■ ■ ■ Нормативные правовые аспекты государственного и муниципального управления в сфере информационно-психологической безопасности граждан

Нечаева И.И.[1], Шевченко А.Н.[2]

1. Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых (ВлГУ), Владимир, Российская Федерация.
2. Владимирский филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (РАНХиГС), Владимир, Российская Федерация.

Аннотация. Современная информационная среда представляет собой сложную сферу общественного устройства. Информация, которая ежесекундно окружает нас, может оказывать как плодотворное влияние, потенциально приводящее к развитию личности и общества, так и негативное, которое нацелено на разрушение систем и человека. В современном обществе, с его стремительно растущими техническими возможностями, объемами производящейся и потребляемой информации риски информационного воздействия распространяются как на технические аспекты безопасности, так и на психолого-идеологические. В связи с этим качественно новой и важной становится задача противодействия информационным угрозам на всех уровнях. Существующее российское законодательство уделяет внимание всем ключевым направлениям информационной безопасности общества, однако не разводит данное понятие по сферам влияния, исследуя вопрос комплексно. В представленной статье внимание уделено анализу нормативно-правовой базы в части установления основ федеральной политики в области государственного развития и в сфере превенции дестабилизирующей информационной активности с позиций внешнего психологического информационного воздействия.

Ключевые слова: государственное и муниципальное управление, правовые основы информационной безопасности, информационная безопасность, информационное воздействие, государственная политика, информационные угрозы, угрозы информационной безопасности, информационно-психологическая безопасность

Для цитирования: Нечаева И.И., Шевченко А.Н. Нормативные правовые аспекты государственного и муниципального управления в сфере информационно-психологической безопасности граждан // Коммуникология. 2021. Том 9. № 2. С. 143-155. DOI: 10.21453/2311-3065-2021-9-2-143-155.

Сведения об авторах: Нечаева Ирина Игоревна – кандидат социологических наук, доцент, доцент кафедры социологии Владимирского государственного университета имени Александра Григорьевича и Николая Григорьевича Столетовых (ВлГУ); Шевченко Александр Николаевич – магистрант Владимирского филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (РАНХиГС). *Адрес:* 600000, Россия, г. Владимир, ул. Горького, 87. *E-mail:* nechaevaii@list.ru; demiurg_08@mail.ru.

Статья поступила в редакцию: 16.05.2021. *Принята к печати:* 07.06.2021.

Современное информационное общество предполагает стремительное развитие новых технологий, прозрачность границ и быстрое реагирование в контексте многозадачности. Роль информационной сферы во всех областях жизнедеятельности трудно переоценить. Информация, информационная инфраструктура, субъекты информационного обмена прочно и с наращиванием объемов входят в общественные отношения, образуя собственные системы и собственные отношения внутри них. Возрастающая скорость обмена информацией, которая сегодня находится на качественно новом уровне, влечет за собой и пропорционально растущую потребность в управлении этими потоками и, прежде всего, на уровне федеральных органов законодательной и исполнительной власти.

Информационное пространство, которое стало неотъемлемой частью жизни людей и стабильного функционирования общества и государства, как и любое другое социальное явление, является противоречивым. С одной стороны, обеспечивается быстрый обмен информацией, наращиваются объемы ее хранения и механизмы аналитики, упрощается доступ к ее получению и использованию на разных уровнях организации общества. С другой стороны, появляются новые угрозы социально-экономической и кибербезопасности, качественно новые возможности ведения информационных и гибридных войн, совершенствуются механизмы сетецентрических войн и т.д., что отражается на национальной безопасности общества в целом, и психологической безопасности граждан в частности.

Вопросу информационной безопасности в отечественной и зарубежной литературе уделено большое внимание. Значительный исследовательский сектор составляют научные работы, посвященные анализу нормативных правовых актов в сфере обеспечения информационной безопасности на государственном уровне.

