системы медиабезопасности), которая подразумевает обеспечение безопасности в особом информационном пространстве, где пересекаются множества, обозначаемые понятиями «цифровая среда» и «медиасреда» (информация, распространяемая через средства массовой коммуникации (медиа) и СМИ, может быть выражена в цифровой форме).

Распространенность новых технологий не могла не привести к тому, что их возможности будут использоваться, в том числе, и для нарушения закона (подготовки и/или совершения проступков/преступлений различной тяжести и направленности). В настоящее время в цифровой среде (понимаемой нами как совокупность информационных технологий и информационных систем, обрабатывающих информацию, имеющую цифровую форму представления, а также содержащих такую информацию информационных ресурсов) существуют условия для совершения не только преступлений в сфере компьютерной информации, но практически любых видов преступлений: против жизни и здоровья, против собственности, общественной безопасности, против мира и безопасности человека и т.д.

Наиболее часто посредством электронных (цифровых) средств массовой коммуникации (таких как сеть Интернет), составляющих значительную часть цифровой среды, могут осуществляться запрещенная законом пропаганда (в т.ч. суицида); диффамационные речевые действия (распространение не соответствующих действительности сведений, порочащих честь, достоинство, деловую репутацию; оскорбление, клевета); угрозы; возбуждение ненависти либо вражды, а равно унижение человеческого достоинства; публичные призывы к осуществлению противозаконной деятельности; нарушение законодательства о защите детей от информации, причиняющей вред их здоровью и (или) развитию и т.п. [10]. Сущность всех этих преступлений заключается в распространении информации, несущей информационную угрозу медиабезопасности.

В современных условиях информационные (в т.ч. цифровые) технологии также активно используются для борьбы внутре- и внешнеполитической; идеологические диспуты и споры зачастую перетекают в конфликтогенное русло и могут приводить к совершению запрещенных законом действий (запрещенной законом пропаганде, клевете, оскорблениям, оправданию различных деструктивных течений и идей и т.п.). Кроме того, угрозы заключаются в том, что средства массовой коммуникации (в т.ч. СМИ) обладают уникальной способностью по формированию мировоззрения граждан [6]. В настоящее время основным критерием истинности информации становится не верифицируемость (проверяемость), а виральность [11] (характеристика, определяющая вероятность возникновения у читателей желания поделиться такой информацией с другими людьми), что препятствует распознанию недостоверной информации и ее широкому распространению. Все это создает серьезные риски для медиабезопасности в цифровой среде.

Использование специальных знаний для обеспечения медиабезопасности в цифровой среде

Функция по обеспечению медиабезопасности в цифровой среде, т.е. по борьбе с информационными угрозами, существующими в цифровой

среде в результате противозаконных деяний (совершаемых с использованием средств массовой коммуникации), лежит (как и в случае с любыми другими нарушениями закона) на правоохранительных органах. Для ее реализации необходимо осуществлять деятельность по выявлению готовящихся и совершаемых правонарушений, раскрытию и расследованию уже совершенных противоправных деяний, несущих общественную опасность, а также по принятию процессуальных решений. Однако действия по обеспечению медиабезопасности выполняются не только должностными лицами государственных органов; в пределах своей «частной территории» этим занимаются и администрации социальных сетей, различных сайтов и цифровых платформ.

Делается это по ряду причин: во-первых, крупные информационные организации (например, Google, Facebook (*организация признана экстремистской в Российской Федерации)*, Twitter и т.д.) принимают все усилия по тому, чтобы на их информационных ресурсах соблюдались требования законодательства (в т.ч. внутреннего законодательства отдельных стран), инкорпорируемые во внутренние правила самих платформ; во-вторых, зачастую у государственных органов возможности мониторинга данных платформ на предмет нарушения законодательства ограничены (как технически, так и с точки зрения соблюдения конфиденциальности пользовательских данных). Да и в целом функции по борьбе с информационными угрозами в рамках отдельной платформы проще выполнять тем, у кого есть полный доступ к ее «обратной» технической стороне. Однако, как это отмечено в п. 1 решения Правительственной комиссии по профилактике правонарушений от 28.12.2020, некоторые интернет-площадки (например, Twitter) не только не удаляют противоправную информацию по своей инициативе, но и не выполняют предписания выявивших противоправный контент компетентных органов, таких как Роскомнадзор. Так, несоблюдение подобных предписаний в недавнем прошлом повлекло наложение ограничений на Twitter (замедление скорости его работы)[1].