Правовые аспекты влияния информационно-коммуникационных технологий на развитие современного общества были исследованы в трудах А.Б. Венгерова [Венгеров]; О.А. Городова [Городов], В.Б. Наумова [Архипов, Наумов, Пчелинцев, Чирко], И.М. Рассолова [Рассолов] и др., среди западных исследователей по данному вопросу можно отметить труды Д.Р. Джонсона [Johnson], Л. Лессига [Lessig], Д. Хьюза [Hughes] и др.

Различные правовые аспекты обеспечения информационной безопасности личности, общества, государства исследованы в трудах С.А. Буданова [Буданов], С.Н. Головина [Головин], Л.А. Коврижных [Коврижных] и др.

Отдельную группу составляют источники, связанные с политическим аспектом обеспечения информационной безопасности РФ: А.В. Кубышкин [Кубышкин], В.Е. Макаров [Макаров], А.В. Манойло [Манойло], Е.С. Муравьева [Муравьева] и др. Так, например, в монографии В.Е. Макарова представлен новый подход к вопросу о влиянии политических и социальных аспектов на обеспечение информационной безопасности личности, социальных групп, общества и государства в современных условиях усилившегося информационного воздействия со стороны США и некоторых стран Западной Европы.

Место информационно-психологической безопасности в контексте государственной безопасности

Одной из наиболее приоритетных задач любого государства является безопасность. Пол Д. Уильямс в целом под безопасностью понимает мощный политический инструмент в привлечении внимания к приоритетным вопросам, относя ее к «козырным картам» в борьбе за распределение ресурсов [Williams: 2]. С. Макинда определяет безопасность как сохранение норм, правил, институтов и ценностей общества, осуществление защиты от военных и невоенных угроз [Makinda: 281-292]. В отечественной литературе понятие «безопасность» синонимизируется с «защищенностью», либо раскрывается непосредственно через объекты безопасности или угрозы, как, например, в российской нормативно-правовой базе. Общим в зарубежных и отечественных научно-правовых изысканиях является связь безопасности, государства и личности. Так, в рамках национальной безопасности Российской Федерации одним из главных направлений обеспечения государственной и общественной безопасности обозначено усиление роли государства в качестве гаранта безопасности личности[1].

Информационная безопасность является неотъемлемой и важной частью национальной безопасности, которая в свою очередь исходит из понимания безопасности в целом. В части установления цепочки «безопасность – национальная безопасность – информационная безопасность» нельзя не согласиться с предложенными коллективом авторов уровнями безопасности [Голубчиков, Новиков, Баранова: 321]. Однако далее в предложенной схеме в качестве следующего уровня безопасности указана ее защита. Статья 16 Федерального закона «Об информации, информационных технологиях и о защите информации» определяет в качестве основных направлений защиты информации «обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; соблюдение конфиденциальности информации ограниченного доступа; реализацию права на доступ к информации»[2], что отражает суть в большей степени технического аспекта вопроса. Непосредственно информационно-психологический уровень воздействия рассматривается авторами лишь в контексте защиты информации в качестве угроз в области информационной безопасности [Голубчиков, Новиков, Баранова: 322]. Мы видим целесообразным выделить в самостоятельный уровень информационно-психологическую безопасность, а в качестве основных угроз указать причинение вреда здоровью человека; нейролингвистическое воздей-

[1] Указ Президента РФ от 31.12.2015 N 683 «О Стратегии национальной безопасности Российской Федерации».

[2] Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 09.03.2021) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 20.03.2021).

ствие на сознание человека, искусственное привитие ему синдрома зависимости; утрату способности к политической, культурной, нравственной самоидентификации человека; манипуляцию общественным сознанием; разрушение единого информационного и духовного пространства Российской Федерации, традиционных устоев общества и общественной нравственности, а также нарушения иных жизненно важных интересов личности, общества и государства, которые были предложены в тексте снятого с рассмотрения законопроекта[1], и т.д. Обратимся к имеющейся базе нормативных правовых документов, затрагивающих вопрос информационной и информационно-психологической безопасности.