Поэтому на смену политике полного контроля содержимого социальных сетей со стороны государства пришел подход к обязательному самоконтролю социальных сетей с последующим отчетом перед государственными органами (для этого, в частности, в настоящее время создается реестр соцсетей[2]), что нашло свое отражение в Федеральном законе от 30.12.2020 № 530-ФЗ[3].

Очевидно, что экспертное обеспечение медиабезопасности необходимо как при работе с традиционными СМК, так и с теми, что размещены в цифровой среде. Однако во втором случае к анализу информационных продуктов будут предъявляться более строгие требования, вытекающие из особенностей такого рода объектов. В свою очередь, особенности таких информационных продуктов являются следствием комбинации:

особенностей средств массовой коммуникации (например, заведомое распространение на неопределенный круг лиц);

особенностей цифровой формы (гипертекстуальность, креолизованность, существование информационного продукта только в электронном виде и т.д.);

специфики отдельных категорий информационных продуктов (направленность на определенную возрастную аудиторию, жанровые и стилистические особенности и т.д.).

Следовательно, для того чтобы компетентные органы могли эффективно выполнять свою правоохранительную функцию, им необходимо содействие обладающих специальными знаниями лиц. Оно необходимо как в техническом, так и в содержательном компонентах информационной безопасности. Технический компонент, связанный с защитой информационной инфраструктуры (технологий, оборудования и состоящих из них сетей, а также функционирующих на их основе систем и программ, программно-аппаратных комплексов), подразумевает необходимость привлечения компьютерно-технических судебных экспертов и специалистов, имеющих соответствующее техническое образование, специальные знания и способных выявить и устранить уязвимости информационных (в т.ч. цифровых) СМК, изучить и описать их элементы, процедуру их нормального функционирования.

Содержательный же компонент, подразумевающий анализ информационного содержимого данных систем, требует привлечения сведущих лиц, обладающих специальными знаниями о таком содержимом (например, экспертов-речеведов, психологов, экономистов и т.д.). У таких

[1] Роскомнадзор принял меры по защите российских граждан от влияния противоправного контента. URL: https://rkn.gov.ru/news/rsoc/news73464.htm (дата обращения: 10.09.2021).

[2] Роскомнадзор приступил к формированию реестра социальных сетей. URL: https://rkn.gov.ru/news/rsoc/news73860.htm (дата обращения: 26.09.2021).

[3] О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»: Федеральный закон от 30.12.2020 № 530-ФЗ // Собрание законодательства Российской Федерации. 2021. № 1 (ч. I). Ст. 69.

экспертов также должны быть определенные специальные знания в компьютерно-технической области, которые необходимы им в силу характера исследуемых объектов (например, цифровая форма подразумевает особый порядок обнаружения, фиксации и изъятия доказательственной информации, особые требования к обеспечению допустимости и достоверности результатов исследования).

Таким образом, для надлежащего анализа распространяемых через цифровые СМК информационных продуктов (в большинстве своем – являющихся речевым продуктом или содержащим текстовый компонент) на наличие специальных признаков правонарушений необходимо привлечь сведущее лицо, обладающее надлежащей компетенцией. В связи с этим представляется рациональным рассмотреть разделение множества цифровых следов на активные и пассивные цифровые следы [11]. Такое деление носит прикладной характер, например, позволяет определить, необходимо ли привлечение компьютерно-технического эксперта для проведения исследования технического компонента или же нет. При «активном» цифровом следе, представляющем собой продукт речевой деятельности (в т.ч. поликодовый), участие компьютерно-технического эксперта не требуется [12], но имеется необходимость привлечения лица, обладающего высшим образованием по специальности «Судебная экспертиза» (специализация № 5 «Речеведческие экспертизы»), в компетенцию которого входят знания, умения и навыки по изучению объектов, представленных на исследование в цифровой форме на цифровых носителях[1].

Для подготовки конкретных методических рекомендаций, составляющих основу эффективного исследования продуктов медиадискурса, имеющих цифровую форму представления, сведущими лицами разных экспертных специальностей необходима разработка особой частной экспертной теории, в рамках которой были бы проанализированы наиболее общие закономерности экспертного обеспечения (через использование специальных знаний) медиабезопасности в цифровой среде. Разработка данной частной теории производится в рамках судебной экспертологии. Теория данной самостоятельной дисциплины [13] была разработана в рамках научной школы, развивающейся на базе кафедры судебных экспертиз Московского государственного юридического университета имени О.Е. Кутафина (МГЮА); ее ведущими представителями являются профессора Е.Р. Россинская, Е.И. Галяшина, А.М. Зинин.