Нормативные основы государственного и муниципального управления в сфере информационной и информационно-психологической безопасности

В целом информационная безопасность обеспечивается комплексом нормативно-правовых актов, прежде всего, основами законодательства выступают Конституция Российской Федерации, Федеральный закон от 14.06.1994 N 5-ФЗ (ред. от 01.07.2017) «О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат Федерального Собрания», Указ Президента РФ от 23.05.1996 N 763 (ред. от 29.05.2017) «О порядке опубликования и вступления в силу актов Президента Российской Федерации, Правительства Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти» и другие.

К стратегическим документам можно отнести «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» (утв. Президентом РФ 24.07.2013 N Пр-1753), Указ Президента РФ от 31.12.2015 N 683 «О Стратегии национальной безопасности Российской Федерации», Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», Указ Президента РФ от 09.05.2017 N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы», Выписка из Основных направлений научных исследований в области обеспечения информационной безопасности Российской Федерации (утв. Секретарем Совета Безопасности Российской Федерации Н.П. Патрушевым 31 августа 2017 г.), Распоряжение Правительства РФ от 03.06.2019 N 1189-р «Об утверждении Концепции создания и функционирования национальной системы управления данными и плана мероприятий («дорожную карту») по созданию национальной системы управления данными на 2019 – 2021 годы», Указ Президента РФ от 10.10.2019 N 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»).

[1] Проект Федерального закона N 99114515-2 «Об информационно-психологической безопасности» (ред., внесенная в ГД ФС РФ, текст по состоянию на 03.12.1999).

Системообразующими документами, которые тем или иным образом регулируют различные аспекты обеспечения информационной безопасности являются Гражданский кодекс Российской Федерации, Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 19.07.2018) «Об информации, информационных технологиях и о защите информации», Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера».

Кроме того, Указ Президента РФ от 16.08.2004 N 1085 (ред. от 08.05.2018) «Вопросы Федеральной службы по техническому и экспортному контролю», Приказ ФСТЭК России от 12.05.2005 N 167 (ред. от 26.04.2018) «Об утверждении Регламента Федеральной службы по техническому и экспортному контролю» (Зарегистрировано в Минюсте России 06.06.2005 N 6682), Федеральный закон от 03.04.1995 N 40-ФЗ (ред. от 07.03.2018) «О федеральной службе безопасности», Указ Президента РФ от 11.08.2003 N 960 (ред. от 03.07.2018) «Вопросы Федеральной службы безопасности Российской Федерации», Постановление Правительства РФ от 02.06.2008 N 418 (ред. от 25.09.2018) «О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации», Постановление Правительства РФ от 16.03.2009 N 228 (ред. от 25.09.2018) «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» (вместе с «Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций») и др.

Вопросы технического регулирования в части стандартизации, определения процедур оценки соответствия средств защиты информации, определения мероприятий по аттестации объектов информатизации по требованиям безопасности информации, особенностей проведения измерений регулируются Федеральным законом от 27.12.2002 N 184-ФЗ (ред. от 29.07.2017) «О техническом регулировании», Федеральным законом от 26.06.2008 N 102-ФЗ (ред. от 13.07.2015) «Об обеспечении единства измерений», Федеральным законом от 29.06.2015 N 162-ФЗ (ред. от 03.07.2016) «О стандартизации в Российской Федерации», Постановлением Правительства РФ от 30.12.2016 N 1567 «О порядке стандартизации в отношении оборонной продукции (товаров, работ, услуг) по государственному оборонному заказу, продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, продукции, сведения о которой составляют государственную тайну, а также процессов и иных объектов стандартизации, связанных с такой продукцией». Это далеко не полный перечень нормативных правовых актов, регулирующих сферу информационной безопасности.

Бесспорно, выходящая на первый план в современном обществе информационная сфера оказывает влияние на состояние всех сфер общества (политической, экономической, оборонной и других) и аспектов безопасности Российской Федерации. Понимание необходимости обеспечения информационной и информационно-психологической безопасности, как неотъемлемой составля-

ющей государственной безопасности, мы видим в тексте Стратегии национальной безопасности Российской Федерации до 2025 года, предписывающей обеспечение, в том числе, предупреждение попыток фальсификации истории России, противодействие пропаганде идей экстремизма в средствах массовой информации и электронных коммуникаций; реализацию мер правового и информационного характера по профилактике использования национального и религиозного факторов, совершенствование государственной информационной системы мониторинга в сфере межнациональных и межконфессиональных отношений и раннего предупреждения конфликтных ситуаций и др.[1]. Стратегия пространственного развития Российской Федерации на период до 2025 года в качестве основных направлений социально-экономического развития субъектов Российской Федерации, относящихся к приоритетным геостратегическим территориям Российской Федерации, характеризующимся эксклавным положением, относит, в том числе, обеспечение транспортной, энергетической и информационно-телекоммуникационной безопасности[2].

Доктрина информационной безопасности Российской Федерации рассматривает информационную безопасность как состояние защищенности жизненно важных интересов личности, общества, государства в информационной сфере от внешних и внутренних угроз, обеспечивающее ее формирование, использование и развитие, через снятие информационной неопределенности. Состояние защищенности при этом возможно лишь через реализацию комплекса правовых, научно-технических, специальных, организационных механизмов и мер, направленных на своевременное выявление, сдерживание, реальное противодействие и пресечение неправомерного получения и распространения защищаемой информации органами государственной власти, физическими и юридическими лицами.

Национальные интересы в сфере информационной безопасности Доктрина подразделяет на четыре основных составляющие: соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны; информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам; раз-

[1] Указ Президента РФ от 19.12.2012 N 1666 (ред. от 06.12.2018) «О Стратегии государственной национальной политики Российской Федерации на период до 2025 года».

[2] Стратегия пространственного развития Российской Федерации на период до 2025 года. Утверждена распоряжением Правительства Российской Федерации от 13 февраля 2019 г. № 207-р.

витие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов; защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России[1].

В соответствии с п. 1 ст. 10 Конвенции о защите прав человека и основных свобод каждый имеет право свободно выражать свое мнение, в том числе, свободу получать и распространять информацию и идеи без какого-либо вмешательства со стороны публичных властей и независимо от государственных границ. Согласно ст. 29 Всеобщей декларации прав человека, п. 3 ст. 19, ст. 20 Международного пакта о гражданских и политических правах, п. 2 ст. 10 Конвенции о защите прав человека и основных свобод, ст. 29, 55 Конституции РФ, реализация указанных прав может быть сопряжена с ограничениями, установленными законом с целью уважения в обществе прав и репутации других лиц, охраны государственной безопасности и общественного порядка, предотвращения беспорядков и преступлений, охраны здоровья и нравственности и т.д. Ст. 4 Закона РФ от 27.12.1991 N 2124-1 «О средствах массовой информации» содержит запрет на злоупотребление свободой массовой информации. Так, не допускается использование СМИ, в том числе, для распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости и материалов, содержащих нецензурную брань. Кроме того, запрещается использование технических приемов распространения информации, воздействующей на подсознание людей и (или) оказывающих вредное влияние на их здоровье и т.д. В соответствии со ст. 15.1 Федерального закона «Об информации, информационных технологиях и о защите информации»[2] в целях ограничения доступа к сайтам в сети «Интернет», содержащим материалы с порнографическими изображениями несовершеннолетних, информации о способах совершения самоубийства, а также призывов к совершению самоубийства, информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), информации, направленной на склонение или иное вовлечение несовершеннолетних в совершение противоправных действий, представляющих угрозу для их жизни и (или) здоровья либо для жизни и (или) здоровья иных лиц и т.д.,

[1] Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Доктрина информационной безопасности Российской Федерации».

[2] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.

создается единая автоматизированная информационная система «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено».