Обсуждение и заключение

В статье сделаны лишь первые шаги в рамках разработки соответствующей частной экспертной теории в русле судебного речеведения и учения о цифровизации судебно-экспертной деятельности. В дальнейшем автор подробно рассмотрит порядок обеспечения медиабезопасности (в т.ч. в цифровой среде) как со стороны государства, так и со стороны граждан, их объединений и частных организаций; изучит совокупность специальных знаний, которыми необходимо обладать сведущему лицу, привлекаемому для обеспечения медиабезопасности, формы использования и применения специальных знаний; проанализирует место и значение специальных речеведческих знаний и их носителей в обеспечении медиабезопасности.

В заключение следует отметить, что на всех этапах (от возникновения потенциальной возможности правонарушения, связанного с распространением деструктивной информации, до привлечения к ответственности нарушителя) настоятельно рекомендуется использование специальных знаний как валидного средства оценки характера распространяемой информационной продукции, наличия у нее специальных признаков правонарушений.

[1] Об утверждении федерального государственного образовательного стандарта высшего образования по специальности 40.05.03 Судебная экспертиза (уровень специалиста): приказ Министерства образования и науки Российской Федерации от 28.10.2016 № 134. URL: www.pravo.gov.ru (дата обращения: 08.12.2016).

СПИСОК ИСТОЧНИКОВ

1. Морозова Л.А. Теория государства и прав. Москва: Эксмо. Российское юридическое образование. 2010. 510 с.
2. Кузьмин А.М. Категория «медиасреда» и ее содержание на современном этапе развития общества // Медиаскоп. 2011. № 1. URL: http://www.mediascope.ru/node/765 (дата обращения: 26.03.2022).
3. Шкондин М.В. Информационный потенциал общества и концепты целостности медиасистемы // Вопросы теории и практики журналистики. 2015. № 4. С. 335-348.
4. Проскурин С.А. Геополитическое измерение глобального информационного пространства // Геополитика: учебник / под общ. ред. В.А. Михайлова. Москва: Изд-во РАГС, 2007. 261 с.
5. Лукина М.М., Фомичева И.Д. СМИ в пространстве Интернета. Серия «Интернет-журналистика». Вып. 1. Москва: МГУ им. М.В. Ломоносова. Фак. Журналистики, 2005. 87 с.
6. Ющенко М.А. Средства массовой коммуникации как механизм формирования властью общественного сознания граждан // Вестник Томского государственного университета. 2007. № 305. С. 67-70.
7. Морозова А.А. Медиабезопасность в эпоху информации / Информационное поле современной России: практики и эффекты: материалы IX Международной научно-практической конференции, 18-20 октября 2012 г. / под ред. Р.П. Баканова: в 2-х т. Т. 1. Казань: Казан. ун-т, 2012. С. 280-287.
8. Фатеева И.А. Что такое медиабезопасность, и как она соотносится с информационной безопасностью? // Экология медиасреды: материалы III Открытой межвузовской научно-практической конференции / под редакцией И.А. Фатеевой, И.В. Жилавской. Московский педагогический государственный университет (Москва), 2018. С. 98-107.
9. Чернышов А.Г. Стратегия и философия цифровизации / Власть. 2018. № 5. С. 13-21.
10. Галяшина Е.И., Никишин В.Д. К вопросу о концепции юридико-лингвистического обеспечения информационной (мировоззренческой) безопасности в цифровой среде // Становление личности в современном обществе: сборник научных трудов Международной научно-практической конференции. Юргинский технологический институт. Томск: Изд-во Томского политехнического университета, 2018. С. 266-269.
11. Никишин В.Д. Цифровые и речевые следы в аспекте обеспечения информационной (мировоззренческой) безопасности в интернет-среде // Судебная экспертиза. 2020. № 1 (61). С. 131-139.
12. Россинская Е.Р. Учение о цифровизации судебно-экспертной деятельности и проблемы судебно-экспертной дидактики // Правовое государство: теория и практика. 2020. № 4 (62). Ч. 1. С. 88-101.
13. Теория судебной экспертизы (судебная экспертология): учебник / Е.Р. Россинская, Е.И. Галяшина, А.М. Зинин; под ред. Е.Р. Россинской. 2-е изд. перераб. и доп. Москва: Норма: ИНФРА-М, 2018. 368 с.