Информационные механизмы психологического воздействия и основные направления борьбы с ними

Несмотря на принимаемые меры, наиболее уязвимым в плане противоправных действий в сфере информационной безопасности на данный момент остается пространство «Интернет». В современной информационной среде, наряду с «разумным» контентом, можно столкнуться с большим количеством «информационных вбросов». Их появление обусловлено множеством причин, в том числе, огромным потоком информации, где качество уступает количеству, так как человек не справляется с предлагаемыми, а порой и навязанными ему объемами, и, как следствие, принимает информацию в «сыром» виде, без тщательного анализа и проверки; доступностью; высокой эффективностью самого механизма и его дешевизной. Современный потребитель контента в своей массе отдает предпочтение коротким, желательно визуализированным, сообщениям, а не полноценным информативным тестам, и информационные вбросы отлично вписываются в контекст подобного стремительного изменения, представляя собой короткие сообщения, вызывающие сильное эмоциональное возбуждение. Если к рекламным вбросам люди уже почти привыкли, то вбросы политические, связанные с созданием определенного отношения к политической ситуации в целом, политическому объекту или субъекту, вызывают большой резонанс в обществе. Именно политические вбросы наиболее негативны и зачастую недостоверны.

Важно отметить, что воздействие на психику и эмоциональное состояние людей, особенно в стрессовой ситуации, оказывает как недостаток информации, так и ее переизбыток и противоречивость. Часто появление «нездоровой» информационной активности противоречивого и не соответствующего реальности содержания приходится на периоды выборов в органы государственной власти, трагических событий и происшествий в обществе, военных действий и прочего. Особенно остро эта проблема встала в период пандемии короновируса в мире, когда достаточно большое распространение и «обратную связь» получили так называемые фейковые новости, спекулирующие на ней. В российском законодательстве под фейком понимается заведомо недостоверная общественно значимая информация, распространяемая под видом достоверных сообщений и создавшая определенную угрозу жизни или здоровью граждан, имуществу, общественному порядку и общественной безопасности[1]. Это понятие, как и мера ответственности, появилось в марте 2019 года с целью противодействия распро-

[1] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

странению заведомо недостоверной информации и нагнетания общественной паники. Также в марте 2019 года был введен механизм ограничения доступа к такой информации Роскомнадзором по обращению Генеральной прокуратуры РФ.

Роскомнадзором ведется единый реестр запрещенных сайтов непрерывно в электронном виде в соответствии с Правилами, утвержденными постановлением Правительства РФ от 26.10.2012 № 1101. Объектом блокировки может быть доменное имя, страница сайта, сетевой адрес, а с 01.10.2020 г. – приложение. Для запуска механизма блокировки Роскомнадзору необходимо основание, которым может быть решение уполномоченного органа (административная блокировка); решение суда (судебная блокировка); предписание судебного пристава-исполнителя, таким образом, не всегда Роскомнадзор самостоятельно принимает решение о блокировке объекта. Далее, при наличии положительного решения, объект в течение суток вносится Роскомнадзором в Реестр. Одновременно с занесением интернет-ресурса в число запрещенных выясняется провайдер хостинга данного ресурса, после этого Роскомнадзор направляет ему и владельцу сайта электронное уведомление о блокировке. При условии, если владелец интернет-ресурса после получения уведомления удалил запрещенную информацию, то сайт не включается в реестр запрещенных. Если владелец не удалил контент, то провайдер хостинга обязан ограничить доступ к нему, а Роскомнадзор включает его в Реестр. В случае, если контент содержит информацию, порочащую честь и достоинство, недостоверную информацию, нарушает авторские права или распространяет персональные данные, тогда для блокировки необходимо судебное решение.

Кроме фейков, в пространстве «Интернет» все чаще встречаются случаи «троллинга» с целью нагнетания негативного восприятия, гнева собеседника или собеседников. Троллинг также может носить политический характер с негативными оттенками и встречается чаще всего в социальных сетях при обсуждении участниками группы контента, даже неполитического. Другим проявлением информационно-психологического воздействия можно назвать кибербуллинг. В самом общем понимании, он представляет собой насилие, травлю в цифровом пространстве. Являясь обобщающим понятием для кибермоббинга, кибертравли и выходящего за границы телекоммуникационных сетей киберсталкинга – преследования жертвы через повторяющиеся сообщения, вызывающие тревогу и раздражение. Кибербуллинг (киберсталкинг) может выражаться в нападении в публичных группах социальных сетей, распространении заведомо ложной порочащей честь и достоинство другого лица информации или ложных сведений, «кража личности» с целью отправки провокационной информации другим пользователям, в том числе, хеппислепинг. Российское агентство правовой и судебной информации отмечает, что в 2020 году эта проблема встала особенно остро, что обусловлено пандемией коронавируса и ее последствиями, как в политической, экономической, так и в социальной сфере. В этой ситуации повышенной тревожности граждан, отсутствия прямой ответственности за кибер-

буллинг и вытекающее из этого ощущение безнаказанности за деяния, совершенные в Сети, клевета становится угрозой практически государственного масштаба. Существующие правовые инструменты, в частности, наказание за доведение до самоубийства (ст. 110 УК РФ), за клевету (ст. 128.1 УК РФ), оскорбление представителя власти (ст. 319 УК РФ) и т.д., на практике не дают возможность пресечь правонарушения подобного рода в Сети.

Категорией, наиболее уязвимой для такого информационного воздействия, являются дети и молодежь в силу своей высокой активности в социальных сетях и в Интернете в целом. Кроме того, рисковой эту группу делают и возрастные особенности восприятия. Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» относит к таковой информацию, побуждающую к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству; способную вызвать у детей желание употребить наркотические средства, психотропные вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и т.д.; обосновывающую или оправдывающую допустимость насилия и жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным; отрицающую семейные ценности, пропагандирующую нетрадиционные сексуальные отношения и формирующую неуважение к родителям или другим членам семьи и другую. В соответствии с п. 1 ст. 14 Федерального закона от 24 июля 1998 г. N 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации» органы государственной власти в Российской Федерации принимают меры по защите ребенка от информации, пропаганды и агитации, наносящих вред его здоровью, нравственному и духовному развитию.

Выводы. Понятие информационно-психологического воздействия включает в себя множество аспектов. Во-первых, это информационное влияние на граждан государства с целью подрыва политической, экономической, социальной и культурной систем общества другим государством в ходе информационной войны. Здесь мы говорим о психолого-идеологическом воздействии, дестабилизирующем общество, манипулировании контентом, дезинформации, подмене традиционных ценностей и моральных норм нравственными суррогатами. Во-вторых, использование информации с целью организации экстремистских, террористических организаций с привлечением новых участников через использование информационных технологий. В-третьих, использование информационно-коммуникационных технологий для ущемления прав и свобод человека и гражданина, реализуемых в информационном пространстве. Это далеко не все направления влияния, по которым должно осуществляться информационное противодействие, являющееся неотъемлемой частью информационной безопасности человека и общества.

Несмотря на наличие механизмов правового регулирования информационного воздействия на население, многие из них не отвечают современным реалиям

в полной мере. На наш взгляд, принципиально новое информационное законодательство Российской Федерации находится сейчас на начальном этапе своего формирования и пока не охватывает всего сложившегося многообразия отношений, связанных с профилактикой и пресечением информационных угроз и их последствий. Так, работающим правовым механизмом на сегодняшний день является блокировка подобного контента Роскомнадзором, однако, осуществить это в рамках множества пользователей и платформ задача достаточно сложная: быстрый обмен информацией, анонимность в Интернете, количество сайтов и приложений и т.д.

Источники

Архипов В.В., Наумов В.Б., Пчелинцев Г.А, Чирко Я.А. (2016). Открытая концепция регулирования Интернета вещей // Информационное право. № 2. С. 18-25.

Буданов С.А. (2006). Правовое обеспечение информационной безопасности несовершеннолетних: дис. ... канд. юрид. наук: 05.13.19 Воронеж.