REFERENCES

1. Morozova L.A. Teoriya gosudarstva i prav. Moskva: Eksmo. Rossijskoe yuridicheskoe obrazovanie. 2010. 510 s.
2. Kuz'min A.M. Kategoriya «mediasreda» i ee soderzhanie na sovremennom etape razvitiya obshchestva // Elektronnyj nauchnyj zhurnal «Mediaskop». 2011. № 1. // URL: http://www.mediascope.ru/node/765 (data obrashcheniya: 26.03.2022).
3. SHkondin M.V. Informacionnyj potencial obshchestva i koncepty celostnosti mediasistemy // Voprosy teorii i praktiki zhurnalistiki. 2015. № 4. S. 335-348.
4. Proskurin S.A. Geopoliticheskoe izmerenie global'nogo informacionnogo prostranstva // Geopolitika: uchebnik / pod obshch. red. V.A. Mihajlova. Moskva: Izd-vo RAGS, 2007. 261 s.
5. Lukina M.M., Fomicheva I.D. SMI v prostranstve interneta. Seriya «Internet-zhurnalistika». Vyp. 1. Moskva: MGU im. M.V. Lomonosova. Fak. ZHurnalistiki, 2005. 87 s.
6. YUshchenko M.A. Sredstva massovoj kommunikacii kak mekhanizm formirovaniya vlast'yu obshchestvennogo soznaniya grazhdan // Vestnik Tomskogo gosudarstvennogo universiteta. 2007. № 305. S. 67-70.
7. Morozova A.A. Mediabezopasnost' v epohu informacii / Informacionnoe pole sovremennoj Rossii: praktiki i effekty: materialy IX Mezhdunarodnoj nauchno-prakticheskoj konferencii, 18-20 oktyabrya 2012 g. / pod red. R.P. Bakanova: v 2-h t. T. 1. Kazan': Kazan. un-t, 2012. S. 280-287.
8. Fateeva I.A. CHto takoe mediabezopasnost', i kak ona sootnositsya s informacionnoj bezopasnost'yu? // Ekologiya mediasredy: materialy III Otkrytoj mezhvuzovskoj nauchno-prakticheskoj konferencii / pod

redakciej I.A. Fateevoj, I.V. ZHilavskoj. Moskovskij pedagogicheskij gosudarstvennyj universitet (Moskva), 2018. S. 98-107.
9. CHernyshov A.G. Strategiya i filosofiya cifrovizacii / Vlast'. 2018. № 5. S. 13-21.
10. Galyashina E.I., Nikishin V.D. K voprosu o koncepcii yuridiko-lingvisticheskogo obespecheniya informacionnoj (mirovozzrencheskoj) bezopasnosti v cifrovoj srede // Stanovlenie lichnosti v sovremennom obshchestve: sbornik nauchnyh trudov Mezhdunarodnoj nauchno-prakticheskoj konferencii. YUrginskij tekhnologicheskij institut. Tomsk: Izd-vo Tomskogo politekhnicheskogo universiteta, 2018. S. 266-269.
11. Nikishin V.D. Cifrovye i rechevye sledy v aspekte obespecheniya informacionnoj (mirovozzrencheskoj) bezopasnosti v internet-srede // Sudebnaya ekspertiza. 2020. № 1 (61). S. 131-139.
12. Rossinskaya E.R. Uchenie o cifrovizacii sudebno-ekspertnoj deyatel'nosti i problemy sudebno-ekspertnoj didaktiki // Pravovoe gosudarstvo: teoriya i praktika. 2020. № 4 (62), ch. 1. S. 88-101.
13. Teoriya sudebnoj ekspertizy (sudebnaya ekspertologiya): uchebnik / E.R. Rossinskaya, E.I. Galyashina, A.M. Zinin; pod red. E.R. Rossinskoj. 2-e izd. pererab. i dop. Moskva : Norma : INFRA-M, 2018. 368 s.

Информация об авторе:
Богатырев Константин Михайлович, младший научный сотрудник Центра правовой экспертизы в сфере противодействия идеологии терроризма и профилактики экстремизма, аспирант кафедры криминалистики Московского государственного юридического университета имени О.Е. Кутафина, https://orcid.org/0000-0001-6300-009X, kbog@rambler.ru

Автор прочитал и одобрил окончательный вариант рукописи.

Information about the author:
Bogatyrev Konstantin M., Junior Researcher of the Center for Legal Expertise in Counteracting the Ideology of Terrorism and Prevention of Extremism, Postgraduate Student of the Forensic Expertise Department at Kutafin Moscow State Law University, https://orcid.org/0000-0001-6300-009X, kbog@rambler.ru

The author has read and approved the final version of the manuscript.

Статья получена: 28.04.2022.
Статья принята к публикации: 21.12.2022.
Статья опубликована онлайн: 26.12.2022.

Против размещения полнотекстовой версии статьи в открытом доступе в сети Интернет не возражаю.