Венгеров А.Б. (2005). Теория государства и права: Учебник. 2-е изд. М.: ОмегаЛ.

Головин Ю.А., Орлов А.Н. (2013). Возрастание роли СМИ в обеспечении информационной безопасности // Знание. Понимание. Умение. № 2. С. 147-152.

Голубчиков С.В., Новиков В.К., Баранова А.В. (2017). Уровни и правовая модель информационной безопасности (защиты информации) // Программные продукты и системы. №2 [режим доступа]: https://cyberleninka.ru/article/n/urovni-i-pravovaya-model-informatsionnoy-bezopasnosti-zaschity-informatsii (дата обращения: 14.05.2021).

Городов О.А. (2008). Информационное право: учебник. М.: Проспект.

Коврижных Л.А. (2009). О проблеме совершенствования информационного законодательства // Актуальные проблемы российского права. Изд-во МГЮА. № 4 (13). С. 334-341.

Кубышкин А.В. (2002). Международно-правовые проблемы обеспечения информационной безопасности государства: автореф. дис. канд. юр. наук. Москва.

Макаров В.Е. (2015). Политические и социальные аспекты информационной безопасности: Монография. Изд.: Scientific magazine «Kontsep».

Манойло А.В. (2019). «Фейковые новости» как угроза национальной безопасности и инструмент информационного управления // Вестник Московского университета. Серия 12: Политические науки. № 2 (Март-Апрель 2019). С. 37-45.

Муравьева Е.С. (2020). Некоторые проблемы обеспечения информационной безопасности на международном уровне // Вопросы российской юстиции. №7 [режим доступа]: https://cyberleninka.ru/article/n/nekotorye-problemy-obespecheniya-informatsionnoy-bezopasnosti-na-mezhdunarodnom-urovne (дата обращения: 14.05.2021).

Рассолов И.М. (2011). Информационное право: учебник. М.: Издательство Юрайт.

Hughes J. (2003). The Internet and the Persistence of Law. Boston College Law Review. Vol. 44, Issue 2 [access]: https://lawdigitalcommons.bc.edu/bclr/vol44/iss2/4.

Johnson D.R., Post D. (2001). Law and Borders – The Rise of Law in Cyberspace. In: Peter Ludlaw (ed.), Crypto Anarchy, Cyberstates, and Pirate Utopias. Cambridge: Massachusetts Institute of Technology.

Lessig L. (1999). Code And Other Laws Of Cyberspace. NY: Basic Books.

Makinda S. (1998). Sovereignity and Global Security, Security Dialogue. Sage Publications. Vol. 29(3) 29: 281-292.

Williams P., ed. (2008). Security Studies: An Introduction. Routledge, UK [access mode]: https://www.academia.edu/25723482/Paul_D_Williams_Security_Studies_An_Introduction.pdf.

■ ■ ■ Regulatory Legal Aspects of State and Municipal Governance in the Sphere of Information and Psychological Security of Citizens

Nechaeva I.I.[1], Shevchenko A.N.[2]

1. Vladimir State University, Vladimir, Russia.
2. Vladimir branch of Russian Presidential Academy of National Economy and Public Administration, Vladimir, Russia.

Abstract. The modern information environment is a complex social structure. The information that surrounds us every second can have both a fruitful influence, potentially leading to the development of the individual and society, and a negative one, which is aimed at the destruction of systems and humans. In modern society with its rapidly growing technical capabilities, volumes of produced and consumed information, the risks of information impact extend both to technical aspects of security and psychological and ideological ones. In this regard, the task of countering information threats at all levels is becoming a qualitatively new and important task. Russian legislation pays attention to all key areas of information security of society, but does not separate this concept by spheres of influence, examining the issue comprehensively. In the presented article, attention is paid to the analysis of the regulatory framework in terms of establishing the foundations of federal policy in the field of state development and in the field of preventing destabilizing information activity from the standpoint of external psychological information impact.

Keywords: state and municipal administration, legal foundations of information security, information security, information impact, government policy, information threats, threats to information security, information and psychological security

For citation: Nechaeva I.I., Shevchenko A.N. (2021). Regulatory Legal Aspects of State and Municipal Governance in the Sphere of Information and Psychological Security of Citizens. *Communicology (Russia).* Vol. 9. No. 2. P. 143-155. DOI: 10.21453/2311-3065-2021-9-2-143-155.

Information about the authors: Nechaeva Irina Igorevna – Cand. Sc. (Soc.), associate professor at the Department of sociology, Vladimir State University; Shevchenko Aleksandr Nikolaevich – postgraduate student at the Department of Public Relations and media policy, Vladimir branch of Russian Presidential Academy of National Economy and Public Administration. *Address:* 600000, Russian Federation, Vladimir, Gorkogo, 87. *E-mail:* nechaevaii@list.ru; demiurg_08@mail.ru

Received: 16.05.2021. *Accepted:* 07.06.2021.

References

Arkhipov V.V., Naumov V.B., Pchelintsev G.A., Chirko Ya.A. (2016). Open concept of regulation of the Internet of things. *Information law*. No. 2. P. 18-25 (In Rus.).

Budanov S.A. (2006). Legal support of information security of minors: dissert. Cand. jurid. sciences. Voronezh (In Rus.).

Golovin Yu.A., Orlov A.N. (2013). The increasing role of the media in ensuring information security. *Knowledge. Understanding. Skills*. No. 2. P. 147-152 (In Rus.).

Golubchikov S.V., Novikov V.K., Baranova A.V. (2017). Levels and legal model of information security (information protection). *Software products and systems*. No. 2 [access mode]: https://cyberleninka.ru/article/n/urovni-i-pravovaya-model-informatsionnoy-bezopasnosti-zaschity-informatsii (In Rus.).

Gorodov O.A. (2008). Information law: textbook. Moscow: Prospect (In Rus.).

Hughes J. (2003). The Internet and the Persistence of Law. Boston College Law Review. Vol. 44, Issue 2 [access]: https://lawdigitalcommons.bc.edu/bclr/vol44/iss2/4.

Johnson D.R., Post D. (2001). Law and Borders – The Rise of Law in Cyberspace. In: Peter Ludlaw (ed.), Crypto Anarchy, Cyberstates, and Pirate Utopias. Cambridge: Massachusetts Institute of Technology.

Kovrizhnykh L.A. (2009). On the problem of improving information legislation. *Actual problems of Russian law*. No. 4 (13). P. 334-341 (In Rus.).

Kubyshkin A. V. International legal problems of ensuring the information security of the state. Dissert. thesis Cand. jurid. sciences. Moscow.

Lessig L. (1999). Code And Other Laws Of Cyberspace. NY: Basic Books.

Makarov V.E. (2015). Political and social aspects of information security. Scientific magazine Kontsep.

Makinda S. (1998). Sovereignity and Global Security, Security Dialogue. Sage Publications. Vol. 29(3) 29: 281-292.

Manoilo A.V. (2019). «Fake news» as a threat to national security and an information management tool. *Bulletin of Moscow University. Series 12: Political Sciences.* No. 2 (March-April 2019). P. 37-45 (In Rus.).

Muravyova E.S. (2020). Some problems of ensuring information security at the international level. *Issues of Russian Justice*. No. 7 [access mode]: https://cyberleninka.ru/article/n/nekotorye-problemy-obespecheniya-informatsionnoy-bezopasnosti-na-mezhdunarodnom-urovne (In Rus.).

Rassolov I.M. (2011). Information law. M.: Yurayt Publishing House (In Rus.).

Vengerov A.B. (2005). Theory of State and Law. 2nd ed. M.: OmegaL (In Rus.).

Williams P., ed. (2008). Security Studies: An Introduction. Routledge, UK [access mode]: https://www.academia.edu/25723482/Paul_D_Williams_Security_Studies_An_Introduction.pdf.